

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	MRO2019021434	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
2	MRO2019021892			Yes	Yes					Yes				Category 2 – 12: 2 years
3	MRO2018019541			Yes	Yes						Yes			Category 2 – 12: 2 years
4	MRO2019021039			Yes	Yes									Category 2 – 12: 2 years
5	MRO2019021432			Yes	Yes									Category 2 – 12: 2 years
6	MRO2019021435			Yes	Yes									Category 2 – 12: 2 years
7	MRO2019021056		Yes	Yes	Yes									Category 2 – 12: 2 years
8	MRO2019021363			Yes	Yes									Category 2 – 12: 2 years
9	MRO2019021428	Yes		Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 years
10	MRO2019021429	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
11	MRO2019021430			Yes	Yes									Category 2 – 12: 2 years
12	MRO2018020525			Yes	Yes						Yes			Category 2 – 12: 2 years
13	MRO2018020526			Yes	Yes						Yes			Category 2 – 12: 2 years
14	MRO2017018868	Yes	Yes	Yes	Yes		Yes			Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
15	MRO2019021977			Yes	Yes									Category 2 – 12: 2 years
16	MRO2019021418			Yes	Yes									Category 2 – 12: 2 years
17	MRO2018020736			Yes	Yes					Yes				Category 2 – 12: 2 years
18	NPCC2019021825	Yes		Yes	Yes		Yes		Yes					Categories 3 – 4: 2 years Categories 1, 6, 8: 3 years
19	NPCC2017017392	Yes		Yes	Yes		Yes		Yes					Categories 3 – 4: 2 years Categories 1, 6, 8: 3 years
20	NPCC2017018219			Yes	Yes				Yes					Categories 3 – 4: 2 years Category 8: 3 years
21	NPCC2017018220			Yes	Yes		Yes							Categories 3 – 4: 2 years Category 6: 3 years
21	NPCC2018019761			Yes	Yes		Yes							Categories 3 – 4: 2 years Category 6: 3 years
23	NPCC2019022086	Yes		Yes	Yes									Categories 3 – 4: 2 years Category 1: 3 years
24	RFC2018020558	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
25	RFC2019021232	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
26	RFC2019022043	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2-12: 2 years
27	RFC2019021193			Yes	Yes				Yes					Category 2-12: 2 years
28	RFC2018020825	Yes		Yes	Yes									Category 1: 3 years; 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)
29	RFC2019020978	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
30	RFC2019022044	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2-12: 2 years
31	RFC2019021054	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
32	RFC2019021235	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
33	RFC2019021052	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2-12: 2 years
34	RFC2019021027	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
35	RFC2019021254			Yes	Yes						Yes	Yes		Category 2-12: 2 years
36	RFC201902045	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
37	RFC2019020925	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
38	RFC2019020924	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
39	RFC2019020908	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
40	RFC2019021404	Yes	Yes	Yes	Yes				Yes					Category 1: 3 years; Category 2-12: 2 years
41	RFC2019021403	Yes	Yes	Yes	Yes				Yes					Category 1: 3 years; Category 2-12: 2 years
42	RFC2019021424	Yes	Yes	Yes	Yes				Yes					Category 1: 3 years; Category 2-12: 2 years
43	SERC2017017674			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
44	SPP2017017004			Yes	Yes									Category 2 – 12: 2 year
45	SPP2017017795			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
46	SERC2017018097			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
47	SERC2019021664			Yes	Yes									Category 2 – 12: 2 year
48	SERC2017018610	Yes		Yes	Yes				Yes					Category 2 – 12: 2 year
49	SERC2017017710			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
50	TRE2018019615	Yes		Yes	Yes	Yes				Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
51	TRE2018019619	Yes		Yes	Yes	Yes				Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
52	TRE2018019808	Yes		Yes	Yes	Yes				Yes				Category 1: 3 years; Category 2 – 12: 2 year
53	TRE2019021442			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
54	TRE2018019892	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
55	TRE2019021289			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
56	WECC2017017509	Yes		Yes	Yes									Category 1: 3 years; 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)
57	WECC2017017510	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
58	WECC2018019643	Yes		Yes	Yes				Yes				Yes	Category 2 – 12: 2 years
59	WECC2018020171			Yes	Yes								Yes	Category 2 – 12: 2 years
60	WECC2018020173			Yes	Yes								Yes	Category 2 – 12: 2 years
61	WECC2018020174	Yes		Yes	Yes									Category 2 – 12: 2 years
62	WECC2019021421			Yes	Yes									Category 2 – 12: 2 years
63	WECC2017017925	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
64	WECC2017017926	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
65	WECC2018018973	Yes		Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 years
66	WECC2018018974	Yes		Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 years

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021434	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	05/30/2018	03/07/2019	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 10, 2019, the Entity, submitted a Self-Log stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R1. [REDACTED]</p> <p>In the first instance of noncompliance, the Entity reported that during a review of change requests, IT control staff identified [REDACTED] Electronic Access Control or Monitoring Systems (EACMS), that only perform logging and monitoring, had a deviation from their baseline without authorization. A prior change request issued did not include the [REDACTED] EACMS upgrades. Additionally, [REDACTED] of the device(s) were not part of the approval group business unit manager and were originally installed on May 30, 2018; the [REDACTED] device(s) had the correct approval group manager. The cause of the noncompliance was that the Entity's process was deficient in that it did not ensure that the correct support group and device(s) was/were selected at the time change control requests were issued to upgrade application versions. The noncompliance began on May 30, 2018, when the device(s) was/were installed, and ended on March 6, 2019 when the change request was submitted and approved by the manager.</p> <p>In the second instance of noncompliance, the Entity reported that during routine monitoring of anti-virus software for Windows, a Subject Matter Expert (SME) identified that [REDACTED] applicable Cyber Asset(s) anti-virus applications was/were updated without authorization. The updates were done automatically when the update was scheduled for non-NERC CIP device(s). The device(s) was/were nested in a sub-folder of non-NERC CIP device(s) within the anti-virus management tool and the scheduled update updated all devices in that folder. The cause of the noncompliance was that the Entity's process was deficient in that it did not ensure that correct device(s) was/were selected for updating the anti-virus software. The noncompliance began on March 6, 2019, when the automatic update took place, and ended on March 7, 2019 when the change request was submitted and approved by the manager.</p> <p>The noncompliance began on May 30, 2018, when the device(s) in the first instance was/were installed, and ended on March 7, 2019 when the change request for selecting updates was submitted and approved.</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 Entity reported the first instance as minimal since the EACMS device(s) of issue were limited to performing monitoring and logging and did not perform electronic access controls. Also, the baseline change was planned and the Entity was intending to include the device(s) of issue in the change request, limiting the issue to the documentation of the device(s) in the authorization request. Lastly, the issue was limited to [REDACTED] EACMS. The Entity reported the second issue as minimal because the update was planned for a later date, limiting the issue to applying the update before the intended implementation date and the update provided a fix for a security vulnerability in the previous version and mitigated an active vulnerability. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) submitted a change request to document the update to the device(s) of issue and the change request was authorized on the same day by the manager; 2) assigned the device(s) to the proper support personnel; 3) added a task to new device work flow in its change management tool to require the SME creating a new device to identify the appropriate support group; 4) added a new field to the change request form for displaying device counts in order to identify missing devices; and 5) updated its change management documentation to include reviewing the support group and applicable devices. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) submitted a change request to document the update to the device(s) of issue and the change request was authorized on the same day by the manager; 2) updated anti-virus management tool, so the folder containing NERC CIP devices was moved from non-NERC CIP folder and placed in the NERC CIP folder; 3) updated anti-virus software documentation to reflect the relocated NERC CIP devices folder; and 4) added a task to the new device implementation work flow which addressed malicious code prevention folder updates and moving the NERC CIP devices to new NERC CIP folder. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021892	CIP-010-2	R4	[REDACTED] (the Entity)	[REDACTED]	08/29/2018	08/29/2018	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 violation.)			<p>On May 2, 2019, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R4. [REDACTED]</p> <p>The Entity reported that its transmission system maintenance (TSM) protection technician connected a testing laptop to an isolated medium impact BES Cyber Asset (BCA). The testing laptop is an unapproved Transient Cyber Asset (TCA) installed with specialized software to interface with the protection relay. The substation superintendent realized that the technician should have used a designated TCA laptop (as required by CIP-010-2 R4) and reported the incident to the Entity's NERC compliance department.</p> <p>The cause of the noncompliance was that the Entity failed to follow its documented TCA plan as per CIP-010-2 R4 for medium impact BCAs.</p> <p>The issue began on August 29, 2018 and ended the same day when the unapproved testing laptop was disconnected from the protection 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. The potential impact was isolated to one medium impact substation containing a single BCA. The Entity's Cyber Security team conducted an extent of condition analysis and verified that the scope did not expand to BCAs beyond the single identified instance. Also, the testing laptop did not have wireless capability, this limited the external connectivity and the testing laptop was scanned and showed no malicious code presence. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) disconnected testing laptop from the protection relay; 2) collected all testing laptops across its TSM and removed them from service; 3) checked all testing laptops for viruses and then sanitized them; 4) Cyber Security team verified that technicians were completing full disk encryption for approved devices past tense activity; 5) provided retraining on TCA use for system protection technicians; 6) provided additional training on TCA for all TSM employees; and 7) created visual displays explaining the detection of unauthorized devices and presented examples of what not to do. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019541	CIP-002-5.1a	R2	██████████ (the Entity)	██████	09/27/2017	02/12/2018	Compliance 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 violation.)			<p>During a Compliance Audit conducted from ██████████, MRO determined that the Entity, as a ██████████, was in noncompliance with CIP-002-5.1a R2.</p> <p>MRO determined that the Entity failed to gain CIP Senior Manager (CIP SM) approval for the identifications as per CIP-002-5.1a within 15 calendar months of the last approval. In preparation for the audit MRO’s audit team discovered that Entity reviewed the identifications at least every 15 calendar months, however, the CIP SM did not approve the identifications within the 15 months after the last CIP SM approval in June of 2016.</p> <p>The cause of the noncompliance was that the Entity’s CIP SM approval process was defective, which resulted in failure to complete the approval within 15 calendar months.</p> <p>The noncompliance began on September 27, 2017, when the CIP SM did not approve the CIP-002-5.1a identifications within 15 calendar months, and ended on February 12, 2018, when the CIP SM reviewed the CIP-002-5.1a identifications and found no changes.</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. No changes were made to the identifications. Additionally, the Entity had a process to review the standards/requirements for changes/updates and modifications to assets or systems every 15 calendar months, and the senior manager approval was not obtained since it had no changes. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) approved “Compliance Document Review Form”; and 2) modified its CIP-002-5.1a R2 CIP Senior Manager or delegate approval process to review once every 15 calendar months, even if it has no identified changes in requirement 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
MRO2019021039	CIP-009-6	R3	[REDACTED] (the Entity)	[REDACTED]	10/21/2018	10/31/2018	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 January 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-009-6 R3.</p> <p>The Entity reported that after performing an active recovery of an applicable Cyber Asset (CA) it failed to update the system recovery plan based on lessons learned from the recovery within 90 days. While performing the recovery the Entity identified the recovery plan was missing specific procedures for recovering a failed RAID. The Entity utilized another recovery plan for a different CA type which included the specific procedures for recovering a failed RAID. After performing the recovery the Entity documented the lessons learned and updated the other recovery plan used instead of the recovery plan of issue. The issue was discovered while reviewing the recovery event. Subsequently, the Entity failed to notify each person or group with a defined role of the updates to the plan.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for updating recovery plans after performing a lessons learned review of an actual recovery process.</p> <p>The noncompliance began on October 21, 2018, when the recovery plan was not updated with lessons learned within 90 days, and ended on October 31, 2018, when the correct recovery plan was updated and notifications 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. The Entity stated that the lessons learned were documented after the recovery and the issue was limited to updating the recovery plan, thus documentation in nature. The Entity updated content from the recovery in another system recovery plan provided to SME’s in the same repository, limiting the issue to updating the recovery plan of issue with the same content. Additionally, the actual recovery test associated to the issue was successful, demonstrating that the update to the plan did not impede a recovery, thus, reducing the risk of a failure to perform an active recovery. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the recovery plan of issue with the lessons learned associated to the actual recovery; 2) notified the SMEs of the changes to the updated recovery plan; 2) coached the SME responsible for updating the recovery plans on the significance of updating it within 90 days and to ensure individuals with an assigned role are notified of the changes; and 3) reviewed the difference between the two recovery plans related to the issue with SMEs to ensure proper understanding of which recovery plan to use based on the CA type. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021435	CIP-004-6	R5	[REDACTED] (the Entity)	[REDACTED]	01/12/2019	01/14/2019	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 9, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5.</p> <p>The Entity reported that for one individual with unescorted physical access, it failed to remove that access within 24 hours of the termination action. The Subject Matter Expert (SME) in charge of removing access attempted to schedule the Physical Access Control System (PACS) to automatically remove access at the end of the day. The scheduled removal was not saved successfully to the PACS system, thus the physical access was not removed.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for removing an individual's unescorted physical access within 24 hours of a termination action.</p> <p>The noncompliance began on January 12, 2019, when the individual's access was not removed within 24 hours of the termination action, and ended on January 14, 2019, when access was removed.</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 Entity identified the issue through a non-required review of access logs, which limited the duration to two days. The individual of issue was in good standing with the Entity, and the termination action was related to retirement without cause. Additionally, the individual of issue did not use the unauthorized unescorted physical access during the time of the noncompliance. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) removed access for the individual of issue; and 2) provided training to the SME responsible for performing the access removal in the PACS, specifically to review and ensure the removal command saved. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021056	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	11/30/2018	12/07/2018	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 violation.)			<p>On January 30, 2019, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R1. The Entity reported that after it reinstalled its anti-virus software [REDACTED], it inadvertently reset the configurations for disabling automatic updates of virus definitions and agent software. This led to several instances of virus software updating (a baseline change) in its production environment automatically prior to its scheduled change management time which was not in accordance with its CIP-010-2 program.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for scheduled changes to baseline configurations in its production environment.</p> <p>The noncompliance began on November 30, 2018 when changes were made to baselines that were not in accordance with its configuration change management process, and ended on December 7, 2018 when the last instance of change occurred.</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 issue was self-identified, limiting the issue to eight days. The change to the baselines was authorized, tested, and scheduled to occur. Additionally, the update to the software strengthened the security posture for the Cyber Assets of issue. No harm is known to have occurred.</p> <p>MRO considered the Entity's compliance history and determined there were no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the anti-virus management console to disable the automatic updates of virus definitions and agent software; 2) added a notification step to its anti-virus process for which the Subject Matter Experts (SME) will email staff responsible for impacted Cyber Assets including dates and times of the change; and 3) implemented a new process specific to managing software updates to the anti-virus management console. The process includes documented steps for checking the desired configurations for automatic updates, including visual aids; and 4) updated its baseline management tool to perform daily scans of baselines and report on deviations to the baselines to desired SMEs. This will assist in identifying deviations from the baseline within 24 hours. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021363	CIP-004-6	R3	[REDACTED] (the Entity)	[REDACTED]	01/07/2019	01/17/2019	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 4, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R3. The Entity reported that during preparation for annual cybersecurity training, it was discovered that the enrollment list was compiled by running an offline version of the quarterly CIP-004-R4 report. This report showed twenty-two discrepancies in Personal Risk Assessment (PRA) dates for contractors.</p> <p>The cause of the noncompliance was that Entity failed to follow its CIP-004-6 process to verify the PRAs were completed prior to completing and closing out its workflow.</p> <p>This noncompliance began on January 7, 2019, when the Entity completed its process to grant security cards for unescorted access in its identity management system, and ended on January 17, 2019, when the Entity disabled the cardholder records in its PACS systems.</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 access cards that had been requested for the 22 contractors were being prepared for future work at a construction site and had never been issued, limiting this issue to a documentation irregularity. Additionally, the 22 contractors of issue had not been onsite during the duration of this issue. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) disabled the impacted cardholder records in the PACS; and 2) addressed the issue with the individual responsible for closing the request prior to PRAs being complete. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021428	CIP-007-6	R5	<div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> (the Entity)	<div style="background-color: black; width: 100%; height: 15px;"></div>	08/01/2016	05/02/2018	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 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5.</p> <p>The Entity reported that while performing an extent-of-condition analysis for a prior instance of noncompliance [REDACTED] for this standard and requirement, it discovered that one interactive shared account password on [REDACTED] Physical Access Control System (PACS) server(s) associated with a high impact BES Cyber System (BCS) had not been changed within 15 calendar months as required by the standard. The previous last password change occurred under CIPv3. Under v3, the “annual” term was ambiguous and could be interpreted within one year, or at least once during each calendar year. The Entity reported their interpretation was per calendar year, which would have given them until December 31, 2016 to update the password; however, with CIPv5 becoming enforceable on July 1, 2016, the window was shortened to 15 calendar months from the previous password change date, resulting in a due date of July 31, 2016.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for handling shared account passwords.</p> <p>The issue began on August 1, 2016, which was the day after the 15 calendar month window to change the password since the previous password change on April 25, 2015, and ended on May 2, 2018, when the password was 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. The issue was limited to a single shared account on [REDACTED] PACS server(s). The shared account of issue was known only to one individual, who had a current Personnel Risk Assessment, had CIP training, and is trusted with other administrative privileges; thus, limited the potential exposure of the password and reduced the potential for misuse. The PACS servers were protected by multiple firewalls and an intrusion detection system, which goes beyond the requirements applicable to a PACS, which further reduced risk. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) changed the password on the PACS server applications; 2) held directed training with the individual who had access to this shared account; 3) created and conducted training with its technical staff regarding its approach to managing shared account passwords; and 4) added the password into its password management vault for improved tracking and reporting. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021429	CIP-007-6	R2	██████████ (the Entity)	██████████	08/16/2018	09/20/2018	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 10, 2019, the Entity submitted a Self-Log stating that, as a ██████████, it was in noncompliance with CIP-007-6 R2. The Entity reported that during a quality review of its patch process it failed to evaluate ██████████ patches within 35 calendar days of the previous evaluation as required by the standard.</p> <p>The cause of the noncompliance was that the Entity's process for ensuring patch evaluations occurs at least every 35 days was insufficient. The noncompliance began on August 16, 2018, which was 36 days after the previous evaluation, and ended on September 20, 2018, when the patches were evaluated.</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. This was limited to ██████████ patches and was discovered through secondary controls, which limited the duration to 36 days. Additionally, the maximum duration from patch release to installation among the ██████████ patches was 95 days, which was only 25 days longer than the maximum duration of 70 days allowed by the standard (maximum 35 days from release to evaluation plus 35 days from evaluation to implementation). No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) evaluated the ██████████ patches; 2) modified its patching process to align its patch discovery window with its evaluation window; and 3) tied its patch evaluation to a fixed number of days after monthly patches are released by vendor to ensure that it occurs within 35 calendar days each cycle. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021430	CIP-004-6	R4	██████████ (the Entity)	██████████	01/07/2019	02/08/2019	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 10, 2019, the Entity submitted a Self-Log stating that, as a ██████████, it was in noncompliance with CIP-004-6 R4.</p> <p>The Entity reported that while reviewing an access management system report, it discovered that ██████ individual(s) were granted physical access to PSPs containing medium and high impact BES Cyber Systems (BCS) without being authorized. The implementation of a change to its identity management system unintentionally led to re-enabling access to individuals whose access had previously been terminated.</p> <p>The cause of the noncompliance was that the Entity failed to account for the impact of potential changes to its identity management system on previously terminated access, which resulted in a failed implementation of its physical access authorization process.</p> <p>The noncompliance began on January 7, 2019, when the individual(s) were granted access, and ended on February 8, 2019, when the Entity revoked the 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 Entity reported that the issue was identified through a periodic internal control, which limited the duration, and the issue was limited to ██████ individual(s). Each of the individual(s) was previously authorized for access, previously had training, and previously had personnel risk assessments. Additionally, the individual(s) to whom access was granted were not notified of the access, which reduced the likelihood of misuse. Lastly, none of the individual(s) to whom access was granted utilized their access during the duration of the issue. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked the erroneous access; and 2) coached access management staff by notifying them of the issue and instructing them to not perform changes without considering the impact to the expiration date for 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
MRO2018020525	CIP-005-5	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	12/03/2018	Compliance 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 violation.)			<p>During a Compliance Audit conducted from [REDACTED], the Audit Team determined that the Entity, as a [REDACTED], was in noncompliance with CIP-005-5 R1. The Audit Team determined that the Entity failed to provide reasoning for granting access for all inbound and outbound access permissions and found at least three examples where justifications were not provided.</p> <p>After performing an extent-of-condition analysis on the firewall configurations provided during the audit, MRO determined that for the primary Control Center redundant firewalls, 4 out of the 67 access rules either had no justification in the "Comments" field or the justification was a note about when or who edited the rule and not a reason for the rule. In each of these instances, the Entity referenced the rule name as its justification, which provided some degree of explanation for the ports; however, the names did not sufficiently justify the need for the ports. MRO also found, specifically for the backup Control Center non-redundant firewalls, that all access rules were found with justifications.</p> <p>The cause of this noncompliance was that the Entity inconsistently followed its process for documenting the justification of need for ports, which led to instances of insufficient justifications.</p> <p>This noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on December 3, 2018, when the Entity enhanced its justification for the ports.</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 limited to four out of 119 rules (67 on the primary firewall pair, 52 on the backup standalone firewall). Additionally, the four impacted rules were for traffic leaving the Electronic Security Perimeter (ESP); all destinations were restricted to known individual IPs/hosts, which limited the potential exposure of the unjustified traffic. Lastly, the noncompliance was resolved by improving the justification for the ports, rather than by making any changes to the firewall rules. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) enhanced its firewall rule justifications to include a more detailed justification of need in the "Comments" field; and 2) changed its process for documenting justification to use these enhanced firewall justifications for all rules in the "Comments" field. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020526	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	06/08/2017	Compliance 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 violation.)			<p>During a Compliance Audit conducted from [REDACTED], the Audit Team determined that the Entity, as a [REDACTED] was in noncompliance with CIP-010-2 R1. The Audit Team determined that the Entity failed to include the version number of one application on a sampled asset as required by the standard. When reviewing the provided evidence, it was determined that this version number was missed on many, if not all, Windows devices included in the provided baselines.</p> <p>The cause of this noncompliance was that the Entity's process lacked sufficient detail to ensure that all version numbers were captured in its baselines.</p> <p>This noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on June 8, 2017, when the Entity added the application to its baseline.</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 issue was limited to one application, was documentation-in-nature, and was resolved through steps to add the version to its baseline documentation, rather than by removing the application of issue from the Cyber Assets. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) manually added the missing application to the Windows registry, such that it could be added to the baseline through its automated tool; 2) reviewed each Cyber Asset with the application of issue installed to ensure the version number was captured in the baseline; 3) updated its process to include updating the Windows registry to include the updated version of the application whenever the application is updated; and 4) configured its baseline automation tool to track the installation date of the application, such that an update of the application would be identified automatically. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2017018868	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	01/21/2017	04/20/2018	Compliance 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 violation.)			<p>During a Compliance Audit conducted from [REDACTED], MRO determined that the Entity, as a [REDACTED] was in noncompliance with CIP-007-6 R2.</p> <p>For each of [REDACTED] PCA devices, one patch that had been evaluated as applicable was not applied to the device within the 35 days required by CIP-007-6 Part 2.3. For device [REDACTED], a patch assessed as applicable on [REDACTED] was not installed on the device until [REDACTED] which was 67 days beyond the installation date required by CIP-007-6 R2. For device [REDACTED], a patch assessed as applicable on [REDACTED], was not verified to have been installed until [REDACTED].</p> <p>The cause of the noncompliance was that the Entity’s documented process for tracking updates/patches, evaluation due dates, and deployment due dates was not sufficiently rigorous to ensure that patch installation would occur in a timely manner.</p> <p>The noncompliance began on January 21, 2017, which was 35 days after patches were assessed, and ended on April 20, 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. The PCA device(s) of issue was/were not accessible via External Routable Connectivity thereby limiting the attack vectors to the device. No harm is known to have occurred.</p> <p>MRO 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) conducted an extent of condition review [REDACTED] using [REDACTED] for security updates; 2) installed the applicable “missing” patches on affected devices; 3) created training documentation and reviewed the relevant CIP standard with EMS personnel to ensure they understand the criticality of change control; and 4) created a methodical approach to tracking updates where a patch/data update will be updated during a biweekly meeting. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021977	CIP-004-6	R4	[REDACTED] (the Entity)	[REDACTED]	05/13/2019	05/21/2019	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 July 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4.</p> <p>The Entity reported that while performing work on a ticket to verify access between a CIP role and the mirrored enterprise role, it was discovered that one intern had been granted CIP access that had not been authorized as per CIP-004-6 requirement R4, Part 4.1.3.</p> <p>The cause of this noncompliance was that the Entity's information center inaccurately understood CIP security group security permissions; as a result, the Entity failed to follow its process for providing access to the intern.</p> <p>This noncompliance began on May 13, 2019, when an intern was granted unauthorized access to BES Cyber System Information (BCSI), and ended on May 21, 2019 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. The intern had unauthorized BCSI access to a CIP working directory used for in-process updates to policies, asset lists, and training documents and the secured CIP directory which contains copies of the currently effective CIP policies and plans; neither location provides any authentication information to BES Cyber Systems. Additionally, the issue was limited to nine days. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked the unauthorized CIP access on the date of discovery; and 2) created a new active directory group, moved all the CIP-related security groups into this new group, and removed permissions to add/remove members of this group from all other user groups except for the Systems Specialist team. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021418	CIP-004-6	R5	[REDACTED] (the Entity)	[REDACTED]	12/01/2018	12/03/2018	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 January 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5.</p> <p>The Entity reported that a contract employee was no longer employed by the contractor, but the contractor did not notify the Entity for four days, when another contract employee mentioned it. The Entity revoked the contract employee's physical access (disabled the access badge) on the date they were notified by the contractor. The badge granted access to the Entity's primary Control Center (medium impact), which contained PACS, PCAs, BCAs, and EACMS.</p> <p>The cause of the noncompliance was that the Entity failed to adequately ensure that its contractor followed its process for notifying the entity upon termination of contract employees.</p> <p>The issue began on December 1, 2018, which was 24 hours after the contract employee was terminated, and ended on December 3, 2018, when the access badge 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. This noncompliance was limited to one contract employee for three days. The contractor retained the contract employee's access badge in a locked office upon termination of the contract employee. Although this office was accessible to four employees of the contractor who did not have authorized access to the associated PSP, the Entity had additional controls in place which would have further restricted use of the card. These additional controls were:</p> <ul style="list-style-type: none"> • access to the Control Center would have required knowledge of the terminated contractor's personal PIN in addition to the card; • the Control Center is staffed 24x7 and had internal and external video surveillance for situational awareness, which would have limited the ability for the card to be misused without being noticed; and • the contract employee was not terminated for cause, initiated the termination on their own, provided two weeks' notice, and worked through those two weeks which demonstrates that the contract employee did not pose an elevated risk beyond the risk posed while still employed. <p>Additionally, the Entity reviewed the logs and determined that the badge was not used to attempt access after the date of termination. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) disabled the access badge, which revoked the contract employee's physical access; 2) reviewed access of other similar contract employees and confirmed that all were still employed by the contractor; and 3) provided training to its employees responsible for knowing when access for these contract employees should be removed, which included the access requirements and notification for changes to staff or responsibilities. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020736	CIP-004-6	R4	[REDACTED] (the Entity)	[REDACTED]	07/23/2018	08/13/2018	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 violation.)			<p>On November 5, 2018, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-004-6 R4. [REDACTED]</p> <p>The Entity reported that an existing employee, with a new role assignment, was given access without authorization, to an electronic designated storage location containing BES Cyber System Information (BCSI). There were two instances where access was granted without authorization, by two different SharePoint developers. In both instances, the unauthorized access was revoked within five days.</p> <p>The cause of the noncompliance was that the SharePoint developers misunderstood that an electronic designated team storage location retained BCSI, following a migration of the site data to another electronic designated team storage location. The nature of the migration was not fully communicated to the developers, who understood the migration to be a move rather than a copy of BCSI. Additionally, the access management program and processes were not reinforced sufficiently with employees, changes to designated storage locations were not adequately communicated, and the team's SharePoint site (the original designated storage location) lacked sufficient identification of BCSI on the SharePoint home page.</p> <p>The issue began on July 23, 2018, when the first access was granted without authorization, and ended on August 13, 2018, when the second 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. Both instances of unauthorized access were self-detected, were limited to a duration of five days, and were limited to one employee. The employee had cyber security training, was intended to be given access to designated storage locations, the employee's Personal Risk Assessment was valid and re-verified, and the employee did not access any BCSI. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked access; 2) removed SharePoint developers' ability to grant access to designated storage locations and access grant responsibility was assigned to an information technology role; 3) reinforced migration date and the nature of the migration of the designated storage location with larger number of employees in addition to developers; 4) provided training on BCSI to the SharePoint developer team; 5) updated internal SharePoint site to more clearly identify the site as containing BCSI; and 6) expunged BCSI from internal team site where issued occurred. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021825	CIP-004-6	R4.	[REDACTED]	[REDACTED]	12/12/2016	7/2/2019	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 July 16, 2019, [REDACTED] (the Entity) submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-004-6 R4. (4.1). The entity failed to follow its procedure in authorizing information access to one of its BES Cyber System Information (CSI) storage locations. The BES CSI storage location at issue is the entity's [REDACTED] which contains documents in electronic format.</p> <p>Four employees and two contractors were granted administrative access to the [REDACTED] based on business needs. This access was granted at different times to the six individuals beginning on December 12, 2016. Access was granted by the [REDACTED] group. However, the [REDACTED] who is the Entity's appropriate approver of access to [REDACTED], was not made aware until after the access was granted. As a result, the entity did not follow its procedure in authorizing information access to one of its BES CSI storage locations. The six individuals in question were not properly informed of best practices regarding the specific handling and protection of BES CSI. Two of the employees had [REDACTED] responsibilities and two employees had [REDACTED] responsibilities. The two contractors employed by [REDACTED] were charged with overall [REDACTED] maintenance. An internally conducted forensic investigation concluded that only a single file containing BES CSI was accessed by one of the [REDACTED] employees while verifying the file's retention settings.</p> <p>Furthermore, the issue led to inaccuracies of less than 5% of the entity's CIP-004 Access List, since the six individuals in question were not added to the list, as individuals with information access, until their request for access was processed and properly authorized.</p> <p>This noncompliance started on December 12, 2016, when the Entity first granted access without following its procedure. The noncompliance ended on July 2, 2019, when the Entity resolved the access for the six individuals and modified its approval process for the [REDACTED] to include the [REDACTED].</p> <p>The root cause of the issue was management's failure to include the BES CSI access approver in the decision-making process of authorizing and granting [REDACTED] administrative access and less than adequate controls to verify access permissions of [REDACTED].</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 its process to authorize access to BES CSI, there is an increased risk of BES CSI being used or shared by unauthorized personnel to gain access to the entity's BES Cyber Systems.</p> <p>At no time did the individuals in question have cyber or unescorted physical access to the entity's BES Cyber Systems. The BES Cyber Systems are physically protected from unauthorized access [REDACTED]. Furthermore, all BES Cyber Systems are protected in accordance with the applicable CIP-005-5, CIP-007-6 and CIP-010-2 Requirements.</p> <p>The risk of the individuals sharing or using BES CSI was reduced given the confidential nature of information handling that their roles and responsibilities require. The employees and contractors are already authorized for access to corporate systems based on business need and have access to other sensitive and confidential entity data within the entity's [REDACTED].</p> <p>A forensic investigation concluded that only one of the files containing BES CSI were accessed. That file was accessed by one of the [REDACTED] employees while verifying the file's retention settings as part of a company-wide retention settings change.</p> <p>Employees receive quarterly cyber security awareness training in accordance with CIP-004-6 R1 and contractors have existing confidentiality agreements in place with the entity. Finally, entity personnel have been trained on incident handling and, if a cyber security incident were to occur, personnel would follow the entity's CIP-008-5 Cyber Security Incident Response Plan.</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) requested immediate access and approval that was granted by the [REDACTED] for one of the [REDACTED] employees following the proper procedure;2) revoked access for two of the employees and the two contractors and did not reinstate access until requests were submitted and approved based on need, best practices emails were sent, and follow-up training completed;3) the fourth employee's access was revoked prior to the discovery of the issue;4) updated the CIP-004 R4 Access List;5) reviewed the issue with [REDACTED] and [REDACTED] to reinforce the procedural steps that need to be taken prior to authorizing and granting information access to BES CSI Storage location;6) modified the approval process (ticketing system) for elevated privileges for the [REDACTED] system to include approval by the [REDACTED]; and7) added a check to quarterly and annual access review process to include request for permission export from [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
NPCC2017017392	CIP-006-6	R1.	[REDACTED]	[REDACTED]	12/08/2016	12/08/2016	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 violation.)			<p>On April 11, 2017, [REDACTED] (the Entity) submitted a Self-Report stating that as a [REDACTED] it had discovered it was in noncompliance with CIP-006-6 R1. (1.2.).</p> <p>On December 8, 2016, approximately after 12:30 P.M., the entity was notified via a PACS alarm that there was an unsecured door to a PSP at the [REDACTED] within a corporate office building. The unsecured door occurred when an employee working in the PSP left the PSP through the third door and an alarm was generated because that door would not remain latched. This unsecured door allowed access to a Medium Impact BES Cyber system [REDACTED] at the access control device. The lead security officer was deployed to look at the door causing the alarms and confirmed that the door would not stay closed. The lead security officer then returned to the [REDACTED] with two authorized employees alone in the PSP. The two employees soon finished their work and left. There was no human observation of the unsecured door. The [REDACTED] then deployed the Lead Technician to see if the door issue had been addressed. The Lead Technician arrived 15 minutes after the two employees vacated the PSP. The Lead Technician informed the [REDACTED] that he could not fix the door. The Lead Technician then left the PSP area at 1:32 P.M., leaving the door unsecured for an additional 65 minutes.</p> <p>At 2:36 P.M., two more employees arrived at the door and the programming issue was corrected soon thereafter. The door was programmed incorrectly in December 2014, prior to commissioning and the cage was still empty. The PSP to which this door provided access was not brought into scope until CIP-006-6 V5, beginning July 1, 2016. Finally, the Entity's [REDACTED] determined that the door was not unlocked manually by anyone who had the ability to do so. On the day of December 8, 2016, the door was unsecured and unobserved for approximately 80 minutes.</p> <p>The noncompliance began on December 8, 2016, the date the door was opened without the capacity for lockout. The noncompliance ended later on December 8, 2016, when the Entity fixed the programming issue.</p> <p>The root cause of this noncompliance was that the Entity's staff overlooked programming of the door which resulted in the error in programming; as well as numerous procedural and training deficiencies which resulted in the Entities failure to observe the door continuously while it was not secured. This noncompliance involves the management practices of workforce management and validation. Workforce management is implicated because the Lead Technician were not properly trained to remain at the unsecured door until it was either fixed or another authorized individual arrived to observe the door. Validation management is involved because the door was improperly programmed and validation of the program would have uncovered the programming issues.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk to the reliability of the bulk power system. The risk posed by this noncompliance is the opportunity for unauthorized physical access to Cyber Assets or Cyber System(s) which could result in harm to the integrity of the BES Cyber Systems or the reliability of the BES as a consequence of intentional compromise or misuse. The risk is minimized because the PSP was within a limited-access controlled area within an access controlled facility. Further minimizing the risk, while the PSP itself was unmanned, the PSP is within a controlled access facility which [REDACTED] Finally, the duration of the noncompliance, approximately 80 minutes, limits the risk. Thus, the risk posed to the Bulk-Power System was minimal.</p> <p>No harm is known to have occurred.</p> <p>NPCC 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) Corrected the programming issue on the PSP door 2) Reviewed and revised the corporate CIP-006 procedure 3) Communicated the CIP-006 procedure updates 4) Conducted training on the revised CIP-006 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
NPCC2017018219	CIP-004-6	R4.	[REDACTED]	[REDACTED]	01/05/2017	08/31/2017	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 August 22, 2017, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it had discovered on March 31, 2017 it was in noncompliance with CIP-004-6 R4. (4.1., 4.3.). On December 26, 2017, the entity submitted an expansion of scope, reporting another instance of noncompliance with CIP-004-6 R4, P4.1. (Instance 2 below)</p> <p>Instance 1:</p> <p>The first instance of noncompliance started on January 5, 2017 when the entity permitted eight unauthorized individuals access to eleven (11) Electronic Access Control and/or Monitoring System Cyber Assets within the firewall cage, and permitted eighteen (18) unauthorized individuals access to seventeen (17) Physical Access Control System (PACS) Cyber Assets within the access control cage without required authorization. The noncompliance ended on April 13, 2017 when the entity completed a re authorization process for all individuals needing access to the modified PSP.</p> <p>Specifically, the entity executed a planned change and modified three distinct and physically separated areas, two of which were PSPs, by removing interior chain-link fencing from between each of them, creating one large cage PSP without interior barriers. Originally, each PSP had its own access control door, which used two-factor authentication to permit authorized access into the individual PSP cage. One cage contained firewalls used to control access to High Impact Bulk Electric System Cyber Systems (BCSs), the second cage contained access control equipment used to manage physical access into facilities containing Medium and High Impact BCSs, and the third contained demilitarized zone (DMZ) equipment. After removing the interior chain-link fencing, the now singular PSP retained the two PSP access doors, but removed the DMZ cage door. This change permitted individuals who only had specific access permissions to one of the three separate areas to have physical access upon entry to Cyber Assets that the entity had not authorized them for.</p> <p>The entity concluded the root-cause of this violation was a lack of training and controls. An individual misunderstood access permissions and the role the individual PSPs' access controls played in permitting access when the entity removed the interior cage walls.</p> <p>Instance 2:</p> <p>The second instance of noncompliance started August 30, 2017, when the entity granted a new database administrator (DBA) contractor electronic access to CIP data the individual had not been authorized for. On August 31, 2017, the same day as discovery, the entity removed the DBA's unauthorized access.</p> <p>Specifically, the entity erroneously granted the DBA electronic access to a PACS database, which supported facilities containing High and Medium Impact BCSs. This error occurred when the security analyst completing the work order inadvertently selected the wrong Active Directory (AD) group due to similar naming conventions used for the AD groups. The next day, on August 31, 2017, the entity discovered this instance as a result of an internal control, where the entity reviews exceptions looking for possible improper access provisioning on a daily basis.</p> <p>During its extent-of-condition assessment, the entity discovered no additional instances of access provisioning problems.</p> <p>The entity determined that the root-cause of this violation was a manual process that lacked detailed instructions and was co-mingled with non-CIP access requests.</p>					
Risk Assessment			<p>This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The entity's failure to properly control access provisions could have permitted unauthorized individuals to access and possibly modify settings, either from unintentional or malicious actions, and cause operational impacts. However, everyone involved in both instances had received cyber security training and had a valid Personnel Risk Assessment on file. For Instance 1, the duration of the unauthorized access was limited to 13 weeks and access was restricted to the same personnel that were originally using the card readers. The individuals did not gain any unauthorized electronic access to the assets. In addition, the entity had located this cage within a secured building with access controls and roving security staff patrols. For Instance 2, the unauthorized access lasted for less than one day and was limited to only one DBA. The DBA was unaware of the unauthorized access. The entity reviewed the DBA's activity and found the DBA did not access the PACS database during the time unauthorized access was granted. Further, the entity discovered the second instance the next day by performing a manual internal control.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					

	NPCC considered the Entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	<p>To mitigate this noncompliance, the entity:</p> <p>For Instance 1:</p> <ol style="list-style-type: none"> 1) Sent communication to all Area Owners, to inform them of the Corporate Security Change Control Process 2) Created new PSP in access control system and obtain authorizations 3) Completed PSP Inspection 4) Created a Configuration Item (CI) for changes to a PSP 5) Created a DSA Job aid which will direct individuals to use the Configuration Item developed in Step 4 and post in the data center PSPs. 6) Trained impacted personnel on the DSA Job Aid developed in Step 5. <p>For Instance 2:</p> <ol style="list-style-type: none"> 1) Removed unauthorized access from DBA's account. 2) Added enhancement to the workflow tool to initiate a pop-up alert when completing a NERC request. To continue with the process, the security analyst requests a peer review and the peer reviewer notes their review in IT Risk Management. 3) Instituted a process improvement to prevent vaulting user accounts in cyber asset until [REDACTED] notifies [REDACTED] that the "Compliance Process is complete."

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018220	CIP-007-6	R2.	[REDACTED]	[REDACTED]	01/17/2017	01/19/2017	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 August 22, 2017, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it had an issue of CIP-007-6 R2.</p> <p>The noncompliance began on January 17, 2017, the date the Entity was required to comply with CIP-007-6 R2. The noncompliance ended January 19, 2017, when the Entity evaluated the patches for applicability.</p> <p>On January 19, 2017, the Entity discovered that three security patches were evaluated for installation 37 calendar days after being released from their monitored source, exceeding the patch deadline in CIP-007-6 R2 by two days. The patches which were not assessed in time included three patches for eight Active Directory Domain Controller servers classified as EACMS supporting eight BES Cyber Systems. The Entity's personnel overlooked the assessment during a period of heavy workload.</p> <p>The root cause of this noncompliance was inadequate internal workforce controls. High workloads and planned absences were managed ineffectively resulting in the entity being unable to complete the patch evaluation in time. This noncompliance involves the management practice of workforce management. Workforce management is implicated because the employees were overburdened with work as a result of poor management practices which included granting planned absences during elevated workflow periods, thereby causing human performance errors.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk to the reliability of the bulk power system. The failure to evaluate patches in a timely manner can expose BES Cyber Systems to cyber security vulnerabilities such as the introduction of malicious code or infiltration of a bad actor into BES Cyber Systems. The risk is minimized because the delay only impacted the assessment and the patches themselves were installed in a timely manner in accordance with CIP-007-6-R2.3. Specifically, CIP-007-6 R2 provides 35 days for patch assessment and an additional 35 days for implementation for a total of 70 days; here it took only 44 days to complete both steps. Further minimizing the risk, the BES Cyber Assets impacted, resided within a PSP where the assets received all applicable logical and physical controls. Finally, this noncompliance only impacted three security patches specific to EACMS. Thus, the risk posed to the Bulk-Power System was minimal.</p> <p>No harm is known to have occurred.</p> <p>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate the noncompliance, the entity:</p> <ol style="list-style-type: none"> 1. Evaluated missed security patches for applicability; 2. Added CIP-007-6 R2.2 task to the Executive Dashboard; 3. Addressed Human Performance; 4. Implemented additional controls around [REDACTED] patching to ensure patches are assessed and implemented; and 5. Performed training to support Step 4. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019761	CIP-007-6	R5.	[REDACTED]	[REDACTED]	07/01/2016	07/09/2018	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 violation.)		<p>On May 24, 2018, [REDACTED] (the Entity) submitted a Self-Report stating that as a [REDACTED] it had discovered on February 19, 2018 it was in noncompliance with CIP-007-6 R5. (5.7.) after a system administrator discovered that the default lockout policy configured on the system did not apply to two types of inventoried administrative accounts.</p> <p>The noncompliance began on July 1, 2016, the date the Entity was required to comply with CIP-007-6 R5. The noncompliance ended on July 9, 2018, the date the Entity completed Mitigating Activities. Risk ended upon [REDACTED] approval of TFE.</p> <p>Specifically, two [REDACTED] accounts and a [REDACTED] account were impacted. There was no existing Technical Feasibility Exception (TFE) in place to comply with CIP-007 R5.7. One [REDACTED] account was deleted when the noncompliance was discovered; the other [REDACTED] account is used to login to the console and the [REDACTED] account is used to login to the [REDACTED]. The default lockout policy did not apply to the remaining [REDACTED] and [REDACTED] accounts because the system manages other accounts in a separate internal database. Therefore, the [REDACTED] and [REDACTED] accounts should be covered by a TFE, but were not at the time of the noncompliance.</p> <p>The root cause of this noncompliance was the Entity's insufficient controls around a process change from Version 3 to Version 5 standards resulting in a failure to identify and request a TFE on these accounts. This noncompliance involves the management practices of workforce management and verification. Workforce management is implicated because the new account administrator was not aware of relevant requirements as a result of an insufficient transition of responsibilities caused by a change in standards. Verification management is involved because the Entity failed to inventory and request a TFE for two types of administrative accounts.</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 the ability for a bad actor to gain access to Cyber Assets. The risk is minimized in this instance because of the following three compensating measures which were in place prior to July 1, 2016:</p> <ol style="list-style-type: none"> 1) the Entity performed log reviews each week for anomalies including review of operations console authentication activity; 2) the Entity utilized password complexity requirements which exceed the NERC password complexity requirements; and 3) a number of the tasks that could be performed with the [REDACTED] credentials also required an additional administrator account and password, this additional account including lockout procedures after a maximum number of failed access attempts. <p>No harm is known to have occurred.</p> <p>NPCC 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. Added a control so that the [REDACTED] can only be accessed through the jump host; 2. Filed a TFE with the [REDACTED] Region for the affected devices; 3. Update commissioning checklist to include a review of "all types of accounts" and test any vendor statement impacting compliance requirements; and 4. Train individuals on the modifications made to the commissioning checklist above. 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019022086	CIP-004-6	R5.	[REDACTED]	[REDACTED]	07/31/2019	08/04/2019	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 August 20, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it was in noncompliance with CIP-004-6 R5. (5.4).</p> <p>The entity discovered that it failed to revoke access to a High Impact BES Cyber System for a terminated employee while revoking access for a different individual. Specifically, the entity terminated an employee on June 30, 2019. The entity failed to revoke access to a non-shared user account within 30 days of a termination action.</p> <p>This noncompliance started on July 31, 2019 when the entity failed to revoke access for one employee within 30 days of a termination action. The noncompliance ended on August 4, 2019, when the entity revoked the access.</p> <p>The root cause of this noncompliance was that the process to remove all non-shared user accounts was not well defined. A contributing cause was the lack of a checklist to be used as guidance during revocations that requires a review of the Electronic Access Control systems that grant access to BES Cyber Assets and their associated PCAs, EACMS, and PACS.</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 revoking access within 30 days of a termination action, the entity could potentially allow unauthorized individuals to access High Impact BES Cyber Systems. However, the access was read-only and did not have privileges to make changes or control the Bulk Electric System.</p> <p>Additionally, in order to access the account, an individual would require physical access or Interactive Remote Access, both of which were removed within 24 hours of the termination action. [REDACTED]. Any compromise of the PSP would trigger an alert and result in an investigation. Finally, all administrative access to any asset in the Electronic Security Perimeter (ESP) was removed as part of the revocation process.</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 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 the access rights of the individual as part of the incident analysis; 2) deleted the individual's non-shared user account; 3) updated the access revocation program document to include Electronic Access Control Systems used to grant access to BES Cyber Assets and their associated PCAs, EACMs, and PACs; and 4) shared the updated version of the access revocation program document with support 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
RFC2018020558	CIP-004-6	R5	[REDACTED]	[REDACTED]	5/5/2018	5/7/2018	Self-Report	November 15, 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 11, 2018, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5.</p> <p>The entity discovered that one individual's physical access was not removed within 24 hours of termination as required by CIP-004-6 R5.1. The individual at issue was an entity retiree who returned as a contractor [REDACTED]. The individual's last day as a contractor was on Friday, May 4, 2018, but the entity did not remove the individual's physical access until Monday, May 7, 2018. The entity confirmed that the individual did not have interactive remote access.</p> <p>The entity's physical access removal process for contractors requires contractor management to inform the entity's [REDACTED] on the contractor's last day so the contractor's access can be removed. [REDACTED] internal process requires the contractor's immediate supervisor to inform the [REDACTED] Manager of the contractor's departure so the [REDACTED] Manager can contact the [REDACTED]</p> <p>The entity conducted an investigation of this noncompliance and found that the contractor's immediate supervisor did properly inform the [REDACTED] Manager of the contractor's last day. On that day, however, the [REDACTED] Manager was in an off-site training and forgot to contact the [REDACTED] to get the individual's physical access removed. The entity properly collected the individual's laptop at the end of the day on May 4, 2018, but forgot to collect the individual's physical security badge on May 4, 2018.</p> <p>The root cause of this noncompliance was that the [REDACTED] Manager did not follow the documented process to revoke the contractor's access within 24 hours of termination.</p> <p>This noncompliance involves the management practices of workforce management and verification. Workforce management through ineffective training is involved because the [REDACTED] Manager was not effectively trained on the need to revoke the individual's physical access (his physical security badge) within 24 hours of the individual's termination.</p> <p>This noncompliance started on May 5, 2018, when the individual's physical access should have been removed and ended on May 7, 2018, when the entity removed the individual's physical 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 (BPS) based on the following factors. The potential risk posed by this noncompliance is that an individual who is no longer permitted to have access will use that access in a manner that will compromise the BPS. The risk is minimized because physical access was removed less than 72 hours after the individual's access was no longer needed. The individual was a retiree of the entity, in good standing with the entity, had a valid Personnel Risk Assessment, and was up to date on his NERC CIP trainings. Additionally, the entity verified that the individual did not attempt to use his physical access during 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 does not warrant an alternative disposition method because most of the prior noncompliances are distinguishable as they involved different circumstances or root causes. For the one issue that is arguably similar, ReliabilityFirst determined that the current noncompliance continues to qualify for compliance exception treatment as it posed only minimal risk, involves high frequency conduct (access revocation), and is not indicative of a systemic or programmatic issue. Further, the entity quickly identified the noncompliance and corrected the issues through its internal controls.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the contractor's physical access on May 7, 2018 upon the Terminating Manager's return to the office; 2) performed an extent of condition and evaluated all [REDACTED] terminations from January 1, 2018 through June 30, 2019 and identified, from that list, all individuals who had either physical or logical access and confirmed that the date each of their accesses were removed aligns with the requirements of the entity's [REDACTED]; 3) enhanced existing documentation for the manager's termination steps to highlight that two steps are needed to fully complete a termination action. In addition to the revised document, the storage location for the Manager's checklist will be made more accessible on the entity's internal webpage. <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by November 15, 2019:</p> <ol style="list-style-type: none"> 4) will establish a biannual detective control in its Compliance Management system. Every 6 months a statistically significant sample set of terminations requiring access revocations will be reviewed to verify access was revoked properly; and 5) will establish a biennial assurance control in the Compliance Management system. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021232	CIP-010-2	R1	[REDACTED]	[REDACTED]	9/30/2018	10/3/2018	Self-Report	5/10/2020
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, 2019, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-010-2 R1.</p> <p>On October 2, 2018, as a result of reviewing baseline exceptions, the entity discovered that one of the [REDACTED] servers received August 2018 patches, but the baseline change did not get promoted within 30 calendar days of completing the change. (The entity verifies applied patches by comparing the number of patches applied to the device against the number of deviations in the baseline tool. The entity noticed this server had patches from August 30, 2018 when reviewing the number of patches applied for the next patch cycle on October 3, 2018. The August 30-day baseline promotion window was from August 30, 2018 to September 29, 2018.)</p> <p>The August patches were implemented on all 24 assets. When the deviations from the August patching change was detected by [REDACTED], it created a line item exception. On 23 of the 24 assets, the entity updated the baselines on September 14, 2018, which was within the 30 day time frame. However, for the other asset, between the August and September 2018 [REDACTED] patching change requests, the entity promoted a separate change request which re-wrote the deviation detection date in the entity's baselining tool. This resulted in the asset's [REDACTED] patch exception not being promoted to the baseline until after the review of September's patching change request on October 2, 2018, which resulted in the baseline being updated a day late.</p> <p>This noncompliance involves the management practices of asset and configuration management, work management, and verification. The root cause of this noncompliance was that within the baseline application, when a new baseline promotion occurs, the first exception detection date is overwritten with the new promoted baseline date.</p> <p>This noncompliance started on September 30, 2018, when the entity was required to promote the baseline changes within 30 days of the last change and ended on October 3, 2018, when the entity analyst collected all evidence supporting the incident and promoted the change to the baselines.</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 a failure to update the baselines is providing an opportunity for unauthorized and undetected modifications to be made to applicable Cyber Assets which could introduce undetected malicious code or adversely affect system configurations and communications of such assets, or allowing the entity to rely on incorrect information when performing subsequent tasks. [REDACTED]</p> <p>[REDACTED] The risk is minimized because only one server was impacted with a short duration of less than a week. The devices were timely tested and patched, but the change detected on one device out of 24 was not promoted in the baseline tool, thereby missing the 30 day baseline promotion process. Although the changes were not properly promoted to the baseline, the changes were implemented both in the testing environment and the production environment. The risk is also lessened because the server at issue is part of a pair and the other server in the pair was promoted in the baselining tool. (These devices have identical pairs with redundant keep alive mechanisms for primary and stand by failover capability.) 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) applied a patch to the baseline tool to repair the overwrite of exception detection dates when multiple baselines are approved to a new baseline. The entity upgraded the baseline tool, [REDACTED] the exception date when a baseline exception first occurs is now maintained even if the exception is ignored or not accepted; 2) approved the changes discovered to the new baseline in the baseline tool; 3) added warning notification triggers to the promote baseline task in the change management system to increase visibility around the 30-day baseline promotion task. Email notification warnings are sent to the group manager, assigned group, and individual when the baseline promotion task reaches specified time frames. At 15 days, a warning message is emailed to the assigned individual to notify them that 50% of the 30 day time period has lapsed. At 22 days, a warning message is emailed to the group manager and assignment group to notify them that 75% of the 30 day time period has lapsed; 4) performed an extent of condition review for [REDACTED] servers for the period August 30, 2018 to December 2, 2018. The entity will examine baselines that were incomplete or not updated within 30 days of a change and will report these to ReliabilityFirst. The review encompasses changes made to existing devices and changes resulting from any patching. Between the August and September [REDACTED] patching change requests a separate change request was promoted which re-wrote the exception detection date in the entity's baselining tool. Therefore, these are the targeted date ranges in question to examine baselines that were incomplete or not updated within 30 days in order to ensure there are no other baseline discrepancies that were not previously promoted. <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by May 10, 2020:</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
RFC2019021232	CIP-010-2	R1	[REDACTED]	[REDACTED]	9/30/2018	10/3/2018	Self-Report	5/10/2020
			<p>5) will create an operational compliance report and process that compares the assets related to the change request and the deviations that are promoted in the baseline tool. This operational compliance validation will be reviewed by a peer during the "Evidence Review" task that is generated for each change request. The peer reviewer will ensure that all assets associated to the change request have the expected deviations promoted in the baseline tool. If the peer reviewer discovers a miss-match on the report or in the baseline tool an incident ticket is opened for the responsible subject matter expert to investigate and correct before the 30 day promotion date expires;</p> <p>6) will train applicable peer reviewers on updated preventive compliance reporting process developed in Milestone #4. The training will be developed by the risk and compliance team and will be provided in a face to face meeting with the peer reviewers. Training will include how to generate the report, how to compare the reports, expected results for evidence, and the incident ticket creation. Completion of the training will be tracked by sign in sheet after the face to face training meeting is completed. The preventive compliance reporting process will be conducted for all change requests after May 8, 2020; and</p> <p>7) will test this preventive operation control for a sample set of change requests that occur between February 10, 2020 and May 8, 2020 to ensure the peer reviewer can output the report, review and validate the results. The entity will modify the process if necessary documenting the changes and tweaking the results as needed. Once the process is valid, the entity will develop a step by step process document to train the peer reviewers.</p> <p>Additional time is required to create the operational compliance report, to train applicable peer reviewers, and to test the preventative operation control and to develop a corresponding process document.</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
RFC2019022043	CIP-004-6	R3	[REDACTED]	[REDACTED]	12/13/2017	1/21/2018	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 August 1, 2018, the entity submitted a [REDACTED] stating that, [REDACTED] it was in noncompliance with CIP-004-6 R3.</p> <p>During the entity's upgrade to a new Human Resources System of Record, the [REDACTED] monitored data that was being fed to the access management system to support the transition. On January 9, 2018, the team identified a blank Personnel Risk Assessment (PRA) field for a person in the access management system that had a NERC role assigned to him that required the completion of a PRA prior to granting access. The access management system team began investigating the issue and found that this specific NERC role in the access management system was not validating the PRA prerequisite for authorized NERC access due to a validation flag not being set on the role.</p> <p>An investigation into the issue was immediately initiated to validate the PRA information in the access management system, and to determine the extent of condition. A query was run on the system, which identified several additional roles that also didn't have the validation flags set as required. The individuals that had access to those roles were reviewed and verified for accuracy. PRA data was updated as necessary, and the roles were set as required by the company processes. Once the verification was complete and all the roles were correct, 1 person was identified as having invalid access to a role for the Physical Security Perimeter (PSP).</p> <p>When roles are created, [REDACTED] his step was bypassed due to a human performance error, which led to [REDACTED]</p> <p>Further investigation into the issue was performed and on 3/12/2018, the entity determined a possible non-compliance may have occurred with CIP-004-6, R3, Part 3.5.</p> <p>The root cause of this noncompliance was the entity's failure to follow its established process and the manual nature of the established process. This root cause involves the management practices of reliability quality management, which includes maintaining a system for deploying internal controls, and workforce management, which includes providing training, education, awareness to employees.</p> <p>This noncompliance began on December 13, 2017, when the individual's PRA lapsed, and ended on January 21, 2018, when the entity revoked access for the individual.</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, a process was in place for requesting [REDACTED] for the roles, but due to the volume of changes being made at the time, the step was overlooked and thought to have been completed. Second, the misconfiguration of the roles in the system was identified within a short period after creation. Immediate steps were then taken to identify, verify, and configure the roles to align with company processes. Third, the person that was granted access without [REDACTED]. Although access was requested and granted by his manager, the [REDACTED], and by the [REDACTED], he never entered the PSP without being properly logged and escorted. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) revoked access for the person who did not have a current PRA on file; 2) set training and PRA verification flags on the roles within the access management system to prevent access from being provisioned without the required training and PRA prerequisites; 3) performed training on the access management system Job Aid for the performers as part of the regular team update; and 4) created an automated report as a control to review whether the access management system PRA and training verification flags are set on all roles. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021193	CIP-004-6	R5	[REDACTED]	[REDACTED]	11/29/2018	1/3/2019	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 27, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5. During the entity's quarterly access review, it discovered accounts for two contractors that should have been previously removed. The accounts were domain administrator accounts that had been provisioned as part of a project.</p> <p>The first contractor's last day of work at the entity was November 28, 2018. The entity did not revoke the first contractor's access in the Physical Access Control System (PACS) or deactivate his badge until December 26, 2018. The entity did not disable the first contractor's electronic account until January 3, 2019.</p> <p>The second contractor's last day of work at the entity was also November 28, 2018. The entity did not revoke the second contractor's access in the PACS system or deactivate his badge until December 11, 2018. The entity did not disable the second contractor's electronic access account until January 2, 2019.</p> <p>The root cause of this noncompliance was inadequate training on the entity's contractor offboarding process. The entity routinely offboards employees and contractors working in a staff augmentation role but does not routinely offboard contractors who are members of a third-party project team. In this case, the contractors were part of a third-party project team, and the [REDACTED] was unfamiliar with the contractor offboarding process.</p> <p>This noncompliance involves the management practice of workforce management. Workforce management includes ensuring that entity personnel, such as employees in the [REDACTED], understand when and how to initiate access revocation processes.</p> <p>This noncompliance started on November 29, 2018, when the entity failed to remove access and ended on January 3, 2019, when the entity completed the process of removing the access of the contractors.</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 risk posed by this noncompliance is the potential for a former contractor to exploit remaining access and actively harm the entity's assets and, in turn, the BPS. The risk was minimized because the entity retrieved the contractors' security badges and computers at the time of their departure, thereby substantially restricting the ability of the contractors to exploit any remaining access. Restated, even though the contractors' accounts were active, the contractors did not have a legitimate way to access those accounts. Without badges, they could not get in the building, and without entity-issued computers, they could not log-in remotely and use the electronic accounts. Further, the contractors left on good terms at the completion of their work (i.e., they were not immediately and involuntarily terminated), thereby further reducing the risk. The entity identified this noncompliance through one of its internal controls, which reduced the likelihood of this issue persisting for a longer period of time. 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) removed the accounts of the contractors; and 2) conducted training at an [REDACTED] to ensure that all individuals know the requirements for submitting contractor access revocation requests immediately upon departure. The information that was reviewed during this training session will also be reviewed annually with the [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
RFC2018020825	CIP-004-6	R5	[REDACTED]	[REDACTED]	8/4/2018	8/7/2018	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 11, 2018, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5. On Monday, August 6, 2018, while investigating issues of users not being properly updated in its access management database, the entity discovered an issue where it failed to revoke access within 24 hours of termination.</p> <p>On Friday, August 3, 2018, a problem occurred in the [REDACTED]. Specifically, [REDACTED]. However, it failed to run on the morning of August 3rd. Consequently, one user, who voluntarily ended his employment on August 3rd, retained his electronic access rights for support of transient cyber assets beyond the 24 hour time limit. The entity disabled his access on August 7, 2018.</p> <p>The root cause of this noncompliance was the technical issue with the [REDACTED]. This root cause involves the management practices of workforce management, which includes managing employees' access to assets, and integration, because the technical issue giving rise to this noncompliance related to the [REDACTED].</p> <p>This noncompliance started on August 4, 2018, when the entity was required to have revoked the employee's access and ended on August 7, 2018, when the entity actually revoked his 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 (BPS) based on the following factors. The risk posed by failing to remove an individual's physical and electronic access after termination is that the individual could use that access to cause harm to the entity's network and BPS as a whole. This risk was mitigated in this case by the following factors. First, the employee's manager collected the employee's badge and laptop upon termination, which reduced the likelihood that the employee could have accessed any assets either physically or electronically. Second, the entity quickly identified and corrected the issue, minimizing the amount of time that the employee's access remained enabled. Third, the employee left voluntarily and on good terms with the company, which reduces the likelihood that the employee would have attempted to cause any adverse impact to 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) ensured the failed [REDACTED]; 2) created a process document for IT support to follow during HR System outages; 3) communicated the process document for IT support to follow during HR System outages; 4) provided the access management team a "look ahead" report of all terminations for the period affected by the HR System outage. This report is auto-generated by the another software tool; 5) updated their access management procedures for actions to take when receiving notifications from HR technology about HR system outages and how to use the look ahead report; 6) communicated access management procedure changes; 7) entity amended existing use of a service manager to add automated monitoring of processes for employee/contractor terminations; and 8) communicated and educated IT support team regarding amended use of a service manager for automated monitoring of processes for employee/contractor terminations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019020978	CIP-010-2	R1	[REDACTED]	[REDACTED]	9/18/2018	10/10/2018	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, [REDACTED] it was in noncompliance with CIP-010-2 R1. On September 17, 2018, a [REDACTED] lost network connectivity. The troubleshooting solution was to uninstall and reinstall a currently installed software tool version on the [REDACTED]. Since no baseline change was expected to resolve this issue, a non-baseline change ticket was opened to memorialize this troubleshooting. The next day, a technician performed the software change. The technician correctly uninstalled the software tool, but accidentally selected a newer version of the software during reinstallation. The installation of the incorrect version of the software created an unauthorized change to the baseline software configuration for the [REDACTED].</p> <p>Subsequently, on September 25, 2018, during the [REDACTED] of baseline configurations, the entity discovered the incorrect version of the software. The [REDACTED] were notified of the discrepancy and the need to correct the issue. Later, on October 10, 2018, in order to correct the issue, the entity created a proper baseline-impacting change ticket and approved the newer version of the software.</p> <p>The root cause of this noncompliance was the technician's lack of familiarity with [REDACTED]. This technician was needed to troubleshoot [REDACTED] because the device administrator could not connect to it due to the device's failure. This root cause involves the management practices of asset and configuration management, which includes controlling changes to assets and configuration items, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on September 18, 2018, when the technician made baseline impacting change without a proper change ticket and ended on October 10, 2018, when the entity formally approved 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. The risk posed by making unauthorized changes is that they could adversely impact the security of the impacted assets. This risk was mitigated in this case by the following factors. First, the entity quickly identified and corrected the issue through effective internal controls [REDACTED]. Second, although the newly installed version of the software tool was not specifically authorized for [REDACTED], it was tested and authorized for use on other devices. Third, [REDACTED] is one of [REDACTED] supporting operations. Because [REDACTED] were available during the time of the noncompliance, the potential impact of [REDACTED] being lost was minimized. No harm is known to have occurred.</p> <p>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 noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) conducted a meeting with [REDACTED] team members to review software baseline variance and reinforce desired behavior to submit change tickets indicating all baseline impacting changes; 2) entered a change request to document the software tool installation and updated the baseline change authorizations for the device; 3) conducted a follow-up meeting with [REDACTED] team members and relevant team members to: summarize the issue causing the baseline variance; discuss potential solutions to the issue; determine next steps; and distribute meeting notes; 4) documented and communicated a process to be used by [REDACTED] team members, and [REDACTED] team members. The process includes: [REDACTED] 5) investigated feasibility to provide selective access for support team members to allow them to troubleshoot devices that are currently inaccessible. The entity also made recommendations for selective access improvements for device support. The entity further developed a proposed action plan for recommended selective access improvements and reviewed proposed action plan with leadership from [REDACTED] gained approval for implementation; and 6) implemented the approved action plan to provide selective access for support team members to allow them to troubleshoot devices that are currently inaccessible. The entity will also document the approved action plan in a job aid and distribute it to all device owners [REDACTED] and all team members who have authorization to [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
RFC2019022044	CIP-004-6	R3	[REDACTED]	[REDACTED]	12/13/2017	1/21/2018	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 August 1, 2018, the entity submitted a [REDACTED] stating that, [REDACTED] it was in noncompliance with CIP-004-6 R3.</p> <p>During the entity's upgrade to a new Human Resources System of Record, the [REDACTED] monitored data that was being fed to the access management system to support the transition. On January 9, 2018, the team identified a blank Personnel Risk Assessment (PRA) field for a person in the access management system that had a NERC role assigned to him that required the completion of a PRA prior to granting access. The access management system team began investigating the issue and found that this specific NERC role in the access management system was not validating the PRA prerequisite for authorized NERC access due to a validation flag not being set on the role.</p> <p>An investigation into the issue was immediately initiated to validate the PRA information in the access management system, and to determine the extent of condition. A query was run on the system, which identified several additional roles that also didn't have the validation flags set as required. The individuals that had access to those roles were reviewed and verified for accuracy. PRA data was updated as necessary, and the roles were set as required by the company processes. Once the verification was complete and all the roles were correct, 1 person was identified as having invalid access to a role for the Physical Security Perimeter (PSP).</p> <p>When roles are created [REDACTED]. This step was bypassed due to a human performance error, which led to [REDACTED].</p> <p>Further investigation into the issue was performed and on 3/12/2018, the entity determined a possible non-compliance may have occurred with CIP-004-6, R3, Part 3.5.</p> <p>The root cause of this noncompliance was the entity's failure to follow its established process and the manual nature of the established process. This root cause involves the management practices of reliability quality management, which includes maintaining a system for deploying internal controls, and workforce management, which includes providing training, education, awareness to employees.</p> <p>This noncompliance began on December 13, 2017, when the individual's PRA lapsed, and ended on January 21, 2018, when the entity revoked access for the individual.</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, a process was in place for requesting [REDACTED] for the roles, but due to the volume of changes being made at the time, the step was overlooked and thought to have been completed. Second, the misconfiguration of the roles in the system was identified within a short period after creation. Immediate steps were then taken to identify, verify, and configure the roles to align with company processes. Third, the person that was granted access without [REDACTED]. Although access was requested and granted by his manager, the [REDACTED] and by the [REDACTED], he never entered the PSP without being properly logged and escorted. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) revoked access for the person who did not have a current PRA on file; 2) set training and PRA verification flags on the roles within the access management system to prevent access from being provisioned without the required training and PRA prerequisites; 3) performed training on the access management system Job Aid for the performers as part of the regular team update; and 4) created an automated report as a control to review whether the access management system PRA and training verification flags are set on all roles. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021054	CIP-011-2	R1	[REDACTED]	[REDACTED]	6/18/2018	2/6/2019	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 11, 2019, the entity submitted a Self-Report stating that [REDACTED] it was in noncompliance with CIP-011-2 R1. At the time of this noncompliance, the entity had a program that addressed sharing Bulk Electric System Cyber System Information (BCSI) with third parties. The program required that a data sharing request be completed before information was shared with a third party. In this case, the entity shared BCSI with a third party prior to completing a data sharing request in accordance with its program. The issue was discovered while executing an internal control [REDACTED].</p> <p>[REDACTED], the entity retains a vendor to assess cyber security measures at one of its power plants. In January, 2018, it began the process of engaging a vendor to conduct the assessment. The vendor's primary assessment was completed onsite at the power plant in June, 2018; however, the vendor intended to draft its evaluation report offsite. To assist in the preparation of the report, entity personnel shared (and allowed vendor representatives to leave with) BCSI, which included host names, IP addresses, and vulnerabilities. But, entity personnel failed to complete a data sharing request and ensure that adequate protections were in place prior to sharing the information. The BCSI was stored on a vendor-issued laptop.</p> <p>The root causes of this noncompliance were (a) a deficient program and (b) the personnel's lack of familiarity with the data sharing process. Although the program required that personnel complete a data sharing request prior to sharing information with a third party, this requirement was not effectively communicated, and the entity did not clearly articulate the steps required to carry out this task.</p> <p>This noncompliance implicates the management practice of workforce management. Workforce management includes the need to (a) develop clear, thorough, and executable processes, procedures, and work instructions and (b) effectively implement those processes, procedures, and work instructions through training and promoting awareness.</p> <p>This noncompliance started on June 18, 2018, when the entity shared BCSI without following the requirements of its program and ended on February 6, 2019, when the entity confirmed that the shared information was deleted by the vendor.</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. Failing to implement or follow procedures for protecting and securely handling BCSI could lead to unauthorized access to such information and corresponding misuse or dissemination, potentially leading to misoperation or instability in the BPS. The risk was minimized based upon the following facts. First, in this case, BCSI was shared with a familiar and trusted vendor, and the entity had previously entered into an agreement with the vendor concerning the handling of information (i.e., a confidentiality and non-disclosure agreement). Second, the entity contracted the vendor, and the vendor confirmed that the information was stored on a vendor-issued laptop. Vendor-issued laptops are password-protected, subject to a password expiration policy, and encrypted. Moreover, [REDACTED]. Collectively, these measures would assist in preventing unauthorized access and the ability to retrieve and read information stored on the laptop. Third, the vendor's employees completed training and were subjected to background checks prior to performing 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 involved different facts, circumstances, and/or causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) confirmed with the vendor that the data had been deleted; and 2) updated its CIP-011 program (and communicated the updates) to make clear to supervisors and subject matter experts that a vendor is not allowed to leave with BCSI without a completed data sharing request and included detailed information [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
RFC2019021235	CIP-004-6	R4	[REDACTED]	[REDACTED]	4/17/2018	12/7/2018	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 March 7, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R4. Specifically, the entity did not have authorization records for three employees who had electronic access to [REDACTED] in violation of CIP-004-6 R 4.1. The [REDACTED] were a subset of components that were implemented as part of the entity's deployment of [REDACTED] which the entity intended to utilize as [REDACTED]. The entity's [REDACTED] discovered this noncompliance while reviewing records relating to the Tripwire implementation project.</p> <p>The root causes of this noncompliance were: (a) a failure to follow the entity's access management program and tracking system, [REDACTED]; and (b) the lack of a verification control in the entity's asset implementation process. The entity was implementing new assets and failed to properly document the user access entitlements referenced herein in accordance with the entity's access management program and tracking system. Further, the entity's asset implementation process did not include a control to check if entitlements were created and properly documented prior to placing an asset into production. Such a control would have assisted in detecting and resolving this issue before resulting in a noncompliance.</p> <p>This noncompliance involves the management practices of workforce management and asset and configuration management. Workforce management includes the development and successful implementation of clear, thorough, and executable processes and procedures that can minimize the likelihood of the occurrence of this type of noncompliance. Asset and configuration management includes the need to effectively inventory, monitor, manage, and control assets, accounts, entitlements, and configuration items.</p> <p>This noncompliance started on April 17, 2018, when the [REDACTED] were implemented with existing user access entitlements that could not be reconciled with records in the entity's access management tracking system and ended on December 7, 2018, after the entity identified and added the entitlements and records to its access management tracking system.</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. Unauthorized electronic access increases the risk of misuse of Bulk Electric System Cyber Systems, which could cause corresponding harm to the reliability and resilience of the BPS. In this case, the risk was minimized based on the following facts. First, this was primarily a documentation issue. For the duration of this noncompliance, three users had access to the [REDACTED] and all three were trusted administrators who had a need for access and all necessary qualifications (i.e., completed training and valid personnel risk assessments). At the time of implementation of the assets, the entity simply failed to document the user access entitlements in its access management tracking system. Second, cyber security controls such as antivirus monitoring and change management controls reduced the likelihood of undetected malicious activity. 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 violations involved different factual circumstances, issues, and/or causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) documented the entitlements and authorization records in its access management tracking system; 2) verified that all employees who had electronic access to the [REDACTED] as of February 7, 2019, had proper authorizations and a need for such access; 3) documented ownership of the [REDACTED]; and 4) updated its asset management process to include controls to verify that asset entitlements have been created and properly documented before an asset is placed into production. And, the entity communicated this update to appropriate personnel 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021052	CIP-010-2	R4	[REDACTED]	[REDACTED]	11/23/2018	11/23/2018	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 1, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R4.</p> <p>On November 23, 2018, an entity Dispatcher used a USB charger to plug his mobile phone into a NERC CIP port within the entity's Physical Security Perimeter (PSP). The Dispatcher removed another USB cord to plug the charger into the port, but the USB cord that was removed controlled a mouse that was used to move between the [REDACTED]. The Dispatcher realized that the mobile phone charger was plugged into the incorrect port when the mouse, which was originally plugged into that port, was not functioning. The Dispatcher removed the mobile phone charger immediately, and plugged the mouse USB chord back in.</p> <p>The workstation impacted is a Medium Impact Bulk Electric System Cyber System (BCS). The mobile phone USB charger was not authorized for use in the NERC CIP port. The power strip into which the mobile phone USB charger was inserted has two sets of USB ports and is a part of the workstation configuration. Two of the ports are used for charging and do not qualify as NERC CIP ports, and the other two ports are used for the keyboard and mouse for the workstation, qualifying as NERC CIP ports.</p> <p>The root cause of this noncompliance was the entity's failure to differentiate between the two NERC CIP ports and the two non-CIP ports resulting in the Dispatcher erroneously inserting the mobile phone USB charger in a NERC CIP port.</p> <p>This noncompliance involves the management practices of implementation and workforce management. Implementation management is involved in this noncompliance because the NERC CIP ports and non-CIP ports were not properly distinguished during the implementation of the workstation, resulting in a lack of clarity as to which ports qualified as NERC CIP ports. Workforce management is involved in this noncompliance because the Dispatcher was not adequately trained on the use of USB devices in NERC CIP ports.</p> <p>This noncompliance started on November 23, 2018, when the Dispatcher plugged the mobile phone USB charger into the NERC CIP port, and ended approximately one minute later when the Dispatcher removed the mobile phone USB charger from the NERC CIP port.</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 the insertion of a mobile phone into a NERC CIP port is the potential for malicious code injection via the mobile phone. This risk was mitigated in this case by the following factors. First, the mobile phone was plugged into the NERC CIP port for less than 60 seconds, minimizing the amount of time that malicious code could have been injected into the workstation. Second, the entity had malicious code prevention tools in place to protect against the introduction of malicious code, thus reducing the risk of malicious code successfully infiltrating the system. ReliabilityFirst also notes that no baseline impacting changes occurred to the workstation as a result of the mobile phone being plugged in. No harm is known to have occurred.</p> <p>ReliabilityFirst notes that preventing this type of unauthorized use of Transient Cyber Assets and Removable Media is a very basic and fundamental cyber security practice. While the risk in this particular case is minimal, entities are expected to have solid controls to prevent this type of issue from occurring altogether.</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 while the result of the prior noncompliance were arguably similar, the prior noncompliance arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) replaced all keyboard and mouse in the [REDACTED] 2) turned on alerts for [REDACTED] removable media events; and 3) reviewed reports for the workstation to confirm that no baseline changes were introduced, and no malicious code was found on the workstation. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021027	CIP-010-2	R1	[REDACTED]	[REDACTED]	4/24/2018	8/31/2018	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 23, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1. This noncompliance is composed of two separate instances of failures to authorize changes that deviate from the existing baseline configuration.</p> <p>In the first instance, on May 7, 2018, the entity discovered that [REDACTED] software had been installed without authorization on April 24, 2018, on a [REDACTED] server [REDACTED] which is classified as an Electronic Access Control or Monitoring System (EACMS) associated with [REDACTED] Bulk Electric System (BES) Cyber System. The entity had installed the software without going through the change management process and without receiving authorization prior to completing the change. The entity discovered the [REDACTED] software installation during the May 7, 2018, bi-weekly review of baseline deviations for the period of April 10, 2018-April 24, 2018.</p> <p>In the second instance, on August 27, 2018, the entity discovered that a [REDACTED] (an EACMS) had added a new agent version without authorization. The entity upgraded the backup software on the [REDACTED] server and the backup software automatically deployed the new agent version to the [REDACTED] server. The installation occurred by an [REDACTED] employee new to their role that was unaware of the change management requirement. The entity discovered the unauthorized change to the [REDACTED] when reviewing baseline deviations detected by the entity's baseline tool.</p> <p>The root cause in both instances of this noncompliance was inadequate training resulting from the entity's lack of an onboarding program to ensure that new system administrators are provided training on the entity's change management process. (Had these changes gone through the change management process, the change ticket owner would have been required to associate assets to the change. If the NERC asset would have been associated to the change ticket the implementer would have been aware. Since the implementer followed no change management process the preventative controls in the change management process were circumvented.) This noncompliance involves the management practices of asset and configuration management and workforce management. Asset and configuration management is involved because both instances involve a failure to authorize a configuration change. Workforce management is involved because entity staff were not properly trained on how to adhere to internal change management processes resulting in this noncompliance.</p> <p>The first instance started on April 24, 2018, when the entity installed the [REDACTED] software without authorization, and ended on May 7, 2018, when the entity performed the necessary review and authorization function. The second instance started on August 24, 2018, when the entity added a new agent without authorization. The second instance ended on August 31, 2018, when the entity performed the necessary review and authorization function.</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 unauthorized software or agents to be implemented which could adversely affect overall system security. The risk is minimized for the following reasons: In the first instance, the installation and software were necessary and appropriate and it was isolated to the single affected device. In the second instance, the loss of this device would have had minimal impact because multiple active directory servers are in place to continue normal functions. Also, the upgrade was necessary and recommended by the vendor. And, both instances were discovered quickly as the result of strong internal controls resulting in short durations of approximately two weeks for the first instance and one week for 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) created a [REDACTED] change request for approval authorization of change and verification of CIP-005 and 007 controls; 2) performed an Extent of Condition review to identify other similar occurrences 3) executed the corrective action to true up current NERC CIP employees receipt of Change Management Training by comparing employees who have taken the training within the last year with employees new to the NERC CIP role since the last time the training was promoted. This training will now be an annual requirement for employees with the identifier of NERC CIP Employee; and 4) created or modified existing banners on NERC CIP Assets that will alert the user that the asset is a NERC CIP Production Cyber Asset that requires an approved Change request prior to performing any updates. Currently, [REDACTED] Servers and workstations have banners that identify some of the assets details (such as Asset Name and Application) that the asset is used for. The intent of this milestone is to strengthen the existing requirement that all production NERC CIP assets must have an approved change request prior to making any modifications to that asset. These banners will appear on the initial logon screen or equivalent that have capabilities to modify the initial logon screen. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021254	CIP-004-6	R2	[REDACTED]	[REDACTED]	7/1/2017	10/23/2017	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 [REDACTED], the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R2. During its preparation for a [REDACTED], the entity was reviewing access and training records and discovered that three contractors had not completed required training during a single interval in violation of CIP-004-6 R2.3.</p> <p>The entity utilizes an online training system and assigns training by selecting all employees and contractors that were hired prior to a certain date. The system tracks completion of training and sends reminders aimed at prompting completion. In this case, one of the entity's annual training assignments was not assigned to the above-referenced contractors in the system, and therefore, completion was not tracked and no reminders were sent. As a result, none of the three contractors completed required training within a single training interval. However, all three completed training during prior intervals. Upon identification of the issue, the entity contacted the responsible vendor, and collectively, they could not figure out why training was not assigned to these three contractors during a single training interval. The entity conducted additional analysis, including unsuccessful attempts to duplicate the issue in test systems. The entity reviewed training records during a multi-year timeframe and did not find any additional instances of noncompliance.</p> <p>The root cause of this noncompliance was reliance on an online system without adequate verification controls. This noncompliance involves the management practice of verification. The entity should have compared records in the online training system with its access management records in order to verify that all personnel completed required training.</p> <p>The first instance started on July 1, 2017, when the first contractor did not complete required training prior to the phased in implementation date of CIP-004-6 R2.3 and ended on August 7, 2017, when the contractor completed training. The second instance started on July 1, 2017, when the second contractor did not complete required training prior to the phased in implementation date of CIP-004-6 R2.3 and ended on September 7, 2017, when the contractor completed training. The third instance started on July 1, 2017, when the third contractor did not complete required training prior to the phased in implementation date of CIP-004-6 R2.3 and ended on October 23, 2017, when the contractor discontinued work with the entity.</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. There is a heightened risk to the reliability of the BPS if personnel with access to Bulk Electric System Cyber Systems are not properly trained to utilize such access in a secure manner. Here, the risk was minimized because all three contractors had completed training in prior years and, therefore, were less likely to improperly utilize their access. Further, all of the contractors subsequently completed training. The first and second contractors completed training in August, 2017, and September, 2017, respectively. The third contractor separated from the entity in October, 2017, but completed training again in June, 2018, upon rejoining the entity. Additionally, all the contractors had only physical access and no electronic access. 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 involves different facts, circumstances, and/or causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) held a meeting with members of various departments to determine a root cause and corrective actions; 2) held a meeting with members of various departments to review reports and determine the best report to verify all required personnel have completed their training; 3) updated its security training compliance procedure to include a step to verify all required personnel have completed their training using the authoritative source. The entity will compare the records within the online training system to authorization records within the access management system. This comparison will take place approximately 75 days after the beginning of the annual training roll out, which will allow time to ensure any discrepancies are identified and training is completed during the 15 month timeframe; and 4) compiled training records of the three contractors showing that they completed subsequent training. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022045	CIP-006-6	R2	[REDACTED]	[REDACTED]	1/23/2018	4/28/2018	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 August 1, 2018, the entity submitted a [REDACTED] stating that, [REDACTED] it was in noncompliance with CIP-006-6 R2.</p> <p>On the afternoon of January 23, 2018, the security center received an invalid access attempt alarm for a control house access point at a Medium Impact substation with External Routable Connectivity (ERC). An employee (Unauthorized Employee) was attempting to use his card access badge on the access point door card reader, generating an alarm.</p> <p>A review of the alarm found that the Unauthorized Employee was provided access to the Physical Security Perimeter (PSP) as a visitor earlier in the morning of that day; he was logged into the Visitor's Log Book and was being escorted by an employee (Escort), who was authorized for unescorted access to the PSP. Further review [REDACTED] provided a timeline indicating that the Escort allowed the Unauthorized Employee to remain in the PSP alone and unescorted, several times throughout the day for various short durations.</p> <p>After arriving at the substation in the early morning, the Unauthorized Employee, realizing his access was revoked due to expired training, left the substation to return to the office to retake the required NERC annual training. The required training for access was successfully retaken, at which point, the Unauthorized Employee and Escort were given direction that his card would be reauthorized within a brief period of time since his training was now current.</p> <p>The steps that were taken by the Unauthorized Employee to renew his training requirements and the direction they were provided left both employees assuming that it was a just matter of time before the Unauthorized Employee's badge would be re-enabled. This was a clear misunderstanding on their part to assume that retaking the training would automatically re-enable card access and that, because of current training, he was now authorized for unescorted access. Because of this misunderstanding, they continued with the work at the substation that was assigned to them. Both employees acknowledged they believed they had an understanding of the entity Visitor Control Program requirements.</p> <p>In a second incident, on April 28, 2018, two substation employees were working in a control house at a Medium Impact substation with ERC. The one employee, who was acting as the visitor escort, was authorized for unescorted access. The visitor escort was escorting the other employee who was not authorized for unescorted access and regarded as a visitor. At approximately 12:17pm, the visitor escort exited the control house to retrieve a bag from his vehicle, leaving the visitor within the PSP unsupervised. The visitor escort returned to the building approximately 35 seconds later, continuing to escort the visitor. This issue was identified during [REDACTED] video records. The visitor escort reported that while repairing the damaged equipment on that weekend day, he didn't realize the implications as he momentarily stepped outside for his bag, leaving the visitor alone in the control house unsupervised.</p> <p>The root cause of this noncompliance was the individuals' failure to follow the established visitor control program. This root cause involves the management practice of workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance has two separate durations. The first incident started on January 23, 2018, when the unauthorized employee was left unescorted throughout the day, and ended later that same day when the unauthorized employee left the PSP for the day. The second incident started on April 28, 2018, when the visitor escort left the visitor unescorted, and ended approximately 35 seconds later, when the escort returned to the building.</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's Visitor Control Program requires and implements controls to ensure Bulk Electric System Cyber Assets within PSPs are secured and monitored at all times, in accordance with the CIP-006-6 requirements. In fact, the above issues were identified as a result of the controls in place at the time of the incident. Second, with respect to the first instance, the person was authorized until his training expired, which when retaken, provided him with the prerequisites for authorization. Third, with respect to the second incident, the employee was working to repair equipment in the control house, which only trusted personnel are permitted to perform. Fourth, in both cases, the individuals were unsupervised for very short durations of time and were trusted employees. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance:</p> <p>For the first issue, the entity:</p> <ol style="list-style-type: none"> 1) invited a compliance representative to their mandatory safety meeting to roll out the exact requirements for unescorted access in a substation and visitor requirements; 2) communicated lessons learned of this issue to the relay department, and the responsible group outlined and discussed what is communicated to clients regarding access questions and processes - specifically, how access reinstatement occurs and what is required by a client due to updated training or PRAs. <p>For the second issue, the entity:</p> <ol style="list-style-type: none"> 1) conducted two safety meetings for the compliance team, providing a presentation delineating the physical access requirements for PSP control houses at medium substations; 2) developed and disseminated a job aid to delineate the physical access requirements for substation PSPs governing authorized unescorted physical access and visitor's access. The job aid was disseminated to personnel with authorized unescorted physical access to entity substation PSPs; and 					

ReliabilityFirst Corporation (ReliabilityFirst)

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
RFC2019022045	CIP-006-6	R2	[REDACTED]	[REDACTED]	1/23/2018	4/28/2018	Self-Log	Completed
			3) developed supplemental training on the guidelines of PSP physical access privileges, to be used as periodic awareness for its substation personnel.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019020925	CIP-002-5.1a	R2	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	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 9, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-002-5.1a R2. The entity registered with NERC on [REDACTED] as a low impact facility. As part of its first-time registration process, the entity completed its initial CIP-002-5.1a Impact Assessment, including having it signed by the CIP Senior Manager, on [REDACTED]. However, during a [REDACTED] year-end review of NERC compliance, the entity discovered that it had failed to review the Impact Assessment and have it approved by the CIP Senior Manager by the 15 calendar month deadline. Upon discovery, the entity completed the necessary review and approval by [REDACTED] (46 days late).</p> <p>The root cause of this noncompliance was the entity's lack of tracking system to notify the entity when the review was due. This root cause involves the management practice of reliability quality management, which includes maintaining a system for deploying internal controls.</p> <p>This noncompliance started on [REDACTED], when the entity was required to complete the review and approval of the Impact Assessment and ended on [REDACTED], when the entity completed its 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. The risk posed by failing to review and approve the Impact Assessment every 15 calendar months is that the assessment could change, which would impact the security controls the entity would have to implement. This risk was mitigated in this case by the following factors. First, the entity quickly identified and corrected the issue through an internal review. Second, the facility is a single low impact site with a three year average net capacity factor of 4.38%, which reduces the potential impact of any adverse consequences. Also, it is important to note that the review did not identify any changes. 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 installed a new work management system and will use it to track due dates for compliance tasks including the Impact Assessment.</p> <p>ReliabilityFirst 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
RFC2019020924	CIP-003-6	R1	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	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 9, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-003-6 R1. The entity registered with NERC on [REDACTED], as a low impact facility. As part of its first-time registration process, the entity completed its initial CIP-003-6 Cyber Security Policy, including having it signed by the CIP Senior Manager, on [REDACTED]. However, during a [REDACTED] year-end review of NERC compliance, the entity discovered that it had failed to review this policy and have it approved by the CIP Senior Manager by the 15 calendar month deadline. Upon discovery, the entity completed the necessary review and approval by [REDACTED] (46 days late).</p> <p>The root cause of this noncompliance was the entity's lack of tracking system to notify the entity when the review was due. This root cause involves the management practice of reliability quality management, which includes maintaining a system for deploying internal controls.</p> <p>This noncompliance started on [REDACTED], when the entity was required to have completed its review and approval of the Cyber Security Policy and ended on [REDACTED], when the entity completed its review and approval of the Cyber Security Policy.</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 review and approve of the Cyber Security Policy every 15 calendar months is that the entity may continue to deploy outdated security practices. This risk was mitigated in this case by the following factors. First, the entity quickly identified and corrected the issue through an internal review. Second, considering the facility is a newer low impact facility with minimal compliance requirements, it is unlikely that the information contained in the Cyber Security Policy would have changed during this first review cycle (and the review did not identify any changes once it was conducted after identifying the noncompliance), reducing the likelihood that the 46 day delay would have resulted in any changes to the policy. 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 added a work order to its work management system to ensure as the date comes due, a work order is issued to complete the review and CIP Senior Manager approval within the fifteen-month requirement. All the annual preventative controls are generated on January 1 of each new year. They are then reviewed monthly by everyone to ensure that submittals are timely. A new "check and balance" is in place where everyone is aware of what is due and when via the work management system program. In addition, this is also part of the new compliance process management program and the NERC team at the entity has a correct calendar for the standards and requirements.</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
RFC2019020908	CIP-002-5.1a	R2	[REDACTED]	[REDACTED]	9/21/2017	1/30/2019	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 31, 2018, the entity submitted a Self-Report stating that [REDACTED] it was in noncompliance with CIP-002-5.1a R2. As background, the entity has historically worked with a consultant company to assist it with its NERC compliance. The consultant company had one employee devoted to this role. When that person left the consultant company, a new person took over and performed a full review of the entity's NERC compliance program. That review identified this issue.</p> <p>On June 21, 2016, the entity implemented a process that considered its assets as required by CIP-002-5.1a, and determined [REDACTED]. However, the entity failed to perform a review of this identification within the 15 calendar month time frame.</p> <p>The root cause of this noncompliance was the entity's lack of internal controls to ensure it performed the annual review. The root cause involves the management practice of reliability quality management, which includes maintaining a system for deploying internal controls.</p> <p>This noncompliance started on September 21, 2017, when the entity was required to comply with CIP-002-5.1a R2 and ended on January 30, 2019, when the entity completed its annual review.</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 risk posed by failing to review the annual list of BES Cyber Systems is that the entity may be unaware of changes to its assets and may not protect them properly. This risk was mitigated in this case by the following factors. First, the entity is [REDACTED], [REDACTED]. Second, the entity has [REDACTED], so it [REDACTED]. Third, [REDACTED]. 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) updated its CIP-002 BES Cyber System Identification and Categorization and completed the review of it; and 2) added a calendar event for the annual review of the entity's assets required under Requirement R2 for management and operating personnel. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021404	CIP-004-6	R2	[REDACTED]	[REDACTED]	2/12/2019	3/19/2019	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 April 22, 2019, the entity submitted a Self-Report stating that [REDACTED] it was in noncompliance with CIP-004-6 R2.</p> <p>On March 18, 2019, as a part of a training-completion audit, the entity identified one instance where an individual was granted access before completing the required training. More specifically, on February 12, 2019, the entity granted a [REDACTED] executive access to a NERC Physical Security Perimeter (PSP) before the executive completed his [REDACTED] training. The executive had previously taken this training, but his training was no longer current. The executive did not enter any NERC PSPs after the entity granted him access and before he completed his [REDACTED] training on March 19, 2019.</p> <p>Regarding the root cause, the entity determined that the Information Technology (IT) [REDACTED] [REDACTED] misread the training record and incorrectly concluded that the executive's physical access training had been completed. The IT [REDACTED] [REDACTED] had been recently trained in the verification process and this was among the first reviews he completed on his own without mentoring. Upon discovery of this issue, the entity reassigned the training immediately and the executive completed the training one day later on March 19, 2019.</p> <p>This noncompliance involves the management practices of workforce management, validation, and verification. The root cause is ineffective training as the IT [REDACTED] [REDACTED] was not effectively trained on how to complete the job. Another contributing cause is a lack of effective verification controls.</p> <p>This noncompliance started on February 12, 2019, when the entity granted a [REDACTED] executive access to a NERC PSP before he completed his training and ended on March 19, 2019, when the executive completed his overdue training.</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 risk posed by allowing someone access into a PSP without having completed the required training is that the individual could unintentionally cause harm to the BPS. The risk is minimized because the individual involved was a trusted employee in good standing with the entity that had previously completed training. Additionally, there was a short duration as a result of the entity self-identifying the noncompliance, thus reducing the period of time during which there was the potential for harm. ReliabilityFirst also notes that the executive did not use his ID card to enter any NERC PSPs during the noncompliance. 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) had the executive complete his overdue [REDACTED] training; 2) completed corrective counseling for the IT personnel who made the identified errors to pay greater attention to detail and not rush through work tasks; and 3) retrained the IT personnel who made the identified errors and the team's manager or senior manager of the team observed 12 verification tasks performed by the person to ensure that the training was effective. (The IT personnel who made the identified errors accepted a job in another area of the company prior to the full completion of the 12 monitored training verifications. Eight verification tasks were completed.) 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021403	CIP-004-6	R2	[REDACTED]	[REDACTED]	2/12/2019	3/19/2019	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 April 22, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R2.</p> <p>On March 18, 2019, as a part of a training-completion audit, the entity identified one instance where an individual was granted access before completing the required training. More specifically, on February 12, 2019, the entity granted a [REDACTED] executive access to a NERC Physical Security Perimeter (PSP) before the executive completed his [REDACTED] training. The executive had previously taken this training, but his training was no longer current. The executive did not enter any NERC PSPs after the entity granted him access and before he completed his [REDACTED] training on March 19, 2019.</p> <p>Regarding the root cause, the entity determined that the Information Technology (IT) [REDACTED] [REDACTED] misread the training record and incorrectly concluded that the executive's physical access training had been completed. The IT [REDACTED] [REDACTED] had been recently trained in the verification process and this was among the first reviews he completed on his own without mentoring. Upon discovery of this issue, the entity reassigned the training immediately and the executive completed the training one day later on March 19, 2019.</p> <p>This noncompliance involves the management practices of workforce management, validation, and verification. The root cause is ineffective training as the IT [REDACTED] [REDACTED] was not effectively trained on how to complete the job. Another contributing cause is a lack of effective verification controls.</p> <p>This noncompliance started on February 12, 2019, when the entity granted a [REDACTED] executive access to a NERC PSP before he completed his training and ended on March 19, 2019, when the executive completed his overdue training.</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 risk posed by allowing someone access into a PSP without having completed the required training is that the individual could unintentionally cause harm to the BPS. The risk is minimized because the individual involved was a trusted employee in good standing with the entity that had previously completed training. Additionally, there was a short duration as a result of the entity self-identifying the noncompliance, thus reducing the period of time during which there was the potential for harm. ReliabilityFirst also notes that the executive did not use his ID card to enter any NERC PSPs during the noncompliance. 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) had the executive complete his overdue [REDACTED] training; 2) completed corrective counseling for the IT personnel who made the identified errors to pay greater attention to detail and not rush through work tasks; and 3) retrained the IT personnel who made the identified errors and the team's manager or senior manager of the team observed 12 verification tasks performed by the person to ensure that the training was effective. (The IT personnel who made the identified errors accepted a job in another area of the company prior to the full completion of the 12 monitored training verifications. Eight verification tasks were completed.) 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021424	CIP-004-6	R5	[REDACTED]	[REDACTED]	3/29/2019	4/1/2019	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 April 30, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5.</p> <p>On Friday, March 29, 2019, a [REDACTED] Buyer at the entity completed his final day of employment (voluntary departure). The employee, who had previously been granted NERC unescorted physical access rights, surrendered his employee identification (ID) cards to his supervisor at the end of his shift.</p> <p>On Monday, April 1, 2019, the supervisor turned the aforementioned employee ID cards in to entity Corporate Security personnel. Corporate Security personnel immediately revoked both corporate and NERC access rights and processed the related NERC revocation workflow. While the entity confiscated the employee's ID cards upon termination, the entity did not revoke the access rights associated with those cards within 24 hours as required.</p> <p>The entity performed an investigation to determine the causes of this noncompliance. The employee's supervisor submitted the corporate form used for revocation of card reader access on March 18, 2019; however the supervisor failed to indicate that revocation from NERC systems was necessary on that form. On March 20, 2019, an entity Corporate Security e-mailbox received a termination report; however Corporate Security personnel monitoring the mailbox did not realize that one of the employees being terminated had NERC access which required revocation. Additionally, specific notices indicating the employee was being terminated were emailed to a Corporate Security group email box on March 22, 2019 and March 29, 2019, were not acted upon.</p> <p>This noncompliance involves the management practices of work management and reliability quality management. The root cause was an error on the part of the supervisor in filling out the form in addition to an ineffective work management process that allowed for reminders and internal controls to not be acted upon which resulted in delayed access revocation.</p> <p>This noncompliance started on March 29, 2019, when the entity was required to revoke the employee's access rights associated with his ID cards within 24 hours as required and ended on April 1, 2019, when the entity completed revoking all of the employee's 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 based on the following factors. The risk posed by this noncompliance is allowing an unauthorized individual to retain access to Bulk Electric System Cyber Systems. The risk is minimized because the employee at issue voluntarily left the company on good terms. The entity confiscated the employee's ID cards on March 29, 2019 at the end of the employee's last shift. During the entire duration of this noncompliance, the employee's supervisor (who has also been granted unescorted physical access to NERC Physical Security Perimeters (PSPs)) [REDACTED] Lastly, the entity confirmed that the employee's ID cards were not utilized during this time period to access (or attempt to access) any NERC PSPs after the employee's termination. 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) assigned additional resources to monitor the Corporate Security group email box; 2) provided an extract of personnel with access to NERC CIP Physical Security Perimeters to the NERC CIP Compliance Team weekly for comparison to the termination/retirement report; 3) completed corrective counseling for the terminated employee's supervisor with respect to proper corporate revocation form completion; 4) required the terminated employee's supervisor to retake the NERC Supervisor training course; 5) completed corrective counseling for the Corporate Security personnel who failed to act upon multiple notices of upcoming termination; 6) implemented automated daily monitoring of physical access rights against reported HR changes; and 7) updated the [REDACTED] "Offboarding Checklist" to identify a single method of requesting NERC access revocation regardless of company affiliation. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017674	CIP-004-6	R3, P3.4	[REDACTED]	[REDACTED]	03/22/2017	04/05/2017	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 June 1, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R3, P3.4. The Entity had one instance where it granted a contractor unescorted physical access to one Physical Security Perimeter (PSP) without a valid personnel risk assessment (PRA) on file.</p> <p>On April 5, 2017, an Entity access approver received an email from a construction supervisor noting that a contractor who had worked on and currently assigned to Entity projects had recently switched employers. The contractor worked on projects for the Entity prior to the change in employers, but did not work on CIP sites and had no authorized unescorted physical access permissions. The receipt of the email prompted the access approver to call the construction supervisor. During the call, it was discovered that the Entity access approver had erroneously granted the contractor unescorted physical access permissions. Although the contractor had also been assigned to Entity projects by the new employer, the PRA on file for the contractor was with the previous employer and not the current employer that was referenced in the Corporate Security records. That same day, the Entity revoked the contractor's physical access. The contractor never accessed any CIP PSP.</p> <p>[REDACTED]</p> <p>The Entity conducted an extent-of-condition assessment by reviewing PRAs for a sample of nine contracted individuals. The Entity found no additional instances of noncompliance.</p> <p>This noncompliance started on March 22, 2017, when the Entity granted physical access to a contractor who did not have a valid PRA on file, and ended on April 5, 2017, when the Entity revoked physical access from the contractor.</p> <p>The root causes of this noncompliance were the absence of sufficient training and an insufficient internal control to ensure successful completion of required Human Resources (HR) paperwork for the contractor. Specifically, the Entity did not complete the termination paperwork upon the contractor's switch to the new employer and the Entity did not ensure that a letter of verification of completion of a PRA with the new employer was on file for the contractor.</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 Entity's failure to verify that a valid PRA was on file for a contractor could allow an unauthorized individual to physically access BCSs, resulting in the misuse or compromise of such systems. However, in this instance, the contractor's PRA associated with a previous employer would have been acceptable had the contractor not changed employers. Additionally, the contractor had physical access only and did not possess electronic access privileges to BCAs. Moreover, the Entity protected the BCAs with the remaining CIP-005 and CIP-007 provisions, including real-time monitoring for configuration changes. 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) revoked the contractor's access badge; 2) enhanced its unescorted access request procedure to include contractor and vendor employment confirmation as an internal control; 3) provided reinforcement training with the administrative staff who failed to follow the termination process in this instance that all HR documentation for contractors must be completed within 24 hours upon notification of termination; 4) retrained the [REDACTED] team on the NERC requirements; and 5) sampled nine contractor records to confirm that contractors have a valid PRA associated with their current employer. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017017004	CIP-007-6	R5; Part 5.3	[REDACTED]	[REDACTED]	7/1/2016	2/3/2017	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 a February 13, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5, Part 5.3. The Entity did not identify individuals who have authorized access to a shared account because it stored passwords in an unsecured file.</p> <p>On October 24, 2016, during a discussion with the managerial staff of the [REDACTED] team, IT Security discovered that that the [REDACTED] team was storing shared passwords to the [REDACTED] Remote Terminal Units (RTUs) in an unencrypted spreadsheet on the [REDACTED] file share. The Entity changed the passwords to the BES Cyber Asset and encrypted the worksheet the same day it discovered the noncompliance.</p> <p>On February 3, 2017, while in discussions with [REDACTED] IT Security discovered that [REDACTED] was storing a password on a hand written note at a [REDACTED] Workstation. IT Security confirmed this on the same day and informed the dispatcher that writing down secure passwords and keeping them in plain sight, even within the Physical Security Perimeter (PSP), did not follow the access management standards portion the Entity's Cyber Security Policies. The Entity changed the password the same day.</p> <p>This noncompliance started on July 1, 2016, when the Standard became enforceable and the Entity did not identify individuals who have authorized access to a shared account by storing passwords in an unsecured file and ended on February 3, 2017 when the shared passwords were properly secured for access by authorized individuals.</p> <p>The cause of the noncompliance was deficient controls surrounding its process. In both instances, the Entity lacked controls to ensure that its manual process was followed.</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>The Entity's failure to properly secure shared passwords could have allowed an unauthorized individual to gain access to an RTU. However, the shared passwords provide access only from within the ESP and did not provide remote access. Further, the system access allowed limited generation control.</p> <p>No actual harm is known to have occurred.</p> <p>SERC considered the Entity's compliance history and determined 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) changed the shared password in the first instance and moved it to a secure location within the CIP network; 2) changed the password in the second instance and removed the notepad containing the password; and 3) created and completed a project that incorporated software to manage shared accounts and provided training on the use of the software. This software replaced encrypted spreadsheets with a team password application to make sharing passwords more secure. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017017795	CIP-007-6	R2; Part 2.3	[REDACTED]	[REDACTED]	5/30/2017	5/31/2017	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 June 24, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2, Part 2.3. The Entity failed to complete its internal paperwork related to a security patch mitigation plan within 35 calendar days of the patch's evaluation completion for three patches.</p> <p>On April 24, 2017, the Entity [REDACTED] evaluated security patches for [REDACTED] Microsoft vulnerabilities. The patches applied to [REDACTED] Intermediate Systems and [REDACTED] Protected Cyber Assets. At the time of the evaluation, the [REDACTED] decided to patch the Cyber Assets, which created the 35-calendar day deadline for patch installation or a mitigation plan to be in place.</p> <p>Although the [REDACTED] responsible for managing security vulnerabilities had agreed on the mitigation actions that were to be taken and the initial mitigation actions had actually taken place, the mitigation plan paperwork was not completed until May 31, 2017, two days past the 35-calendar day required timeframe. Independent from this mitigation plan process, the Entity applied the patches the same day.</p> <p>This noncompliance started on May 30, 2017, when the Entity did not apply the evaluated patches or document a patch mitigation plan and ended on May 31, 2017 when the patch mitigation plan was completed and the patches were installed.</p> <p>The cause of the noncompliance was lack of an internal control, which then allowed a process failure in timely completing the Entity's relevant mitigation plan paperwork.</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 Entity's failure to document a patch mitigation plan as required could have resulted in a known vulnerability being exploited and potentially compromising the unpatched Cyber Assets impacting the BPS. However, even though the patch mitigation plan was not formally completed, actions to mitigate risk by monitoring and alerting on potential exploits to the vulnerabilities using the [REDACTED] had been implemented on May 24, 2017. [REDACTED] reporting showed that no threats were detected during the timeframe in question. Furthermore, the [REDACTED] unpatched vulnerabilities required manual input from a user visiting a potentially compromised website. Due to lack of activity on these Cyber Assets for any web browsing functionality, the risk of exposure to this vulnerability was virtually eliminated. Lastly, the actual application of the patches was only two days beyond the required implementation date.</p> <p>No harm is known to have occurred.</p> <p>SERC considered the Entity's compliance history and determined there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> retrained [REDACTED] on the CIP-007 R2.3 requirement with emphasis on the requirement that, if the action taken is to create a dated mitigation plan, the plan must be created within 35 calendar days of the evaluation completion; and added internal control to set up calendar task reminders to individuals responsible for creating the mitigation plan. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018097	CIP-007-6	R3, P3.3	██████████ (██████)	██████████	07/01/2016	08/11/2017	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 violation.)			<p>On August 2, 2017, the Entity submitted a Self-Report to SERC stating that, as a ██████████, it was in noncompliance with CIP-007-6 R3, P3.3. The Entity did not have an implemented process to update malicious code signatures.</p> <p>On August 1, 2017, the Entity’s IT Staff discovered that its firewall outbound connection to its vendor’s malicious code signature update was blocked and the Entity was not receiving its signature updates. The Entity’s IT Staff checked the firewall logs, which revealed that the blocked outbound connection attempts were initiated by the firewall to the firewall vendor. On August 9, 2017, the Entity’s IT Staff corrected the blockage and tested the signature updates. On August 11, 2017, the Entity’s IT Staff installed the missing signature updates.</p> <p>The Entity conducted an extent-of-condition and discovered that its ██████████ engine signature updates were not included in the patch management process its IT Staff had been using. The Entity discovered a total of ██████ Entity assets that relied on the ██████████ for the prevention of malicious code, but were not updated.</p> <p>This noncompliance involved ██████ Electronic Security Perimeters (ESPs) associated with ██████ medium impact Bulk Electric System (BES) Cyber Systems that contained ██████ BES Cyber Assets (BCAs), ██████ Protected Cyber Assets (PCAs), ██████ Electronic Access Control Monitors (EACMSs), and ██████ Physical Access Control Systems (PACs).</p> <p>This noncompliance started on July 1, 2016, when the standard became mandatory and enforceable, and ended on August 11, 2017, when the Entity installed the missing signature updates on its ██████████ engine.</p> <p>The root cause of this noncompliance was procedural deficiency. The Entity’s IT department assumed that, at the time of deployment, its firewall could reach the vendor’s site to download signature updates, however, the procedure did not require the IT department to verify that the signatures were successfully downloaded.</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 Entity’s failure to update its signatures on its ██████████ created an increased potential for the execution of malicious code, unknown to the ██████████ engine, thereby creating potential risk to the BPS. However, the Entity segmented its network such that the systems running its EMS are on its own network separate from those of the infrastructure support systems and operator workstations. Also, the Entity installed firewall rules to restrict the ingress and egress traffic to only allow that which is necessary. No harm is known to have occurred.</p> <p>SERC determined that the Entity’s CIP-007-6 R3 compliance history should not serve as a basis for aggravating any penalty. The Entity’s relevant prior noncompliance involves one relevant instance of noncompliance. The underlying cause of the prior and instant noncompliance is different. The prior noncompliance was due to inexperience staff implementing the new standard, and the entity discovered the instant noncompliance while in the process of implementing mitigation for the prior noncompliance.</p>					
Mitigation			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none"> 1) verified access of the firewall to the vendor for signature downloads; 2) downloaded and installed the latest signature updates; 3) updated its patch management process documentation to include the testing and installation of ██████████ signatures; and 4) trained affected staff on the updated patch management program. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2019021664	CIP-010-2	R4	[REDACTED] (the Entity)	[REDACTED]	04/01/2017	10/10/2019	Audit	11/18/2019
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>During a Compliance Audit conducted from [REDACTED] SERC determined that the Entity, as a [REDACTED] was in noncompliance with CIP-010-2 R4. The Entity allowed a third-party consultant to use a Transient Cyber Asset (TCA) to connect to Cyber Assets but its documented plan for TCAs did not authorize third-party consultants to use TCAs.</p> <p>On March 3, 2017, the Entity updated its change management procedure with specific requirement language for TCAs and RM, and in the process, omitted process and procedures for third party TCAs. In addition, the Entity failed to detect the omission when it implemented its TCA process and procedures on CIP-010-2 R4's phased-in implementation date of April 1, 2017.</p> <p>Since April 1, 2017, there was one instance where the Entity permitted a consultant to use a laptop with only needed and freshly installed software, in order to perform a Vulnerability Assessment. The Entity employee and the consultant did not connect the laptop to any network between its fresh install and the time it was used to conduct the assessment. Physical access to the laptop was restricted to the consultant and the authorized employee, who was constantly present while the consultant connected the TCA to the Cyber Assets. For the Entity's extent-of-condition, SERC auditors reviewed the process and procedure documentation and found no other instances of omission.</p> <p>This noncompliance started on April 1, 2017, when the standard became mandatory and enforceable, and ended on October 10, 2019, when the Entity updated its TCA process and procedures regarding third parties.</p> <p>SERC determined the root cause to be lack of awareness as the Entity did not detect the omission of third party TCAs in the procedure, and then permitted a third party to use a TCA.</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 (BPS). The Entity's lack of a documented procedure for securing TCAs of third parties from possible compromise or corruption, could lead to a situation where a contractor could plug a compromised device into the BCS and infect the BCS network, which could ultimately compromise the BPS. However, the Entity only had one instance where a TCA, managed by another party, was used. The consultant was retained by the Entity to perform a Vulnerability Assessment, and did so in the presence of an Entity employee. 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 will complete the following mitigation activities by November 18, 2019:</p> <ol style="list-style-type: none"> 1) inform all applicable departments not to allow any third parties to use its TCAs on its BCS until the Entity updates its TCA process and procedure regarding third parties; 2) modify the CIP-010 documented process to address TCAs managed by a third party, which will include collecting evidence to demonstrate software vulnerabilities mitigation, malicious code mitigation, and any additional mitigation actions necessary; and 3) train employees on the updated process and procedures. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018610	CIP-003-6	R2	██████████	██████████	04/02/2017	06/23/2017	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 violation.)			<p>On November 8, 2017, the Entity submitted a Self-Report to SERC stating that, as a ██████████, it was in noncompliance with CIP-003-6 R1, P1.2. The Entity did not test its ██████████ prior to the implementation date of the Standard and Requirement. SERC later determined that the Entity was in noncompliance with CIP-003-6 R2, not CIP-003-6 R1.</p> <p>On April 1, 2017, when CIP-003-6 R2 became effective, the Entity was required to test, or already have tested, its ██████████. However, the Entity and its parent company, ██████████, misinterpreted the Standard and believed that it had 36 months from the effective date to test its ██████████. The Entity discovered that it failed to test its ██████████, in accordance with the required timeframe, on June 2, 2017.</p> <p>On June 23, 2017, the Entity tested its ██████████, for the first time, by performing a ██████████ table top exercise that involved a possible Ransomware attack against both business and ██████████ networks. In addition to the table top exercise, the Entity participated in NERC's 2017 GridEX exercise.</p> <p>The extent-of-condition consisted of the Entity, and its parent company, participating in NERC's 2017 GridEX exercise to better understand the CIP standard requirements. The Entity also had its ██████████ attend industry conferences, webinars and other learning opportunities to make sure that the Entity had no other areas of misinterpretation in regard to its CIP requirements. The Entity found no other instances of misinterpretation of its CIP-003-6 R2 requirements.</p> <p>This noncompliance started on April 2, 2017, when the Entity was required to have tested its ██████████, and ended on June 23, 2017, when the Entity tested its ██████████.</p> <p>The root cause of this noncompliance was the Entity's misunderstanding of the CIP-003-6 R2 timeframe required to test its ██████████.</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 Entity's failure to test its ██████████ created an increased potential for the Entity's ██████████ to not function as intended, during an actual cyber incident, thereby creating potential risk to the BPS. However, the Entity completed its test by performing a cyber security table top exercise that involved a possible Ransomware attack against both business and ██████████ networks during the same month that it discovered its misinterpretation of the CIP standard, which was 83 days after the required due date.</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) completed testing via a table top exercise; 2) updated the CIP-003-6 R2 procedure to clearly indicate that testing is to be done every 36 months; 3) created recurring pre-scheduled work orders by using work planning software for the CIP-003 required scheduled testing every 36 months deadline, with key stakeholders; 4) participated in the NERC GridEX event for 2017; and 5) trained key stakeholders responsible for testing the ██████████ on the updated CIP-003-6 R2 required procedure (evidence of review indicated via sign-off). 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017710	CIP-010-2	R1, P1.1, P1.1.1	██████████ (████)	██████████	07/01/2016	03/10/2017	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 June 7, 2017, the Entity submitted a Self-Report stating that, as a ██████████, it was in noncompliance with CIP-010-2 R1, P1.4. SERC determined that this issue was more appropriately addressed under CIP-010-2 R1, P1.1, P1.1.1. The Entity failed to develop an accurate baseline configuration.</p> <p>The manufacturer for the firmware utilized by the Entity's switches added the capability to disable web access. With the new feature at its disposal, the Entity had opted to disable web access on all in-service and new switches in order to harden cyber defenses. However, while field instructions for installing the firmware on existing devices contained steps for disabling web access, instructions for installing new switches did not contain steps for disabling web access. On March 7, 2017, the Entity's ██████████ (Staff) discovered an inconsistency while comparing a switch's intended documented baseline configuration with its actual configuration. Specifically, Staff found web access enabled on a switch, but the documented baseline configuration indicated it was disabled.</p> <p>The scope of affected facilities included ██████ medium impact Bulk Electric System (BES) Cyber Systems (BCSs) comprising of ██████ BES Cyber Assets (BCAs) and ██████ Protected Cyber Assets.</p> <p>The Entity conducted an extent-of-condition assessment by reviewing new installation asset records for its switches - beginning with the date the manufacturer changed firmware, which was sometime in May of 2016. The Entity discovered a total of ██████ affected switches. On March 10, 2017, to rectify the noncompliance, the Entity updated baseline configuration documentation for the ██████ affected switches to reflect web access enabled.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on March 10, 2017, when the baseline documentation was updated to reflect the enabling of the web access on the ██████ affected switches.</p> <p>The root cause of this noncompliance was a procedural deficiency and lack of an internal control. The Entity's procedure did not include instructions for disabling web access for newly installed switches. Additionally, the Entity did not require a verification review of intended and actual baseline configurations for newly commissioned BCAs to ensure an accurate baseline configuration.</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 Entity's failure to accurately document and track changes that deviate from existing baseline configurations increased the risk that the Entity would not identify unauthorized changes, which could adversely impact BCSs. However, the devices were firmware-based Cyber Assets, which greatly reduced modifications or compromise. Additionally, the affected Cyber Assets did not possess External Routable Connectivity and were protected with Electronic and Physical Access Controls and Monitoring. No harm is known to have occurred.</p> <p>The Entity's has one prior noncompliance with CIP-010-2 R1. SERC determined that the Entity's CIP-010-2 R1 compliance history should not serve as a basis for aggravating any penalty. The prior instance of noncompliance was ten years ago and before a CIP program overhaul was required by CIP Version 5.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) performed the extent-of-condition assessment, which revealed that there was a total of ██████ switches impacted; 2) created a baseline configuration to include web access for the ██████ switches impacted to bring the Entity immediately back into compliance with CIP-010-2 R1; and 3) updated the turn-up instructions and provided the instructions to telecom field personnel to ensure web access and other services were checked on future switch installs. The updated turn-up instructions included a verification review of baseline configurations for newly commissioned BCAs as an internal control. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019615	CIP-006-6	R1; R1.3	[REDACTED] (the "Entity")	[REDACTED]	07/01/2016	03/13/2017	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 [REDACTED] the Federal Energy Regulatory Commission (FERC) determined the Entity, as a [REDACTED] was in noncompliance with CIP-006-6 R1. Specifically, the Entity's documented physical plan did not document the [REDACTED] physical access controls in use for one of the Entity's Control Centers. FERC stated that this noncompliance would be processed by Texas RE in accordance with the North American Electric Reliability Corporation Inc.'s (NERC) Rules of Procedure.</p> <p>During the noncompliance, the Entity's documented physical security plan did not document that [REDACTED] were used, in addition to another physical access control, as the Entity's [REDACTED] physical access control for the Entity's [REDACTED] Control Center, which is associated with [REDACTED] BES Cyber System. Instead, the documented physical security plan erroneously stated a [REDACTED] was the [REDACTED] physical access control used for the [REDACTED] Control Center. In addition, the Compliance Audit determined that [REDACTED] were in the possession of individuals who were no longer employed by the Entity. However, the Entity stated that, using a separate access control, the Entity had revoked the authorization for physical access by any individual that still possessed [REDACTED], meaning that such an individual would not have the capability to obtain unauthorized access.</p> <p>On March 13, 2017, the Entity ended the noncompliance by documenting the [REDACTED] as an access control. Subsequently, the Entity further addressed this issue by replacing the use of [REDACTED] with a different physical access control.</p> <p>The root cause of this issue is that the Entity's documentation did not fully describe its process. Specifically, the Entity's documented physical security plan accurately described the physical access controls for the Entity's primary Control Center, but the document omitted details specific to the [REDACTED] Control Center.</p> <p>This noncompliance started on July 1, 2016, when CIP-006-6 became enforceable, and ended on March 13, 2017, when the Entity revised its documented physical security 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. This issue affected a backup Control Center that is associated with a [REDACTED] BES Cyber System. The risk posed by this issue is increased by the fact that the [REDACTED] Control Center can be used to control the Entity's [REDACTED], with combined nameplate ratings of approximately [REDACTED], and the Entity's [REDACTED] of [REDACTED]. However, this issue was limited to the Entity's documentation only. In particular, although the Entity's documented physical security plan did not accurately identify the [REDACTED] physical access controls in use at the Control Center, the Entity did have [REDACTED] physical access controls in place. Finally, the Entity did not detect any unauthorized access to its BES Cyber Systems relating to these issues. No harm is known to have occurred.</p> <p>Texas RE 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) revised the documented physical security plan to reflect the use of [REDACTED] as a physical access control at the backup Control Center; 2) [REDACTED]; and 3) [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
TRE2018019619	CIP-007-6	R1; R1.1	██████████ (the "Entity")	██████████	07/01/2016	03/03/2017	Compliance 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 violation.)			<p>During a Compliance Audit conducted ██████████, the Federal Energy Regulatory Commission (FERC) determined that the Entity, as a ██████████, was in noncompliance with CIP-007-6 R1. Specifically, the Entity did not enable only logical network accessible ports that have been determined to be needed by the Entity. FERC stated that this noncompliance would be processed by Texas RE in accordance with the North American Electric Reliability Corporation Inc.'s (NERC) Rules of Procedure.</p> <p>The root cause of this issue is that the script used by the Entity to detect and document its devices' enabled ports had a flaw that caused the script to fail to detect enabled ports using a certain protocol. As a result, for ██████ devices located in ██████ Control Centers, the undetected ports were not included in the Entity's port justification documentation.</p> <p>This noncompliance started on July 1, 2016, when CIP-007-6 R1 became enforceable, and ended on March 3, 2017, when the Entity documented justifications for the ports 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. The risk posed by this issue is that enabling logical networks accessible ports that are not determined to be needed may increase the risk that a BES Cyber System will be compromised. This issue affected ██████ Cyber Assets, comprising ██████ BES Cyber Assets, ██████ Physical Access Control System, ██████ Electronic Access Control or Monitoring Systems, and ██████ Protected Cyber Assets, which are associated with ██████ Control Centers that are each associated with a ██████ BES Cyber System. The risk posed by this issue is increased by the fact that the ██████ Control Center can be used to control the Entity's ██████████, with combined nameplate ratings of approximately ██████████, and the Entity's ██████████. However, the risk posed by this issue was reduced by the following factors. First, this issue was limited to the Entity's documentation only. In particular, although the Entity did not document the justifications for certain enabled ports, the ports at issue only permit communication within the ESP. Second, after the Entity documented the justifications for the ports at issue, all of the ports at issue were determined to be needed and were not required to be disabled. Third, during the noncompliance, the Entity conducted monthly reviews of active services and disabled services that were not needed. Finally, the Entity did not detect any unauthorized access to its BES Cyber Systems relating to these issues. No harm is known to have occurred.</p> <p>Texas RE 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 justifications for the ports at issue; and 2) corrected the error in the script used for documenting the justifications for enabled ports. <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
TRE2018019808	CIP-007-6	R2; R2.1	[REDACTED] the "Entity")	[REDACTED]	11/10/2017	05/01/2018	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 violation.)			<p>On June 4, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-007-6 R2. In particular, the Entity did not identify a source or sources that the Entity tracks for the release of cyber security patches for applicable Cyber Assets for certain software, as required by CIP-007-6 R2, Part 2.1.</p> <p>On November 10, 2017, the Entity installed new monitoring software on one device, which performs monitoring functions for the Entity's [REDACTED] Control Centers. However, the Entity did not include a patch source for the monitoring software in its patch source list, as required by CIP-007-6 R2, Part 2.1. On May 1, 2018, the Entity discovered this issue, and, on May 2, 2018, the Entity updated its source list, ending the noncompliance. The Entity further confirmed that it applied all outstanding cyber security patches for the software at issue.</p> <p>The root cause of this issue is an insufficient change management process for installing new software on the Entity's applicable Cyber Assets. In particular, to address this noncompliance, the Entity revised the forms that it uses as part of its change management process to prompt personnel to determine if a patch source for the new software should be included in the Entity's patch source list.</p> <p>This noncompliance started on November 10, 2017, when monitoring software was installed without updating the Entity's source list, and ended on May 3, 2018, when the Entity updated its source list and applied all outstanding cyber security patches for the software 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 based on the following factors. As a result of the noncompliance, for approximately six months, the Entity failed to evaluate or apply cyber security patches for the monitoring software installed on a single device that performs monitoring functions for [REDACTED] Control Centers that are each associated with a [REDACTED] BES Cyber System. The risk posed by this issue is increased by the fact that the Entity's Control Centers can be used to control the Entity's [REDACTED] Facilities, with combined nameplate ratings of [REDACTED], and the Entity's [REDACTED] Facilities. However, the risk posed by this issue is reduced by the following factors. First, the software and the device that it was installed on are used only for monitoring purposes and do not have the ability to control the Entity's network or Bulk Electric System Elements. The software and device monitor and communicate with devices inside the Entity's Electronic Security Perimeter (ESP), but they do not communicate outside of the ESP. Second, although the Entity identified [REDACTED] outstanding cyber security patches when it ended the noncompliance, the Entity confirmed that none of the [REDACTED] patches was critical to the security of the Entity's BES Cyber Systems. No harm is known to have occurred.</p> <p>Texas RE 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) updated its source list; and 2) revised the form for its change management process to prompt personnel to determine if a patch source for new software should be included in the Entity's patch source list. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019021442	CIP-004-6	R2.3	[REDACTED] (the "Entity")	[REDACTED]	11/01/2018	01/14/2019	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 26, 2019, the Entity submitted a Self-Log stating that, as [REDACTED], it was in noncompliance with CIP-004-6 R2.3. In particular, the Entity is unable to demonstrate that it required the completion of training specified in CIP-004-6 R2.1 at least once every 15 calendar months for one user.</p> <p>The root cause of this noncompliance was insufficient detective controls for a subset of users. The Entity [REDACTED] and carried forward the training dates of the users. The user affected by this noncompliance had not taken CIP-004-6 R2.1 training through the Entity's CIP compliance program. The Entity has performed a spot check to ensure that no other users [REDACTED] are at risk of having their training expire.</p> <p>This noncompliance started on November 1, 2018, which is the first day after 15 calendar months had elapsed since the user completed training and ended on January 14, 2019, when the user completed training.</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 duration of the noncompliance was relatively short, lasting 75 days. The employee in question did not have electronic access to BES Cyber Systems, their need for training was due to having physical access to BES Cyber Systems. The employee did access the Entity's Control Center during the noncompliance period, however the Entity determined that the access was due to valid business justifications. No harm is known to have occurred.</p> <p>Texas RE determined that the entity's CIP-004-6 R2 compliance history should not serve as a basis for aggravating the penalty due to the amount of time between instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance:</p> <ol style="list-style-type: none"> 1) the Entity had the affected user complete the training specified in CIP-004-6 R2.1; and 2) the Entity implemented a control to provide a three month warning before annual training is due. <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
TRE2018019892	CIP-002-5.1	R1; 1.3	██████████ ("the Entity")	██████████	07/01/2016	07/31/2018	Compliance 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 violation.)			<p>During a Compliance Audit conducted from ██████████, Texas RE determined that the Entity, as a ██████████ was in noncompliance with CIP-002-5.1, R1. Specifically, the Entity had failed to categorize its Inter-Control Center Communication Protocol (ICCP) servers as part of a ██████████ BES Cyber System, believing that ICCP assets were not critical to the ability for the Entity to perform Real-time monitoring.</p> <p>The root cause of the noncompliance was insufficient expertise within the organization regarding knowledge of proper categorization of assets.</p> <p>This noncompliance started on July 1, 2016, when the standard became effective, and ended on July 31, 2018, when the Entity categorized its ICCP as a Cyber Asset.</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 identify assets correctly could potentially result in a loss, compromise, or misuse of BES Cyber Systems. However, the Entity has a relatively ██████████ and the Entity's ICCP Cyber Assets were secured within a DMZ. Additionally, the Entity stated that loss of ICCP data would not prevent the Entity from monitoring its system and performing its function as a ██████████. Because of the Entity's transmission and interconnection in ERCOT, ██████████</p> <p>██████████ Finally, the Entity states that even though the Entity did not include the ICCP servers as BES Cyber Assets, the Entity was still maintaining them in accordance with a large majority of the CIP Standards (patching, recognizing baseline changes, performing security event monitoring, controlling both electronic and physical access, etc.). No harm is known to have occurred.</p> <p>Texas RE 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) has categorized its ICCP as a BES Cyber Asset; and 2) underwent an organizational restructuring to improve the Entity's compliance process and managerial-level expertise. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019021289	CIP-004-6	R5.5	██████████ ██████████) ("the Entity")	██████████	03/15/2019	03/19/2019	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 March 28, 2019, the Entity submitted a Self-Report stating that, as a ██████████) it was in noncompliance with CIP-004-6, R5. Specifically, the Entity terminated an employee on February 12, 2019, and did not change passwords for shared account(s) known to the user within 30 calendar days of the termination action.</p> <p>The root cause of the noncompliance was a failure to follow the Entity's procedure whereby passwords were to be changed immediately following an employee's termination: the ██████████ had sought to streamline the process by changing passwords in the calendar month following the calendar month an employee was terminated, which would not necessarily fall within the required 30-day deadline required by the standard.</p> <p>This noncompliance started on March 15, 2019, the 31st day after the employee had been terminated, and ended March 19, 2019, when the Entity changed all passwords of shared accounts known to the terminated employee.</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. A failure to change passwords could allow an individual to have unauthorized access that could be used to compromise the physical security of BES Cyber Systems, and ultimately impact the reliability and security of the bulk power system, if that individual also had physical or remote access to facilities. However, the terminated employee had no physical or remote access, which would be required to use ██████████ known by the terminated employee. Additionally, all employees were notified immediately upon termination, lessening the likelihood that the terminated employee would gain physical access by piggybacking into a facility. Finally, the duration of the noncompliance was relatively short at four days. No harm is known to have occurred.</p> <p>Texas RE 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) changed all passwords of shared accounts known to the user, ending the noncompliance; and 2) reviewed with applicable employees that passwords are to be changed immediately as part of the termination 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
WECC2017017509	CIP-005-5	R1; P1.1	[REDACTED]	[REDACTED]	7/1/2016	8/28/2017	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 April 28, 2017, the entity submitted a Self-Report stating, as a [REDACTED], it was in noncompliance with CIP-005-5 R1. Specifically, during the updating of its Interactive Remote Access (IRA) methodology and architecture, it identified [REDACTED] Bulk Electric System (BES) Cyber Assets (BCAs) associated with its Medium Impact BES Cyber System (MIBCS), within both the primary and backup Control Centers, that were not located within a defined Electronic Security Perimeter (ESP) as required by R1 Part 1.1. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on April 28, 2017, when the entity placed the BCAs within an identified ESP, for a total of 302 days.</p> <p>The root cause of the issue was attributed to the entity not understanding what was required for compliance with the Standard and Requirements. Specifically, the entity believed a virtual local area network separation was adequate for an ESP, which was how the entity had initially set up the network for the BCAs in scope. Additionally, the entity had insufficient manpower to support its compliance obligations.</p>					
Risk Assessment			<p>WECC determined 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, the entity failed to adequately implement a documented process that included CIP-005-5 R1 Part 1.1 for [REDACTED] BCAs, as described above.</p> <p>These failures could have led to unauthorized access to BES Cyber Systems, potentially compromising critical operational systems within the Control Centers and affecting the reliability of the BPS. However, as compensation, the entity afforded the seven BCAs the same protective measures of the standards as it did to the Cyber Assets within the ESP, that is, they were in a Physical Security Perimeter, had enabled firewalls, system-level malicious code prevention and monitoring, access management at the application and operating system levels; monitoring of security logs and alerting, and application whitelisting on the local machines. Additionally, single factor authentication was required to access the BCAs which was restricted to individuals with personnel risk assessments and CIP training and the BCAs do not directly affect the production environment as they are part of the entity's development environment. Finally, IRA was limited to sessions initiated from the entity's network segments dedicated to supervisory control and data acquisition support. No harm is known to have occurred.</p> <p>WECC notes that the entity does not have any previous violations of this or similar Standards and Requirements.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) placed the BCAs in scope behind an EAP and created a new ESP network segment; 2) implemented a new workflow platform where all change requests, including the commissioning of new Cyber Assets, will flow through, ensuring that Cyber Assets classified as BCSs will be placed inside an ESP; and 3) contracted with a third party vendor to augment its compliance staffing issues, address education, and mature its compliance program to ensure future compliance. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017510	CIP-005-5	R2; P2.1; P2.2, P2.3	[REDACTED]	[REDACTED]	7/1/2016	8/28/2017	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 April 28, 2017, the entity submitted a Self-Report stating, as a [REDACTED], it was in noncompliance with R2. Specifically, during the updating of its Interactive Remote Access (IRA) methodology and architecture, it identified [REDACTED] Bulk Electric System (BES) Cyber Assets (BCAs) associated with its Medium Impact BES Cyber System (MIBCS), within both the primary and backup Control Centers, that were not located within a defined Electronic Security Perimeter (ESP) as required by R1 Part 1.1. As such, and because the BCAs had External Routable Connectivity (ERC), the entity failed Part 2.1 for not utilizing an Intermediate System (IS) such that any Cyber Asset initiating IRA did not directly access the affected BCAs, Part 2.2 for not utilizing encryption that terminated at an IS, and Part 2.3 for not requiring multi-factor authentication for all IRA sessions to the BCAs. This issues began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on April 28, 2017, when the entity placed the BCAs within an identified ESP, for a total of 302 days.</p> <p>The root cause of the issue was attributed to the entity not understanding what was required for compliance with the Standard and Requirements. Specifically, the entity believed a virtual local area network separation was adequate for an ESP, which was how the entity had initially set up the network for the BCAs in scope. Had those BCAs been in an ESP, the entity would not have had an R2 issue. Additionally, the entity had insufficient manpower to support its compliance obligations.</p>					
Risk Assessment			<p>WECC determined 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, the entity failed to adequately implement a documented process that included CIP-005-5 R2 Parts 2.1 through 2.3, for [REDACTED] BCAs, as described above.</p> <p>These failures could have led to unauthorized access to BES Cyber Systems, potentially compromising critical operational systems within the Control Centers and affecting the reliability of the BPS. However, as compensation, the entity afforded the seven BCAs the same protective measures of the standards as it did to the Cyber Assets within the ESP, that is, they were in a Physical Security Perimeter, had enabled firewalls, system-level malicious code prevention and monitoring, access management at the application and operating system levels; monitoring of security logs and alerting, and application whitelisting on the local machines. Additionally, single factor authentication was required to access the BCAs which was restricted to individuals with personnel risk assessments and CIP training and the BCAs do not directly affect the production environment as they are part of the entity's development environment. Finally, IRA was limited to sessions initiated from the entity's network segments dedicated to supervisory control and data acquisition support. No harm is known to have occurred.</p> <p>WECC notes that the entity does not have any previous violations of this or similar Standards and Requirements</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) updated its authentication process to require two-factor authentication for all IRA; 2) implemented firewall access control lists to only allow IRA from an IS internet protocol address; and 3) contracted with a third party vendor to augment its compliance staffing issues, address education, and mature its compliance program to ensure future compliance. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019643	CIP-004-6	R3: P3.3	[REDACTED]	[REDACTED]	01/24/2018	02/07/2018	Self-Report	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>On May 7, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in potential noncompliance with CIP-004-6 R3. Specifically, a contractor with a criminal history that required, per the entity’s documented [REDACTED], a review by the entity’s internal [REDACTED] committee prior to provisioning electronic access and unescorted physical access, was given said access without the review. The entity’s plan specifies that a [REDACTED] committee will be convened to evaluate whether authorization should be granted to a prospective employee or contractor when the background check reveals a specific criminal history. In this instance, a check was completed, and access incorrectly approved, despite the background check indicating a prior specific criminal history, by an employee performing the work on a temporary basis. The employee failed to initiate the evaluation process of the contractor’s criminal history and the contractor was granted authorized unescorted physical access to [REDACTED] Physical Security Perimeters (PSP) associated with High Impact Bulk Electric System (BES) BES Cyber Systems (HIBCS) and authorized electronic access to the Physical Access Control Systems (PACS) and the security guard station. This issue began on January 24, 2018, when the employee approved the contractor’s access without convening a [REDACTED] committee and ended on February 7, 2018, when the entity revoked the contractor’s access, for a total of 15 days.</p> <p>The root cause of the issue was attributed to less than adequate process design and lack of controls. Specifically, the entity had a documented process, including a checklist, for employees to reference during the PRA review. However, the entity’s process did not include oversight prior to granting access to prevent a noncompliance from occurring.</p>					
<p>Risk Assessment</p>			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to implement its documented PRA process to evaluate criminal history records checks to attain authorized electronic or authorized unescorted physical access to BES Cyber Systems as required in CIP-004-6 R3 Part 3.3 for one contractor.</p> <p>Failure to evaluate criminal history records could have resulted in the entity allowing an individual unfettered access to the PSPs, thereby potentially endangering the physical safety of employees. However, the contractor in scope was in training and continuously escorted upon entry into a PSP. Furthermore, the contractor’s electronic access to the PACS was limited to that of a user as the contractor did not have elevated administrative privileges. As such, the contractor could not modify access or open any doors electronically. Additionally, this issue was discovered during a routine periodic review conducted by the manager of the [REDACTED] process. No harm is known to have occurred.</p> <p>The entity’s prior compliance history with CIP-004-6 R3 includes NERC Violation IDs: [REDACTED]. Each prior instance of noncompliance involved one individual for whom the entity did not complete a PRA and not a failure to convene the [REDACTED] committee per the entity’s documented process as occurred in the current instance. As such, the facts and circumstances of the current issue are distinct from the previous instances of noncompliance. Therefore, WECC determined the entity’s compliance history is not relevant to this instance and should not serve as a basis for pursuing an enforcement action and/or applying a penalty.</p>					
<p>Mitigation</p>			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) revoked the contractors authorized unescorted physical and authorized electronic access; 2) hired a full-time employee to facilitate the [REDACTED] review process; 3) reviewed and discussed the [REDACTED] process checklist with the [REDACTED] manager and the full-time employee; 4) implemented an oversight policy that included consistent review of each [REDACTED] conducted for a full six months and as needed thereafter; and 5) implemented an automated control that requires the manager of the [REDACTED] process to enter a [REDACTED] completion date into the access tool before an access request for a new contractor or employee is processed. <p>WECC 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
WECC2018020171	CIP-004-6	R4: P4.1, P4.1.3	[REDACTED]	[REDACTED]	03/22/2018	03/22/2018	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 violation.)			<p>On August 1, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in noncompliance with CIP-004-6 R4. Specifically, a system administrator accessed a Bulk Electric System (BES) Cyber System Information (BCSI) storage location without authorization for one day. In this instance, one of the entity's servers that contained the baseline configuration of Physical Access Control Systems (PACS) was experiencing a technical issue. A member of the Cyber Security team emailed the system administrators regarding the server that was not functioning properly and requested that the on-call system administrator address the issue. The system administrator on-call did not have authorized electronic access to the server, a designated BCSI storage location. Therefore, the system administrator contacted a team member and requested the password to the server; the team member gave the on-call system administrator the password. This issue began on March 22, 2018, when the on-call employee accessed a BCSI storage location without authorization and ended the same day, when the password to the server was changed, for a duration of one day.</p> <p>The root cause of the issue was attributed to less than adequate training, and management policy and guidance regarding proper handling of BCSI was not well-defined or understood.</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. In this instance, the entity failed to implement its documented process to authorize access to designated storage locations of BCSI as required by CIP-004-6 R4 Part 4.1 subpart 4.1.3. for one individual.</p> <p>Failure to limit access to BCSI to authorized individuals could have resulted in exposure of critical information to a malicious actor. However, in this instance, the system administrator required access to the BCSI storage location to perform their job responsibilities. Additionally, the entity's internal processes and controls enabled discovery of the issue within an hour. Finally, the entity employs Intrusion Detection and Prevention Systems to monitor for malicious activity in the PACS environment. No harm is known to have occurred.</p> <p>The entity's relevant prior compliance history with CIP-004-6 R4 Part 4.1 subpart 4.1.3. includes NERC Violation IDs: [REDACTED]. WECC determined the entity's compliance history is not relevant to the current instance and should not serve as a basis for pursuing an enforcement action and/or applying a penalty. [REDACTED] was attributed to a lack of controls whereas the current instance was attributed to less than adequate training; [REDACTED] was attributed to a less than adequate program; and [REDACTED] occurred during implementation of the first version of the requirement and is thus not indicative of a systemic issue.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1. changed the password for the server associated with this issue; 2. provisioned access to BCSI locations to employees with Information Technology (IT) domain administrator responsibilities; 3. provided training to IT personnel with domain administrator responsibilities, including the individuals involved in this issue, regarding the BCSI information protection program and proper handling of BCSI; 4. provided training to Cyber Security personnel regarding BCSI and access to the information stored on the server. <p>WECC 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
WECC2018020173	CIP-003-6	R2	[REDACTED]	[REDACTED]	04/01/2017	08/01/2018	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 violation.)			<p>On August 3, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in noncompliance with CIP-003-6 R2. Specifically, the entity did not provide cyber security awareness communication to five third-party vendors which resulted in ten contractors with authorized unescorted physical access to the entity's Low Impact Bulk Electric System (BES) Cyber Systems (LIBCS) not receiving cyber security awareness communication. This issue began on April 1, 2017, when the Standard and Requirement became mandatory and enforceable to the entity and ended on August 1, 2018, when the entity provided cyber security awareness communication to its contractors per its documented cyber security plan for LIBCS, for a duration of 488 days.</p> <p>The root cause of the issue was attributed to less than adequate process design. Specifically, the entity's process did not include a documented process to maintain a record of contract workers that needed to receive security awareness communication.</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 (BPS). In this instance, the entity failed to implement its documented cyber security plan for its LIBCS to provide cyber security awareness communication to five third-party vendors which resulted in ten contractors not receiving the required communication.</p> <p>Such failure could have resulted in the contractors being unaware of appropriate security practices or ill equipped to identify risks associated with their behavior. However, the contractors were not granted authorized electronic access to the LIBCS. Additionally, because this instance of noncompliance was regarding authorized unescorted physical access to LIBCS only, the risk to the BES is minimal. No harm is known to have occurred.</p> <p>The entity's prior compliance history with CIP-003-6 R2 includes NERC Violation ID [REDACTED]. WECC determined the entity's compliance history is not relevant to the current instance and should not serve as a basis for pursuing an enforcement action and/or applying a penalty. The relevant version of the requirement associated with the noncompliance does not specifically address LIBCS. Further, the prior noncompliance was issued for less than adequate content of the policy and not less than adequate process design.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1. provided cyber security to the contractors via the associated third-party vendor; 2. developed and implemented role-specific procedures for teams involved in the LIBCS cyber security awareness process; and 3. corporate compliance team met with the teams associated with the entity's LIBCS cyber security awareness process to review and confirm understanding of the applicable procedures. <p>WECC 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
WECC2018020174	CIP-004-6	R1: P1.1	[REDACTED]	[REDACTED]	04/01/2018	08/11/2018	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 violation.)			<p>On August 2, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in noncompliance with CIP-004-6 R1. Specifically, the entity did not provide cyber security awareness to two third-party vendors resulting in eight contractors with authorized unescorted physical access to at least one of [REDACTED] Medium Impact Bulk Electric System (BES) Cyber Systems (MIBCS) associated with substations not receiving communication regarding cyber security awareness. The entity had temporarily assigned the work associated with its documented process for delivering cyber security awareness for contractors to an employee temporarily, while it sought a full-time employee for the position. The employee assigned to perform the work temporarily was instructed to provide cyber security awareness per the documented process to all contractors but was not adequately trained on how to complete this task. This issue began on April 1, 2018, when eight contractors did not receive cyber security awareness per the entity's documented process and ended on August 11, 2018, when the entity delivered cyber security awareness to the associated third-party vendors, for a total of 133 days.</p> <p>The root cause of the issue was attributed to less than adequate training and oversight. Specifically, the employee was in a temporary role and was not provided adequate guidance and instruction on how to determine which contractors required cyber security awareness per the entity's documented process. Additionally, management failed to provide adequate oversight of task completion when it identified contractors that had not been provided cyber security awareness through the internal review process but did not discuss the issue directly with the employee performing the task.</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. In this instance, the entity failed to implement its documented process to provide cyber security awareness, at least once each calendar quarter, to eight contractors who had authorized unescorted physical access to BCS as required by CIP-004-6 R1 Part 1.1.</p> <p>Failure to provide cyber security awareness to contractors could have resulted in those contractors being unaware, or less mindful, of company policy regarding physical security. However, the eight contractors were only authorized for unescorted physical access and were not provisioned with authorized electronic access. Additionally, the contractors associated with this issue had a completed Personnel Risk Assessment (PRA) on file and therefore had been evaluated for risk. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) provided cyber security awareness to the contractors; 2) hired a permanent employee to fulfill the duties associated with delivering security awareness; and 3) provided training to the manager and newly hired employee to emphasize departmental responsibilities associated with compliance obligations. <p>WECC 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
WECC2019021421	CIP-006-6	R2: P2.1	[REDACTED]	[REDACTED]	12/06/2018	12/06/2018	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 29, 2019, the entity submitted a Self-Log stating that, as a [REDACTED] it was in potential noncompliance with CIP-006-6 R2 Part 2.1. Specifically, on December 6, 2018, two contractors were not continuously escorted in accordance with the entity's documented visitor control program within a Physical Security Perimeter (PSP) controlling access to a High Impact Bulk Electric System (BES) Cyber Systems (HIBCS). The entity's documented program stipulates that the employee identified as the escort must continuously accompany visitors for which they are identified as the escort while in the PSP. In this instance, the employee left the visitors with a contractor who had authorized unescorted physical access to the PSP; the employee left the first visitor with the contractor for approximately three and a half minutes and left the second visitor with the contractor for twenty-four seconds. This issue began on December 6, 2018, when the employee failed to continuously escort the visitors for which they were responsible and ended on December 6, 2018, when the employee resumed escorting the visitors, for a duration of one day.</p> <p>The root cause of the issue was attributed to less than adequate training. Specifically, the employee had completed the entity's Critical Infrastructure Protection (CIP) access training on November 24, 2017 and April 2, 2018. However, the employee had erroneously assumed that the requirement to "continuously escort" visitors was satisfied if an individual with authorized unescorted physical access accompanied the visitor.</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. In this instance, the entity failed to properly implement its documented visitor control program as required by CIP-006-6 R2 Part 2.1 for two visitors that required the employee identified as the escort to continuously escort visitors within PSPs.</p> <p>Such failure could result in the visitors having the opportunity to disable the Energy Management System (EMS) workstations; if the workstations were physically damaged and the EMS operators were unable to utilize their workstations, it could reduce visibility of and control of the system. However, the EMS workstations were manned during regular business hours and were password protected. Additionally, the entity had a back-up control center that could be utilized in the case of an event. Finally, the visitors were not left unattended in the PSP; they were accompanied by a contract worker who had been authorized for unescorted physical access. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) met with the appropriate personnel to review and discuss the entity's documented visitor control program; and 2) adjusted its process to obtain authorized unescorted physical access for visitors that meet certain criteria and that need extended access for legitimate business needs. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017925	CIP-007-6	R1	[REDACTED]	[REDACTED]	7/1/2016	9/28/2016	Compliance 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 violation.)			<p>During a Compliance Audit conducted from [REDACTED], WECC determined that the entity, as a [REDACTED] had a potential noncompliance with CIP-007-6 R1. Specifically, the entity could not provide sufficient R1 evidence, for [REDACTED] Cyber Assets that were decommissioned on September 28, 2016, to demonstrate that it had been compliant with CIP-007-6 R1 Parts 1.1 and 1.2. The [REDACTED] Cyber Assets included [REDACTED] High Impact Bulk Electric System (BES) Cyber System (HIBCS) BES Cyber Assets (BCAs), [REDACTED] Protected Cyber Assets (PCAs) and [REDACTED] Electronic Access Control or Monitoring Systems (EACMS) associated with [REDACTED] HIBCS that were decommissioned as part of the entity’s Energy Management System (EMS) upgrade. Once the Cyber Assets were decommissioned, the evidence proving that the entity had enabled only logical network accessible ports determined to be needed and protections against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media, were no longer available because the baseline configurations, which contained network port information, were purged on January 1, 2017. the entity’s SIEM system treated automatically-collected compliance evidence in a manner similar to security logs and deleted it after 90 days.</p> <p>After reviewing all relevant information, WECC determined that the entity failed to provide sufficient evidence that it had enabled only logical network accessible ports, including port ranges or services where needed to handle dynamic ports, and protected against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media for [REDACTED] Cyber Assets, as required by CIP-007-6 R1 Parts 1.1 and 1.2, respectively.</p> <p>The root cause of the issue was a system configuration issue. Specifically, the entity’s SIEM system treated automatically-collected compliance evidence in a manner similar to security logs and deleted it after 90 days. It was not the intent of the entity that its SIEM should include a 90-day deletion for compliance evidence. Rather it was an unexpected process within the SIEM that led to evidence being lost for decommissioned Cyber Assets after 90 days.</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on September 28, 2016, the day the entity decommissioned the Cyber Assets in scope, for a total of 90 days.</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. In this instance, the entity failed to provide evidence that it had enabled only logical network accessible ports, including port ranges or services where needed to handle dynamic ports, and to protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media for [REDACTED] Cyber Assets, as required by CIP-007-6 R1 Parts 1.1 and 1.2, respectively. Such failure could potentially result in unauthorized access or vulnerable application(s) running, possibly resulting in unauthorized access or compromised critical systems within the entity’s [REDACTED] HIBCS. Unauthorized access due to unmanaged software could result in malware infection or other successful intrusion into the network locations of the vulnerable systems by a malicious actor. The result could be complete control (installation of software, exfiltration of data, remote control, etc.) of the affected system and an anchor point for reconnaissance throughout the environment, which could have severe negative affect on the entity’s connected BES Cyber Systems and result in significant negative affects to the BES. Compromise of the HIBCS could potentially cause operators to lose visibility or could lead to the operators making decisions on manipulated information, which could negatively affect the local operational environment as well as the interconnected BES. Lastly, the impact of not having physical port protections in place could potentially lead to personnel connecting network cables or USB devices to the Cyber Assets. This could lead to either undocumented network connectivity or the potential upload of malicious code via USB or to network ports. [REDACTED]</p> <p>However, the entity implemented good internal controls. While at audit, WECC verified the Cyber Assets in scope were located within a Physical Security Perimeter (PSP) and were protected by Electronic Access Points (EAPs). Additionally, the entity’s program document clearly stated that all Cyber Assets and cabinets were to be labeled and all ports disabled or blocked. As further compensation, the entity performed monthly monitoring of baseline configurations on the Cyber Assets in scope up until the time they were decommissioned, with no unauthorized changes identified. The entity utilized its SIEM to monitor for changes on all Cyber Assets. [REDACTED]. No harm is known to have occurred.</p> <p>WECC determined that the entity has no relevant compliance history for this noncompliance.</p>					
Mitigation			<p>To satisfy remediation for this issue:</p> <ol style="list-style-type: none"> 1) WECC auditors verified a sample set of the entity’s Cyber Assets to ensure that the new EMS Cyber Assets did have port scans and justifications as per CIP-007-6 R1 Part 1.1. Evidence was verified the day after close of audit, and no issues were identified with current production systems. 2) WECC auditors verified the entity’s configuration settings at the Cyber Asset level, GPO and signage for the sampled Cyber Assets above to gain a reasonable assurance the Cyber Assets were compliant with CIP-007-6 R1 Part 1.2. Evidence was verified the day after close of audit, and no issues were identified with current production systems. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017925	CIP-007-6	R1	██████████	██████████	7/1/2016	9/28/2016	Compliance Audit	Completed
			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated its ██████████ decommissioning process to include information and process requirements for collecting and preserving required information from Cyber Assets being decommissioned with the following specifications: <ol style="list-style-type: none"> i) the collection and preservation of information pertaining to authentication methods used and corresponding enforcement; ii) the collection of evidence pertaining to user ID and all password parameters; iii) all required information must be collected and verified, regardless of source, before the Cyber Asset begins final disposal, or any other process that could damage or delete required information; iv) all required information collected as part of this process must be preserved in designated secure storage for three years from the date of decommissioning; and v) information collection must utilize the new ██████ Asset Pre-Disposal Checklist, and must be completed within 14 days of decommissioning. 2) updated its ██████ Change Management Program Guide to include information and requirements related to how Cyber Asset decommissioning fits into the overall change management program. This is to further ensure that required information elements such as authentication methods and password requirements are collected and preserved prior to final Cyber Asset disposal; 3) developed and approved for production use a ██████ Asset Pre-Disposal Checklist to help ensure a consistent, repeatable, and documented process for the collection of Cyber Asset information prior to any final disposal; 4) verified that all process changes have been reviewed and understood by its ██████ EMS team; and 5) had all EMS Subject Matter Experts review and acknowledge acceptance and understanding of the updated guides and supporting materials, and the new Cyber Asset decommission processes. <p>WECC 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
WECC2017017926	CIP-007-6	R5	[REDACTED]	[REDACTED]	7/1/2016	9/28/2016	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 noncompliance.)</p>			<p>During a Compliance Audit conducted from [REDACTED], WECC determined that the entity, as a [REDACTED], had a potential noncompliance with CIP-007-6 R5. Specifically, WECC found two instances; 1) the entity could not provide sufficient R5 evidence, for [REDACTED] Cyber Assets that were decommissioned on September 28, 2016, to demonstrate that it had been compliant with CIP-007-6 R5 Parts 5.1, 5.5, and 5.7. The [REDACTED] Cyber Assets included [REDACTED] HIBCS BCAs, [REDACTED] PCAs and [REDACTED] EACMS associated with [REDACTED] HIBCS that were decommissioned as part of the entity’s EMS upgrade. Once the Cyber Assets were decommissioned, the evidence proving that the entity had enforced authentication of interactive user access; for password-only authentication for interactive user access, either technically or procedurally enforced the password parameters; and limited the number of unsuccessful authentication attempts or generated alerts after a threshold of unsuccessful authentication attempts was no longer available because the evidence was purged on January 1, 2017. The entity’s Security Information Event Management (SIEM) system treated automatically-collected compliance evidence in a manner similar to security logs and deleted it after 90 days. 2) For [REDACTED] Cyber Assets, [REDACTED] PCAs and [REDACTED] EACMS associated with [REDACTED] HIBCS, the entity did not limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts but instead relied on the Active Directory (AD) Group Policy Objects (GPO) and [REDACTED] Access Control System (ACS) server to enforce lockout and alerting because the [REDACTED] Cyber Assets configuration settings could not enforce controls on their local accounts. The entity had misinterpreted the phrase “where technically feasibly” to mean “per device capability,” and did not submit a Technical Feasibility Exception (TFE) for the Cyber Assets not capable of compliance with CIP-007-6 R5 Part 5.7.</p> <p>After reviewing all relevant information, WECC determined that for the first instance, the entity failed to provide evidence that it enforced authentication of interactive user access; for password-only authentication for interactive user access, either technically or procedurally enforced the password parameters; and limited the number of unsuccessful authentication attempts or generated alerts after a threshold of unsuccessful authentication attempts for the [REDACTED] Cyber Assets in scope, as required by CIP-007-6 R5 Parts 5.1, 5.5, and 5.7, respectively. For the second instance, the entity failed to limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts or submit a TFE for [REDACTED] Cyber Assets, as required by CIP-007-6 R5 Part 5.7. Additionally, WECC determined that the entity was compliant with CIP-007-6 R5.6 and has removed it from the scope of this issue.</p> <p>The root cause of the first instance was a system configuration issue. Specifically, the entity’s SIEM system treated automatically-collected compliance evidence in a manner similar to security logs and deleted it after 90 days. It was not the intent of the entity that its SIEM should include a 90-day deletion for compliance evidence. Rather it was an unexpected process within the SIEM that led to evidence being lost for decommissioned Cyber Assets after 90 days.</p> <p>The root cause of the second instance was an incorrect interpretation of newly enforceable NERC CIP Standards and Requirements. Specifically, the entity misinterpreted the “where technically feasible” section of Part 5.7 and did not seek guidance from the NERC ROP CMEP Appendix 4D or WECC.</p> <p>This first instance of noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on September 28, 2016, when the entity decommissioned the Cyber Assets in scope, for a total of 90 days.</p> <p>This second instance of noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on November 22, 2017, when the entity updated each capable Cyber Asset to meet the requirements of CIP-007-6 R5 Part 5.7, for a total of 510 days.</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 the first instance, the entity failed to provide evidence that it enforced authentication of interactive user access; for password-only authentication for interactive user access, either technically or procedurally enforced the password parameters; and limit the number of unsuccessful authentication attempts or generated alerts after a threshold of unsuccessful authentication attempts for [REDACTED] Cyber Assets, as required by CIP-007-6 R5 Parts 5.1, 5.5, and 5.7, respectively. In the second instance, the entity failed to limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts or submit a TFE for an additional [REDACTED] Cyber Assets, as required by CIP-007-6 R5 Part 5.7. Such failures could lead to a bad actor with malicious intent with the ability to not have a login attempt limit. That bad actor could keep attempting to login by using a brute force attack. The entity would not be aware of the unsuccessful logins as alerts were not generated after a certain number of unsuccessful logins. This could cause the bad actor the ability to further attempt to login to Cyber Assets and compromise the accounts which could result in complete control (installation of software, exfiltration of data, remote control, manipulation of data, etc.) of the affected system and an anchor point for reconnaissance throughout the environment, which could have severe negative affect on the connected BES Cyber Systems. Compromise of the HIBCS could potentially cause operators to lose visibility or could lead to the operators making decisions on manipulated information, which could negatively affect the local operational environment as well as the interconnected BES. [REDACTED]</p> <p>However, the entity implemented good internal controls. While at audit, WECC verified the Cyber Assets in scope were located within a PSP and were protected by EAPs. The entity utilized its SIEM to monitor for unauthorized changes on all Cyber Assets. As further compensation, the entity performed monthly monitoring of baseline configurations on the Cyber Assets in scope up until the time they were decommissioned, with no unauthorized changes identified. Lastly, WECC auditors found no issues with the baseline configurations and monitoring of the new production environment, which significantly reduced the risk. For the second instance, the network, server, and workstation accounts utilized AD GPO and [REDACTED] server to limit or alert after a threshold of unsuccessful authentication</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
WECC2017017926	CIP-007-6	R5	██████████	██████████	7/1/2016	9/28/2016	Compliance Audit	Completed
			<p>attempts, and the only way to access local accounts on these Cyber Assets would be to physically remove them from the network. 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 the entity has no relevant compliance history for this noncompliance.</p>					
Mitigation			<p>To satisfy remediation for this issue:</p> <ol style="list-style-type: none"> 1) WECC auditors verified evidence regarding authentication of interactive user access for the above sampled the entity Cyber Assets to gain a reasonable assurance the Cyber Assets were compliant with CIP-007-6 R Part 5.1. Evidence was verified the day after close of audit, and no issues were identified with current production systems; 2) WECC auditors verified evidence regarding password length and complexity requirements for the above sampled the entity Cyber Assets as well as the entities password procedures to gain a reasonable assurance the Cyber Assets were compliant with CIP-007-6 R5 Part 5.5, and Sub-Parts 5.5.1 and 5.5.2. Evidence was verified the day after close of audit, and no issues were identified with current production systems; and 3) WECC auditors verified the entity’s procedures as well as evidence to gain a reasonable assurance the Cyber Assets were compliant with CIP-007-6 R5 Part 5.7. <p>To mitigate the first instance, the entity:</p> <ol style="list-style-type: none"> 1) updated its █████ decommissioning process to include information and process requirements for collecting and preserving required information from Cyber Assets being decommissioned with the following specifications: <ol style="list-style-type: none"> i. the collection and preservation of information pertaining to authentication methods used and corresponding enforcement; ii. the collection of evidence pertaining to user ID and all password parameters; iii. all required information must be collected and verified, regardless of source, before the Cyber Asset begins final disposal, or any other process that could damage or delete required information; iv. all required information collected as part of this process must be preserved in designated secure storage for three years from the date of decommissioning; and v. information collection must utilize the new █████ Asset Pre-Disposal Checklist, and must be completed within 14 days of decommissioning. 2) updated its █████ Change Management Program Guide to include information and requirements related to how Cyber Asset decommissioning fits into the overall change management program. This is to further ensure that required information elements such as authentication methods and password requirements are collected and preserved prior to final Cyber Asset disposal; 3) developed and approved for production use a █████ Asset Pre-Disposal Checklist to help ensure a consistent, repeatable, and documented process for the collection of Cyber Asset information prior to any final disposal; 4) verified that all process changes have been reviewed and understood by its █████ EMS team; and 5) had all EMS Subject Matter Experts review and acknowledge acceptance and understanding of the updated guides and supporting materials, and the new Cyber Asset decommission processes. <p>To remediate and mitigate the second instance, the entity:</p> <ol style="list-style-type: none"> 1) reviewed all applicable Cyber Assets in the HIBCS for capability to either limit or alert after some number of unsuccessful authentication attempts. For each incapable Cyber Asset either: <ol style="list-style-type: none"> i. patched, updated, or reconfigured the Cyber Asset so that it meets Part 5.7 requirements; or ii. reconfigured its EMS network to remove the incapable Cyber Asset from direct involvement in BES operations; 2) updated its guidebooks to clarify the specific meanings of “where technically feasibly” and “per device capability”, with a focus on expanding the sections pertaining to TFEs. The section on implementing new Cyber Asset will be updated to emphasize the need to file a TFE where required, and the revised supporting forms; and 3) had all EMS Subject Matter Experts review and acknowledge acceptance and understanding of the TFE requirements for all applicable Cyber Assets. <p>WECC 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
WECC2018018973	CIP-004-6	R4; P4.1	[REDACTED]	[REDACTED]	6/22/2017	10/13/2017	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 violation.)			<p>On January 8, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in potential noncompliance with CIP-004-6 R4. Specifically, on June 27, 2017, during the entity's annual review of access to Bulk Electric System (BES) Cyber System Information (BCSI) repositories (cabinets), it discovered two individuals who had been authorized by their manager for read-only electronic access to three BCSI cabinets within its document management system based on a group membership instead of through the entities documented CIP-004-6 R4 Part 4.1 processes; that is by approval from their Manager, as well as the cabinet custodians. Therefore, the two individuals were not appropriately authorized to have said access. This issue began on June 22, 2017, when the first individual was provisioned unauthorized access to BSCI and ended on October 23, 2017, when BSCI was revoked for the same individual, for a total of 124 days. The second individual was provisioned and revoked access with the timeframe of the first individual. The root cause of the issue was attributed to a less than adequate documented process for authorizing access to BSCI cabinets in the document management system.</p>					
Risk Assessment			<p>WECC determined 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, the entity failed to appropriately implement it documented processes for authorizing access to BSCI for two individuals as required by CIP-004-6 R4 Part 4.1.</p> <p>Such failure could result in BSCI being used in a malicious manner to cause harm to the entity's Cyber Assets associated with its High Impact BES Cyber Systems. However, as compensation, the two individuals had a business need to access the BSCI and had been approved by their managers. Effectively, this issue is an administrative error. Additionally, the BCSI in the cabinet was several years old, reducing the likelihood of the information being an actual risk to the BPS. No harm is known to have occurred.</p> <p>WECC considered the entity's compliance history in its designation of this remediated issue as a CE. The entity's prior compliance history with CIP-004-6 R4 includes NERC Violation ID [REDACTED]. WECC determined the entity's compliance history should not serve as a basis for pursuing an enforcement action and/or applying a penalty because it is only one instance of previous noncompliance and not indicative of a programmatic problem or failed mitigation.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) revoked access to the BSCI cabinets for the two individuals in scope; 2) added a tag or indicator to all BSCI cabinets to remind Information Technology (IT) personnel that approvals are required from the cabinet custodian before provisioning access; 3) updated its BSCI access request process to require cabinet owner approval and removed all "mirrored/counterpart" access requests; 4) created a new form in its ticketing system for requesting access to BSCI; 5) held a meeting with IT management to ensure everyone understands the new process which includes routing all BSCI request to the service desk for approval before the ticket is sent for provisioning; and 6) removed all group access provisioning for all BSCI cabinets. <p>WECC has verified completion of 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
WECC2018018974	CIP-004-6	R4; P4.4	[REDACTED]	[REDACTED]	7/1/2017	12/19/2017	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 January 8, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in potential noncompliance with CIP-004-6 R4. Specifically, the initial verifications of [REDACTED] BSCI designated storage locations were either performed after July 1, 2017 or not performed at all. Additionally, for [REDACTED] BSCI designated storage locations that were reviewed prior to or on July 1, 2017, the entity did not adequately document the review results; specifically, the results were missing information or there was no actual collection of evidence. This issue began on July 1, 2017, when the Standard and Requirement became mandatory and enforceable and ended on December 19, 2017, when the entity verified the access to [REDACTED] BSCI designated storage locations was correct and necessary for performing assigned work functions, for a total of 172 days. The root cause of the issue was attributed to a lack of internal controls to ensure the reviews were performed on time and evidence was adequately collected, compounded by the human performance of an individual no longer employed by the entity.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to adequately implement its documented access management program when it did not timely verify or obtain evidence of verification that access to BSCI designated storage locations was correct and necessary for performing assigned work functions as required by CIP-004-6 R4 Part 4.4.</p> <p>Such failure could lead to the entity not knowing who has access to BSCI or whether access privileges exceed the minimum needed to perform work function. This could potentially result in BSCI being used in a malicious manner to cause harm to the entity's Cyber Assets associated with its High Impact BES Cyber Systems. However, as compensation, once the verification was performed, it was determined that the accesses were correct and necessary for performing assigned work functions and required no changes and no irregularities or anomalies were identified. Additionally, although the verification for [REDACTED] of the BSCI designated storage locations were not performed by the effective date, they were performed within two months of that date, and [REDACTED] other BSCI designated storage locations had verifications with less than adequate evidence to demonstrate such. No harm is known to have occurred.</p> <p>WECC considered the entity's compliance history in its designation of this remediated issue as a CE. The entity's prior compliance history with CIP-004-6 R4 includes NERC Violation ID [REDACTED]. WECC determined the entity's compliance history should not serve as a basis for pursuing an enforcement action and/or applying a penalty because it is only one instance of previous noncompliance and not indicative of a programmatic problem or failed mitigation.</p>					
Mitigation			<p>To remediate and mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) developed a template for all business areas to use to document the annual verification. The template includes prompts for screenshots or copy of the list(s) of individuals with access, documentation of the results of the review, and date the review was completed. The template also includes a section to clearly document whether the access is correct, and necessary for the work function; 2) eliminated one, and verified the remaining BSCI designated storage locations in scope utilizing the new template; 3) conducted training sessions for applicable personnel on how to use the new template; 4) created a process to document request, approval, and 15 calendar month review for IT administrator logical access to BSCI designated storage locations; 5) implemented the following internal controls – <ol style="list-style-type: none"> a) kickoff meeting for each verification cycle to ensure individuals responsible for the verifications are aware of task due dates and are trained on the most current processes; b) updates to its repository access management procedure which assigns responsibility for performing the 15 calendar month verification to help ensure personnel have the information needed to perform the verification in a consistent manner and defines process steps for each type of BSCI designated storage location access; and c) updates to the review template to capture appropriate information including evidence of screenshots to help ensure quality and consistency of the verification process. <p>WECC verified completion of mitigating activities.</p>					

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	RFC2019020926	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 years
2	RFC2019021024	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 years
3	RFC2019020927	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 years
4	RFC2019021023	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 years
5	RFC2019020962	Yes	Yes	Yes	Yes	Yes								Category 1: 3 years; Category 2 – 12: 2 years
6	RFC2019020933	Yes		Yes	Yes	Yes	Yes				Yes			Category 1: 3 years; Category 2 – 12: 2 years
7	RFC2019020932	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 years
8	RFC2018019691	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
9	RFC2018020752	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 years
10	RFC2019021198	Yes		Yes	Yes			Yes						Category 1: 3 years; Category 2 – 12: 2 years
11	RFC2018019695	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
12	SERC2017017323	Yes		Yes	Yes					Yes				Category 2 – 12: 2 year
13	SERC2017018775			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
14	SERC2017018720			Yes	Yes				Yes	Yes	Yes		Yes	Category 2 – 12: 2 year
15	SERC2019021862			Yes	Yes					Yes				Category 2 – 12: 2 year
16	SERC2017017321		Yes	Yes	Yes					Yes	Yes			Category 2 – 12: 2 year
17	TRE2017018555	Yes		Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 year

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)
18	TRE2018020401	Yes		Yes	Yes			Yes		Yes				Category 1: 3 years; Category 2 – 12: 2 year
19	TRE2017018659	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
20	TRE2017018671	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
21	TRE2017018674	Yes		Yes	Yes						Yes			Category 2 – 12: 2 year
22	TRE2017018675	Yes		Yes	Yes	Yes					Yes			Category 1: 3 years; Category 2 – 12: 2 year
23	TRE2018020572	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
24	TRE2018019171	Yes		Yes	Yes	Yes					Yes			Category 1: 3 years; Category 2 – 12: 2 year
25	TRE2018019175	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 year
26	WECC2018020620	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
27	WECC2018020621	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
28	WECC2017018528	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
29	WECC2018019132			Yes	Yes									Category 2 – 12: 2 years
30	WECC2018019302			Yes	Yes					Yes				Category 2 – 12: 2 years
31	WECC2018019748			Yes	Yes									Category 2 – 12: 2 years
32	WECC2018019749	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
33	WECC2018020363			Yes	Yes									Category 2 – 12: 2 years
34	WECC2018020445			Yes	Yes					Yes				Category 2 – 12: 2 years
35	WECC2018018941			Yes	Yes					Yes				Category 2 – 12: 2 years
36	WECC2018019685			Yes	Yes						Yes			Category 2 – 12: 2 years
37	WECC2018020041			Yes	Yes									Category 2 – 12: 2 years

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019020926	CIP-010-2	R1	[REDACTED]	[REDACTED]	10/15/2018	10/31/2018	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 9, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>On October 15, 2018, the entity discovered that three [REDACTED] workstations in [REDACTED] were not labeled as retired, even though the assets had been retired from NERC production on August 22, 2018. The entity discovered this as a result of an [REDACTED] updating the status of three [REDACTED] workstations in [REDACTED] (the entity's asset inventory system of record). The assets were, upon retirement, being repurposed [REDACTED] for testing and the entity had labeled them as retired in the entity's baseline monitoring tool and baseline system of record, but not in [REDACTED]. These retired assets were off and unplugged from the entity's network starting on August 22, 2018 and until October 15, 2018. Therefore, the entity did not implement any security patches during the above described timeframe. On October 15, 2018, the entity turned the assets back on, and connected them to the network [REDACTED]. This occurred before the entity brought the assets up-to-date on their security patches.</p> <p>The root cause of this noncompliance was an unclear process without sufficient steps for an update to an asset's CIP Status and inadequately trained staff resulting in the entity's failure to follow its process to retire assets.</p> <p>This noncompliance involves the management practices of asset and configuration management, and validation. Asset and configuration management is involved because the entity failed to establish and maintain asset retirement records and processes. Validation is involved because the entity failed to validate that the asset retirement process had been successfully implemented for the three [REDACTED] workstations involved in this noncompliance.</p> <p>This noncompliance started on October 15, 2018, when the entity brought the [REDACTED] workstations online without implementing the required security patches and ended on October 31, 2018, when the entity installed the missing security patches.</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 risk posed by this instance of noncompliance is that [REDACTED] workstations with out-of-date security patches provide an attack vector to bad actors to access and utilize the [REDACTED] workstations to adversely impact the BPS. The risk is mitigated because the three [REDACTED] workstations were only used for testing and configured to interact with the test server only. The entity confirmed that the configurations of the [REDACTED] software on these three assets made them incapable of interacting [REDACTED]. Also, the three [REDACTED] workstations were off and unplugged from the entity's network from August 22, 2018 until October 15, 2018, thus reducing the period of time that any harm could have occurred as a result of the workstations not being patched. Lastly, ReliabilityFirst notes that 35 other workstations were properly maintained, secured, and performing as expected. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different facts and circumstances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) installed the missing security patches on the three assets; 2) performed an extent of conditions to determine if any other [REDACTED] workstations did not receive all security patches between the start date of the three assets being off and unplugged from the network until the day after the three workstations security patches were brought up to date; 3) updated the retirement procedure to include steps so that if an asset is turned off and unplugged from the network it requires the retirement process be executed and to ensure that the system of record and compliance tools are all updated to reflect retirement of an asset. All assets that will be reused must be re-onboarded; and 4) designated testing workstations as a preventative measure. These workstations were also configured to only use the [REDACTED]. <p>ReliabilityFirst 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
RFC2019021024	CIP-010-2	R1	[REDACTED]	[REDACTED]	8/24/2018	8/31/2018	Self-Report	October 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 noncompliance.)			<p>On January 23, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>On August 27, 2018, as a result of a review of baseline daily reports, the entity [REDACTED] discovered that the recently patched [REDACTED] server deployed a new backup agent automatically to a [REDACTED] server without proper change management documentation. [REDACTED] It is not associated with a Bulk Electric System Cyber System. This incident occurred on August 24, 2018 after the [REDACTED] server received a patch that applied vendor recommended bug fixes and enhancements. The entity was not aware that the patch also changed the process of [REDACTED] because that was not listed in the description of the patch from the vendor. (Had these changes gone through the change management process, the change ticket owner would have been required to associate assets to the change. If the NERC asset would have been associated to the change ticket the implementer would have been aware. Since the implementer (SME) followed no change management process, the preventative controls in the change management process were circumvented.)</p> <p>This noncompliance involves the management practices of external interdependencies, workforce management, and verification. The root cause is that the Subject Matter Expert (SME) responsible for patching was not effectively trained to make sure that he understood all consequences of applying a potential patch. External interdependencies is involved and is a contributing factor because the vendor did not list in its description of the patch that the patch would change [REDACTED]</p> <p>This noncompliance started on August 24, 2018, the day the server deployed a new backup agent automatically to a NERC [REDACTED] sever without proper change management documentation and ended on August 31, 2018, when the entity approved the change request.</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 risk posed by making an unapproved change to a server without proper change management documentation is that the unapproved change could negatively affect the BPS. The risk is lessened because if this device failed, there are multiple other [REDACTED] servers in place to continue normal functions. Additionally, the patch that was applied had been tested on a representative system to determine impact and functionality before application. The agent upgrade did not propagate to the other domain controller because the agent is isolated to this server and this server is the only [REDACTED] being backed up, meaning this noncompliance only affected one server. The vendor determined the installation of this upgrade to be necessary and recommended. Lastly, the noncompliance only lasted for seven days and was discovered through an internal control. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history does not warrant an alternative disposition method and should not serve as a basis for applying a penalty because some of the prior noncompliances are distinguishable as they involved different circumstances or root causes. For the two issues that are arguably similar, ReliabilityFirst determined that the current noncompliances continues to qualify for compliance exception treatment as it posed only minimal risk and is not indicative of a systemic or programmatic issue. Further, the entity quickly identified the noncompliance and corrected the issue through its internal controls. The current noncompliance also has a short duration of just seven days.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> created a [REDACTED] change request for approval authorization of change and verification of CIP-005 and 007 controls; performed an extent of condition review. No additional unauthorized changes were detected based on the entity's detective controls for baseline reviews that discovered the two incidents. The controls scope for baseline review included all assets in the NERC environments; implemented "Change [REDACTED]" as required training for new employee onboarding. The entity will also implement the "Change [REDACTED]" as an annual requirement for employees with the identifier of NERC CIP Employee; <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by October 31, 2019:</p> <ol style="list-style-type: none"> [REDACTED] The intent of this milestone is to strengthen the existing requirement that all production NERC CIP assets must have an approved change request prior to making any modifications to that asset. [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
RFC2019020927	CIP-010-2	R1	[REDACTED]	[REDACTED]	10/15/2018	10/31/2018	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 9, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>On October 15, 2018, the entity discovered that three [REDACTED] workstations [REDACTED] were not labeled as retired, even though the assets had been retired from NERC production on August 22, 2018. The entity discovered this as a result of [REDACTED] updating the status of three [REDACTED] workstations [REDACTED] (the entity's asset inventory system of record). The assets were, upon retirement, being repurposed [REDACTED] for testing and the entity had labeled them as retired in the entity's baseline monitoring tool and baseline system of record, but not in [REDACTED]. These retired assets were off and unplugged from the entity's network starting on August 22, 2018 and until October 15, 2018. Therefore, the entity did not implement any security patches during the above described timeframe. On October 15, 2018, the entity turned the assets back on, and connected them to the network [REDACTED]. This occurred before the entity brought the assets up-to-date on their security patches.</p> <p>The root cause of this noncompliance was an unclear process without sufficient steps for an update to an asset's CIP Status and inadequately trained staff resulting in the entity's failure to follow its process to retire assets.</p> <p>This noncompliance involves the management practices of asset and configuration management, and validation. Asset and configuration management is involved because the entity failed to establish and maintain asset retirement records and processes. Validation is involved because the entity failed to validate that the asset retirement process had been successfully implemented for the three [REDACTED] workstations involved in this noncompliance.</p> <p>This noncompliance started on October 15, 2018, when the entity brought the [REDACTED] workstations online without implementing the required security patches and ended on October 31, 2018, when the entity installed the missing security patches.</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 (BPS) on the following factors. The risk posed by this instance of noncompliance is that [REDACTED] workstations with out-of-date security patches could provide an attack vector to bad actors to access and utilize the [REDACTED] workstations to adversely impact the BPS. The risk is mitigated because the three [REDACTED] workstations were only used for testing and configured to interact with the test server only. The entity confirmed that the configurations of the [REDACTED] software on these three assets made them incapable of interacting [REDACTED]. Also, the three [REDACTED] workstations were off and unplugged from the entity's network from August 22, 2018 until October 15, 2018, thus reducing the period of time that any harm could have occurred as a result of the workstations not being patched. Lastly, ReliabilityFirst notes that 35 other workstations were properly maintained, secured, and performing as expected. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different facts and circumstances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) installed the missing security patches on the three assets; 2) performed an extent of conditions to determine if any other [REDACTED] workstations did not receive all security patches between the start date of the three assets being off and unplugged from the network until the day after the three workstations security patches were brought up to date; 3) updated the retirement procedure to include steps so that if an asset is turned off and unplugged from the network it requires the retirement process be executed and to ensure that the system of record and compliance tools are all updated to reflect retirement of an asset. All assets that will be reused must be re-onboarded; and 4) designated testing workstations as a preventative measure. These workstations were also configured to only use the [REDACTED]. <p>ReliabilityFirst 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
RFC2019021023	CIP-010-2	R1	[REDACTED]	[REDACTED]	8/24/2018	8/31/2018	Self-Report	October 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 noncompliance.)			<p>On January 23, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>On August 27, 2018, as a result of a review of baseline daily reports, the entity [REDACTED] discovered that the recently patched [REDACTED] server deployed a new backup agent automatically to a [REDACTED] server without proper change management documentation. The server at issue is a [REDACTED]. This incident occurred on August 24, 2018 after the [REDACTED] server received a patch that applied vendor recommended bug fixes and enhancements. The entity was not aware that the patch also changed the process of [REDACTED] because that was not listed in the description of the patch from the vendor. (Had these changes gone through the change management process, the change ticket owner would have been required to associate assets to the change. If the NERC asset would have been associated to the change ticket the implementer would have been aware. Since the implementer (SME) followed no change management process, the preventative controls in the change management process were circumvented.)</p> <p>This noncompliance involves the management practices of external interdependencies, workforce management, and verification. The root cause is that the Subject Matter Expert (SME) responsible for patching was not effectively trained to make sure that he understood all consequences of applying a potential patch. External interdependencies is involved and is a contributing factor because the vendor did not list in its description of the patch that the patch would change [REDACTED].</p> <p>This noncompliance started on August 24, 2018, the day the server deployed a new backup agent automatically to a [REDACTED] sever without proper change management documentation and ended on August 31, 2018, when the entity approved the change request.</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 risk posed by making an unapproved change to a server without proper change management documentation is that the unapproved change could negatively affect the BPS. The risk is lessened because if this device failed, there are multiple other [REDACTED] servers in place to continue normal functions. Additionally, the patch that was applied had been tested on a representative system to determine impact and functionality before application. The agent upgrade did not propagate to the other domain controller because the agent is isolated to this server and this server is the only [REDACTED] being backed up, meaning this noncompliance only affected one server. The vendor determined the installation of this upgrade to be necessary and recommended. Lastly, the noncompliance only lasted for seven days and was discovered through an internal control. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history does not warrant an alternative disposition method and should not serve as a basis for applying a penalty because some of the prior noncompliances are distinguishable as they involved different circumstances or root causes. For the two issues that are arguably similar, ReliabilityFirst determined that the current noncompliances continues to qualify for compliance exception treatment as it posed only minimal risk and is not indicative of a systemic or programmatic issue. Further, the entity quickly identified the noncompliance and corrected the issue through its internal controls. The current noncompliance also has a short duration of just seven days.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) created a [REDACTED] change request for approval authorization of change and verification of CIP-005 and 007 controls; 2) performed an extent of condition review. No additional unauthorized changes were detected based on the entity's detective controls for baseline reviews that discovered the two incidents. The controls scope for baseline review included all assets in the NERC environments; 3) implemented [REDACTED] Training" as required training for new employee onboarding. The entity will also implement the [REDACTED] Training" as an annual requirement for employees with the identifier of NERC CIP Employee; <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by October 31, 2019:</p> <ol style="list-style-type: none"> 4) [REDACTED]. The intent of this milestone is to strengthen the existing requirement that all production NERC CIP assets must have an approved change request prior to making any modifications to that asset. [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
RFC2019020962	CIP-005-5	R2	[REDACTED]	[REDACTED]	10/6/2018	11/29/2018	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 15, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-005-5 R2. Due to a setting change in its multi-factor authentication system, under certain circumstances (i.e., when multi-factor service was unreachable), an Interactive Remote Access session could be initiated with only single-factor authentication (i.e., username and password). More specifically, on September 18, 2018, the entity changed the multi-factor authentication system's failure mode to [REDACTED]. In [REDACTED] mode, if multi-factor service is unreachable, users are allowed to access multi-factor-protected applications if they pass primary authentication. The other available failure mode is [REDACTED]. In [REDACTED] mode, if multi-factor service is unreachable, users are denied access to multi-factor-protected applications even if they pass primary authentication. The entity changed the setting because it wanted to allow support in emergency situations if communications to the multi-factor system were interrupted. In summary, as a result of the setting change, the two-factor authentication server would be bypassed if multi-factor service was unreachable, thus allowing access with only single-factor authentication.</p> <p>The issue was discovered on October 6, 2018. On that date, operators called the on-call telephone number to report [REDACTED] and other outages, which were later determined to be due to core switch instability in the entity's corporate network. The on-call system administrator drove to the facility to address the issue, as VPN access was down. After arriving, the administrator logged into an entity-issued laptop to begin troubleshooting. At this time, while logging into the entity's remote support solution, the multi-factor authentication system automatically bypassed the two-factor authentication server for the reasons identified above (i.e., core switch instability rendered multi-factor service unreachable and the [REDACTED] setting allowed access with only single-factor authentication). The administrator immediately recognized that he had logged in with only single-factor authentication and contacted members of the operations technology team to report that multi-factor authentication was down. On October 8, 2018, the operations technology team met with compliance personnel to discuss the situation, and the operations technology team disclosed the setting change that was implemented on September 18, 2018.</p> <p>The root cause of this noncompliance was the failure to fully evaluate the implications of a specific setting change. This noncompliance implicates the management practices of asset and configuration management and implementation. Asset and configuration management involves, in part, controlling changes to asset and configuration items. Implementation was implicated because when an entity decides to implement a change, it is important for the entity to ensure that the change does not compromise the reliability or resilience of the bulk power system (BPS).</p> <p>This noncompliance started on October 6, 2018, when the multi-factor authentication system became unreachable and Interactive Remote Access sessions were possible without multi-factor authentication, and ended on October 20, 2018, after multi-factor authentication functionality was restored. During its review of access records as part of its Mitigation Plan, the entity identified an additional instance that started and ended on November 29, 2018, when the multi-factor authentication system went into [REDACTED] mode during an [REDACTED] internet outage.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS based on the following factors. By allowing access without requiring multi-factor authentication, the entity increased the risk of compromise of assets in the Electronic Security Perimeter (ESP) by an unauthorized actor. In this case, the risk was mitigated by the following facts. First, it is worth noting that multi-factor authentication was still required after the setting change was implemented on September 18, 2018. Access with single-factor authentication was only possible if the multi-factor authentication system went down. After the setting change, these circumstances only presented between October 6, 2018, and October 20, 2018, and again on November 29, 2018. At all other times, multi-factor authentication was required. Second, during the period of this noncompliance, VPN was down, and the entity was experiencing internet connectivity issues. This means that in order to exploit the vulnerability (i.e., Interactive Remote Access with only single-factor authentication), a malicious user would have to (a) be on-site at the entity's facility, (b) be connected to the network with an entity-issued device with the remote support solution installed, (c) know a set of active credentials (i.e., username and password) for the remote support solution, and (d) know sets of active credentials (i.e., usernames and passwords) for the devices that the malicious user intended to access inside of the ESP. 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) re-configured its multi-factor authentication system and placed it back into [REDACTED] mode; 2) reviewed logs of remote support solution access during the time that the two-factor authentication was not working. Additionally, once the multi-factor authentication system was back in [REDACTED] mode, the entity compared all remote support solution and multi-factor authentication system records for the time the system was in [REDACTED] mode; 3) developed a procedure for access to its systems in the event that that the multi-factor authentication system is not functioning with two-factor authentication; and 4) trained all individuals with access to the remote support solution on the new procedure to ensure that they understand how to access systems if there is a remote access failure. <p>ReliabilityFirst 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
RFC2019020933	CIP-006-6	R1	[REDACTED]	[REDACTED]	7/1/2016	2/1/2019	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>On January 9, 2019, ReliabilityFirst determined that the entity, [REDACTED] was in noncompliance with CIP-006-6 R1 identified during a Compliance Audit conducted from [REDACTED]. During the audit, ReliabilityFirst determined that the entity failed to implement at least 2 different controls to restrict access to the High Impact Bulk Electric System Cyber Systems and their associated Electronic Access Control or Monitoring Systems and Protected Cyber Assets residing at the entity's [REDACTED] location. Specifically, ReliabilityFirst identified a roof hatch that the entity did not identify as an access point to the Physical Security Perimeter (PSP). After physically inspecting the location, ReliabilityFirst did not observe any physical access controls to prevent physical access into the PSP through the roof hatch. However, the entity attested that the roof hatch is continuously monitored by a [REDACTED]. The entity also attested that the roof hatch cannot be locked because it is an emergency exit for employees on the second floor of the [REDACTED] location if the only other entrance (i.e., the main entrance) is not accessible due to fire.</p> <p>The root cause of this noncompliance was the entity's assumption that the roof hatch did not constitute an "access point" under its Physical Security Plan because it was not used for normal entry/exit from the PSP. This root cause involves the management practice of workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-006-6 R1 and ended on February 1, 2019, when the entity properly secured the roof hatch.</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 secure access points to the PSP is that an unauthorized individual could gain access to the PSP. The risk was mitigated in this case by the following factors. First, the roof hatch at issue is not easily accessible by the public. The hatch is located at the main level roof, which would require the use of an extension ladder to access from the ground. Second, the entity has other physical controls in place at the [REDACTED] to protect against unauthorized physical entry, such as [REDACTED]. Third, the entity also has multiple detective controls in place at the roof hatch to identify any attempted unauthorized access such as a [REDACTED]. 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) reviewed the final new alternate egress path design proposal and obtained appropriate approvals to facilitate installation; 2) commissioned a new alternate egress path; 3) secured the roof hatch; 4) updated Access Point definition in management model documents to include all door/portals; and 5) updated Physical Security Perimeter Diagrams to reflect changes from Alarm Only Points to Access Points. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019020932	CIP-007-6	R2			9/22/2018	12/14/2018	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 11, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-007-6 R2.2. On September 19, 2018, the entity deployed three Electronic Access Control or Monitoring Systems (EACMS) [REDACTED] but failed to properly classify the assets in its systems. As a result, the entity patched the assets in accordance with its standard corporate patching procedure, which did not include a CIP-007-6 R2.2 evaluation step. Between September, 2018, and October, 2018, the entity applied five security patches/updates to the three [REDACTED], but the patches/updates had not been evaluated in accordance with CIP-007-6 R2.2 and baseline configurations were not updated in accordance with CIP-010-2 R1.3. A subject matter expert (SME) identified the issue on October 23, 2018, while reviewing reports and preparing to perform patch assessments for the assets. The entity implemented corrective actions (i.e., classified the [REDACTED] as NERC assets), but an additional instance occurred on December 1, 2018, when a monthly rollup was deployed prior to being evaluated in accordance with CIP-007-6 R2.2. The additional instance occurred because even though the [REDACTED] had been reclassified, responsible personnel failed to update the patch field for the [REDACTED] (i.e., the field should have been changed from patch on the "3rd Saturday at 9:00 a.m." to "Do Not Patch"). The additional instance was also identified by a SME who was reviewing reports and preparing to perform patch assessments for the assets.</p> <p>The root cause of this noncompliance was a deficient asset onboarding process. The entity did not provide responsible personnel with adequate instructions regarding the performance of necessary tasks to classify new assets in its systems. There were various steps that needed to be followed to ensure proper classification and treatment, but those steps were not clearly outlined.</p> <p>This noncompliance involves the management practice of workforce management. As part of workforce management, an entity should strive to develop and implement thorough, clear, and executable processes and procedures and, further, ensure that staff are properly trained to perform necessary tasks.</p> <p>The first instance started on September 22, 2018, when the entity failed to evaluate security patches/updates in accordance with CIP-007-6 R2.2 and ended on October 30, 2018, when the entity evaluated the patches/updates that had been deployed and updated baseline configurations. The second instance started on December 1, 2018, when the entity failed to evaluate the monthly rollup in accordance with CIP-007-6 R2.2 and ended on December 14, 2018, when the entity completed the 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 (BPS) based on the following factors. A failure to evaluate patches in a timely manner could result in missing the installation of critical security patches that could leave assets vulnerable to malicious activity. And, failing to update baseline configurations in a timely manner could lead to reliance on inaccurate information when responding to a security incident or conducting an evaluation, a reconciliation, or a recovery. Here, the risks were mitigated based on the following facts. The entity's misclassification of the assets in its systems did not result in any missed patches. The entity was applying (but not evaluating) patches for the assets at regular intervals. And, even though baseline configurations were updated eight days late after the initial changes, the entity was actively investigating and handling the issue during this brief period, thus further reducing the risk. The assets are used for [REDACTED], and there is no remote capability from these assets to the BPS. Also, these assets are housed in a physical security perimeter that is monitored 24/7/365 by security. Lastly, the assets are located behind firewalls, which restrict access and reduce the attack vectors that could be utilized by a malicious actor. 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, circumstances, and/or causes. Further, the entity promptly self-identified and corrected the issues described in the current noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) verified that patches were applied in September and October; 2) evaluated the patches that were applied in September and October; 3) updated its inventory database to define the assets as NERC assets; 4) updated its standard work instruction to make sure NERC assets are identified and designated as "Do Not Patch;" 5) updated its inventory database to change the patching field for the assets to "Do Not Patch;" 6) evaluated patches that were applied in December; and 7) verified that patches were applied in December. <p>ReliabilityFirst 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
RFC2018019691	CIP-003-6	R1	[REDACTED]	[REDACTED]	4/1/2017	8/14/2018	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 May 4, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in violation of CIP-003-6 R1. Specifically, the entity did not develop a policy or policies for assets identified in CIP-002 containing low impact Bulk Electric System (BES) Cyber Systems that addressed physical security controls (CIP-003-6 R1.2.2) or electronic access controls for Low Impact External Routable Connectivity and Dial-up Connectivity (CIP-003-6 R1.2.3). The issue was discovered during an internal, comprehensive compliance assessment after [REDACTED]</p> <p>The root cause of this noncompliance was inadequate planning, which resulted in confusion regarding the development and implementation of policies and controls relating to physical security and electronic access for assets containing low impact BES Cyber Systems. This noncompliance implicates the management practice of planning, which includes the need to effectively understand standards and requirements and establish safeguards to avoid an unintentional adverse effect on bulk power system (BPS) reliability and resilience.</p> <p>The violation began on April 1, 2017, when the entity failed to document and have a CIP Senior Manager approve a policy by the enforcement date and ended on August 14, 2018, after the entity documented and obtained necessary approval of the policy.</p>					
Risk Assessment			<p>This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS based on the following factors. The failure to have one or more adequate policies that address physical security and electronic access for assets containing low impact BES Cyber Systems could result in personnel not having proper direction and guidance when creating procedures and processes for and implementing various cyber security matters, thereby increasing the likelihood of a deficient security posture. Here, the risk was minimized based on the following factors. Even though the overarching policy should have been in place and approved on or before April 1, 2017, the actual implementation of the controls subject to that policy (i.e. physical and electronic access controls for Low Impact External Routable Connectivity and Dial-up Connectivity) did not have to occur, initially, until September 1, 2018. And, pursuant to FERC Order 843 approving CIP-003-7 (which supersedes the prior version), the compliance date for the implementation of those physical and electronic controls is January 1, 2020. In summary, this noncompliance is primarily a documentation issue. No harm is known to have occurred.</p> <p>ReliabilityFirst considered each 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) developed a Physical Security Controls and Electronic Access Controls for Low Impact External Routable Connectivity and Dial-up Connectivity policy; 2) conducted training for all effected personnel on the Physical and Electronic Access Control policy; 3) developed a new standard application form to identify implementation time frames for new or modified standards; 4) reviewed corporate compliance policies to ensure that discovered areas of potential non-compliance are corrected promptly; 5) enhanced the [REDACTED] by specifying practices to improve the understanding of current standards and requirements and identify and plan for future standards at the entity; and 6) provided training to staff regarding new [REDACTED] practices for current and future standards and requirements and implementation time frames. <p>ReliabilityFirst 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
RFC2018020752	CIP-007-6	R2	[REDACTED]	[REDACTED]	5/1/2018	10/2/2018	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 November 13, 2018, the entity [REDACTED], submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-007-6 R2. [REDACTED]</p> <p>[REDACTED] In this case, the entity discovered that it had determined that two patches were not applicable, but failed to properly document that conclusion and corresponding justification.</p> <p>Specifically, on October 2, 2018, the entity installed the latest patch for its authentication manager. In the course of completing the corresponding change management tasks, the entity discovered that two prior patches for this tool had not been applied. However, there was no documentation regarding this conclusion or the underlying justification. Upon further investigation, the entity determined that those decisions were accurate when made, but just not documented properly.</p> <p>The root cause of this noncompliance was a lack of understanding regarding the documentation requirements for patches that the entity determines are not applicable. This root cause involves the management practice of workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on May 1, 2018, when the entity determined that the first patch was not applicable to its environment and ended on October 2, 2018, when the entity installed the latest patch for its [REDACTED].</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 document the determination that a patch is not applicable is that it makes it more difficult for the entity to review the accuracy of that determination, which could potentially lead to patches being inappropriately deemed not applicable. This risk was mitigated in this case based on the following factors. First, this issue was primarily a documentation issue. The entity confirmed that the determination of the patches as inapplicable was accurate when made, but just not documented properly. So, there was no operational risk posed by failing to apply them. Second, the entity self-identified this issue while performing its normal change management process, which is indicative of effective internal controls. Third, this issue was an isolated incident given the fact that the entity applies up to [REDACTED] every month on approximately [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 while the result of some of the prior noncompliances were arguably similar, those prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) enrolled the technician in CIP [REDACTED] training; and 2) ensured that the technician completed CIP [REDACTED] training. <p>ReliabilityFirst 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
RFC2019021198	CIP-004-6	R3	[REDACTED]	[REDACTED]	7/2/2018	12/12/2018	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 March 4, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R3.</p> <p>On December 12, 2018, while performing a CIP-004-6 review, the entity discovered that the entity did not possess a Personal Risk Assessment (PRA) for a [REDACTED]. (The individual did not have a prior, expired PRA.) The substation electrician at issue had access to High Impact facilities. The [REDACTED] was provided access based on the work required under the job description for that position. However, during the time period which the [REDACTED] had access to high-impact facilities without a PRA, the [REDACTED] did not have a business reason to use the access which they had been provisioned.</p> <p>When the entity discovered the access-provision error, the entity removed the employee's access. The employee then had a verified PRA performed and retook all required training before access was reinstated. Both before and after the error was cured, the user was provisioned access related to the job role. The business justification was that this [REDACTED] needed access to perform scheduled and emergent work in the substation department.</p> <p>The root cause of this noncompliance was an inadequate process and insufficient training which resulted in a failure to catch a human input data error regarding the PRA date. A PRA administrator responsible for inputting the data for the preparation of CIP Version 5 prior to July 1, 2016, searched an incorrect name and input the date of that individual's PRA into the sheet used as input data.</p> <p>This noncompliance involves the management practice of verification. Verification is involved because the entity's verification procedures were inadequate resulting in the entity's failure to identify the data input error.</p> <p>This noncompliance started on July 2, 2018, when the [REDACTED] was provisioned access and ended on December 12, 2018, when the entity revoked the [REDACTED] access to High Impact facilities.</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 risk posed by the failure to possess a current PRA is the opportunity for a dangerous or malicious actor to access High Impact facilities, and use that access to adversely impact the BPS. The risk here is minimized because the employee without a current PRA was in good standing. Further minimizing the risk, the user was given CIP Training when they were provided access without a current PRA. Upon discovery of the noncompliance and review of the relevant employee's access, the entity determined that the employee did not enter the High Impact facility with their access privileges. No harm is known to have occurred.</p> <p>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 these types of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) immediately disabled the user access to High Impact facilities; 2) informed the users Manager that a new personnel risk assessment (PRA) was needed. The Manager immediately called the HR Representative and ordered a new PRA for the employee; 3) ran a Journal check on the affected employee to assess how many times the access was used. The report showed that the employee only utilized access for general (non-CIP/protected) ingress/egress as well as low impact ingress/egress; and 4) added a step to the access issuance process where the human resource department is required to send a screen capture of the approved PRA to the entity's CIP Compliance Department, which is then added to the identity management system, and access cannot be provisioned until a screen capture of the complete and clear PRA is received. <p>ReliabilityFirst 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
RFC2018019695	CIP-003-6	R1	[REDACTED]	[REDACTED]	4/1/2017	8/14/2018	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 May 4, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance with CIP-003-6 R1. Specifically, the entity did not develop a policy or policies for assets identified in CIP-002 containing low impact Bulk Electric System (BES) Cyber Systems that addressed physical security controls (CIP-003-6 R1.2.2) or electronic access controls for Low Impact External Routable Connectivity and Dial-up Connectivity (CIP-003-6 R1.2.3). The issue was discovered during an internal, comprehensive compliance assessment after [REDACTED]</p> <p>The root cause of this noncompliance was inadequate planning, which resulted in confusion regarding the development and implementation of policies and controls relating to physical security and electronic access for assets containing low impact BES Cyber Systems. This noncompliance implicates the management practice of planning, which includes the need to effectively understand standards and requirements and establish safeguards to avoid an unintentional adverse effect on bulk power system (BPS) reliability and resilience.</p> <p>The violation began on April 1, 2017, when the entity failed to document and have a CIP Senior Manager approve a policy by the enforcement date and ended on August 14, 2018, after the entity documented and obtained necessary approval of the policy.</p>					
Risk Assessment			<p>This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS based on the following factors. The failure to have one or more adequate policies that address physical security and electronic access for assets containing low impact BES Cyber Systems could result in personnel not having proper direction and guidance when creating procedures and processes for and implementing various cyber security matters, thereby increasing the likelihood of a deficient security posture. Here, the risk was minimized based on the following factors. Even though the overarching policy should have been in place and approved on or before April 1, 2017, the actual implementation of the controls subject to that policy (i.e. physical and electronic access controls for Low Impact External Routable Connectivity and Dial-up Connectivity) did not have to occur, initially, until September 1, 2018. And, pursuant to FERC Order 843 approving CIP-003-7 (which supersedes the prior version), the compliance date for the implementation of those physical and electronic controls is January 1, 2020. In summary, this noncompliance is primarily a documentation issue. No harm is known to have occurred.</p> <p>ReliabilityFirst considered each 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) developed a Physical Security Controls and Electronic Access Controls for Low Impact External Routable Connectivity and Dial-up Connectivity policy; 2) conducted training for all effected personnel on the Physical and Electronic Access Control policy; 3) developed a new standard application form to identify implementation time frames for new or modified standards; 4) reviewed corporate compliance policies to ensure that discovered areas of potential non-compliance are corrected promptly; 5) enhanced the [REDACTED] by specifying practices to improve the understanding of current standards and requirements and identify and plan for future standards at the entity; and 6) provided training to staff regarding new [REDACTED] practices for current and future standards and requirements and implementation time frames. <p>ReliabilityFirst 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
SERC2017017323	CIP-010-2	R1, P1.3	[REDACTED]	[REDACTED]	01/01/2017	01/19/2017	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 April 3, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED], it was in noncompliance with CIP-010-2 R1, P1.3. The Entity did not update its baseline configuration within 30 calendar days of completing a change that deviated from the existing baseline configuration.</p> <p>In December 2016, the IOS firmware in [REDACTED] high impact BES Cyber Assets ([REDACTED]) was updated. On December 1, 2016, the Entity completed testing of the update by using the development environment network switches and installed the update on the [REDACTED] production switches at the backup control center. On December 6, 2016, the update was also installed on the production switches at the primary control center. The Network Technicians that performed the update notified the Cyber Compliance Staff that a change had been made, which required a manual update of the baseline for the switches.</p> <p>On January 19, 2017, the Entity conducted a documentation review to assess testing documentation and discovered that the [REDACTED] network switches had inaccurate baselines documented. The [REDACTED] network switches had firmware versions that differed between the baseline documentation and the actual Cyber Assets. The Entity investigated the baseline discrepancy and determined that the documentation associated with [REDACTED] firmware upgrades did not get properly updated after the change, as required. The Entity determined that the post change paperwork and instructions did not result in the appropriate baseline updates to the documentation.</p> <p>The scope of affected assets included [REDACTED] BCAs (switches – [REDACTED] at the primary and [REDACTED] at the backup control center), which are associated with a high impact Bulk Electric System (BES). The Entity performed an extent-of-condition assessment and determined that no other changes that required baseline updates occurred within the December 2016 review period.</p> <p>This noncompliance started on January 1, 2017, when the Entity was required to have updated the existing baseline configuration to reflect the change, and ended on January 19, 2017, when the Entity updated the baseline configuration to reflect the change.</p> <p>The root cause of this noncompliance lack of an internal control and insufficient training. The Network Technicians were responsible for implementing the firmware updates to the subject switches; however, they were not responsible for making changes to the baseline documentation. At monthly review meetings, the Network Technician were instructed to note the need for baseline updates in the change management system. The Cyber Compliance Staff were then expected to review the task notes, recognize that baseline updates were required, and perform the manual updates. More training was required for staff to clearly understand their roles and responsibilities, and there was not an internal control to verify that baseline configurations 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 Entity's failure to update changes that deviate from the existing baseline configuration increased the risk that the Entity would not identify unauthorized changes, which could adversely impact Bulk Electric (BES) System Cyber Systems. However, the baseline documentation update was only 18 days late and only involved [REDACTED] BES Cyber Asset (BCA) network switches out of [REDACTED] total BCAs. The update to the baseline was a documentation or administrative type failure. Thus, the devices were properly updated with the most secure and recent firmware to ensure operational integrity and security. 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) updated the firmware baseline to reflect current firmware level; 2) installed a automated baseline monitoring tool that compares documented baselines to the running configuration in the field and alerts of any changes or anomalies; and 3) trained affected staff on their roles and responsibilities regarding the automated baseline monitoring tool. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018775	CIP-006-6	R1, P1.1	[REDACTED]	[REDACTED]	08/01/2017	08/03/2017	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 December 12, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], [REDACTED], and [REDACTED], it was in noncompliance with CIP-006-6 R1, P1.1. The Entity reported six instances where it did not implement a documented physical security plan that included defining operational or procedural controls to restrict physical access.</p> <p>On August 3, 2017, at approximately 2:30 p.m., an Entity Cyber Security employee contacted Corporate Security to report the discovery of a telephone closet door that was open and unlocked. The door was used to restrict physical access to one Physical Access Control System (PACS) security panel. The PACS security panel housed within the telephone closet had a small security door with a tamper alarm. The employee closed and secured the closet door immediately. That same day, the Entity conducted an investigation to determine who had opened the door, how long it had been open, who had accessed the PACS secured within, and whether unauthorized persons had tampered with the PACS.</p> <p>Corporate Security reviewed video surveillance for the period of July 31, 2017 through August 4, 2017, and determined that the door had been open for 72 hours. The Entity discovered that on August 1, 2017, six service contractors installed a new fire alarm system and that an employee had accessed the closet and left without securing it. The video review concluded that no one had opened or tampered with the security panel or cables attached. In addition to video surveillance, Corporate Security interviewed affected personnel and reviewed all card access transactions and alarms at the door, as well as security panel tamper alarms. The alarm report revealed that, for the period of July 31, 2017 through August 4, 2017, there were several unaddressed open door alarms for the subject door, but there were no unaddressed alarms for the security panel door. Per the Entity, this instance took 72 hours to discover because the security panel door alarm was routed to the Entity's [REDACTED] as a protected door alarm, but the telephone closet door alarm was not. Additionally, local audible door alarms received minimal attention because Entity employees understood the necessity of contractors working in the area.</p> <p>[REDACTED]</p> <p>The Entity conducted an extent-of-condition assessment by reviewing alarms and video footage of the subject area. The Entity found no other instances of noncompliance with CIP-006-6 R1.</p> <p>This noncompliance started on August 1, 2017, when the access door to the PACS was left unsecured, and ended on August 3, 2017, when the employee closed and secured the PACS access door.</p> <p>The root cause of this noncompliance was lack of training and lack of internal controls.</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 Entity's failure to restrict physical access to a PACS for 72 hours could have allowed malicious intruders to make PACS configuration changes or render it inoperable, which could result in unauthorized access to sensitive assets across a wide area and lead to grid disruptions. However, in this instance, multiple layers of physical security were in place. Specifically, the main building required card access and the Entity staffed the main building with guards at all times. Additionally, [REDACTED] for prompt response if the need arose. Moreover, the assets protected by the PACS were themselves protected with the electronic controls required by CIP-005. 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) removed the door's core lock and verified the same with Corporate Security; the door can no longer be accessed by a key and can be accessed by the badge reader only; 2) renamed the door in the Entity door security system to eliminate any confusion as to the location of the door; 3) amended the alarm instructions in the Entity door security system for all "forced door" alarms to include "treat this as an intrusion"; 4) trained contract security personnel on responding to "forced door" alarms; and 5) added signs to the inside and outside of the door indicating that access was controlled and that only authorized persons were allowed 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
SERC2017018720	CIP-007-6	R2, P2.2, P2.4	[REDACTED]	[REDACTED]	07/01/2016	06/30/2018	Self-Report	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>On November 27, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], it had one instance of noncompliance with CIP-007-6 R2. The Entity did not implement a documented process that developed detailed documentation related to the software patching process, including evaluations and applicability, at least once every 35 calendar days (P2.2).</p> <p>On October 1, 2017, during an internal examination of its security patch tracking documentation, the Entity discovered that it had not created any documentation relating to receiving notification of security patches for [REDACTED] switches, [REDACTED] routers and [REDACTED] of its Physical Access Control Systems (PACS), when it evaluated the patches for the applicability of each patch. The Entity’s [REDACTED] assessed and patched its other Bulk Electric System (BES) Cyber Assets (BCAs), associated Protected Cyber Assets (PCAs), and Electronic Access Control and Monitoring Systems (EACMS) on a monthly basis. The Entity used a system center configuration manager to assess and deploy patches on its servers, but the Entity failed to document the applicability of its patches for certain switches, routers and [REDACTED] PACS. The Entity’s [REDACTED] believed that monitoring security mailing lists and vendor websites and then creating a change request when a patch was applicable was sufficient.</p> <p>During a Compliance Audit from [REDACTED] through [REDACTED], SERC discovered another instance with CIP-007-6 R2. The Entity failed to have a documented procedure for its mitigation plan implementation timeframe (P2.4). This instance was assigned [REDACTED], which was dismissed and consolidated with the initial November 27, 2017 Self-Report.</p> <p>The Entity’s patch management process did not specify a timeframe for the implementation of patching mitigation plans. Rather, the Entity utilized email reminders, weekly meetings, and working notes as internal controls to make sure that it followed through and completed its mitigation plans on schedule. On June 30, 2018, the Entity updated its mitigation plan procedure to specify a timeframe for the implementation of mitigation plans.</p> <p>The Entity conducted an extent-of-condition assessment by reviewing its patching and mitigation plan procedures for additional gaps in its process for [REDACTED] of its medium impact BES Cyber Systems. No additional instances of noncompliance with CIP-007-6 R2 were found.</p> <p>The scope of affected facilities included [REDACTED] medium impact BES Cyber Systems (BCSs), which collectively housed [REDACTED] BCAs with associated PACS, PCAs, and EACMS.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on June 30, 2018, when the Entity updated its procedures with its missing mitigation process.</p> <p>The root causes of this noncompliance were training and an incomplete procedure. Specifically, the Entity had a misunderstanding of its patching procedure and an incomplete procedure that did not require CIP Senior Manager (or delegate) approval for any revision or extension to the mitigation plan that might become necessary. Additionally, the Entity’s procedure did not reference that ‘mitigation plans must be implemented in the timeframe specified in the 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 (BPS). The Entity’s failure to document a procedure for its mitigation plan implementation timeframe and its failure to document its security patch evaluation for its switches and routers and [REDACTED] of its PACS could have caused the Entity to fail to assess security patches or complete mitigating activities. Additionally, should a security breach occur, the Entity’s failure to document its security patch evaluations could hinder an investigation into the cause of the breach. However, the Entity deployed the security patches using its change management ticket process and did have a mitigation plan for all security patches. The Entity followed its mitigation schedule using e-mail reminders, weekly meetings, and working notes as internal controls. Moreover, the Entity had patching sources for all its operating systems and accompanying software residing on its BCSs. 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>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed a documented security patch evaluation for its devices and PACS assets; 2) developed spreadsheets for tracking security patches for its devices; 3) retrained the Subject Matter Experts (SMEs) and the PACS service provider on the requirements for monthly patch evaluation, tracking, and documentation procedures; 					

- | |
|--|
| <ol style="list-style-type: none">4) conducted performance evaluations on its SMEs and PACS service providers using a performance checklist;5) provided a reminder to SMEs and the PACS service providers of the required documentation tasks relating to security patches during each end-of-month supervisor meeting;6) created a calendar tracking system to ensure team leads completed patch evaluations at the end of every month;7) updated the CIP-007 procedure to state that CIP Senior Manager (or delegate) approval for any revision or extension to the mitigation plan is required, and to state that mitigation plans needed to be implemented on schedule; and8) trained applicable staff on the updated CIP-007 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
SERC2019021862	CIP-003-6	R1	[REDACTED] (The Entity)	[REDACTED]	02/10/2019	05/01/2019	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 July 22, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED], it was in noncompliance with CIP-003-6 R1. The Entity, for its high and medium impact BES Cyber Systems, failed to obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies.</p> <p>On April 15, 2019, the Entity discovered through an internal review process that its Cyber Security Policy document ([REDACTED]) was not reviewed and approved by the General Manager and the CIP Senior Manager within 15 months of the previous approval, which occurred on November 9, 2017. The Cyber Security Policy document was reviewed and approved on May 25, 2017, and when additional updates were identified on November 9, 2017, the document was again updated, reviewed, and approved by both the General Manager and CIP Senior Manager. However, the document was not reviewed and approved for any additional updates within 15 calendar months of November 9, 2017.</p> <p>This noncompliance started on February 10, 2019, when the Entity was required to obtain CIP Senior Manager approval of the Cyber Security Policy document, and ended on May 1, 2019, when the Entity's CIP Senior Manager reviewed and approved the Cyber Security Policy.</p> <p>The primary causes of this noncompliance were a lack of a documented procedure and an internal control to ensure that the Cyber Security document was timely approved.</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 Entity's failure to obtain CIP Senior Manager's approval of the Cyber Security Policy document every 15 calendar months could have led to reduced awareness and engagement by senior leadership, leading to diminished focus on compliance by the utility. The risk posed by this noncompliance was mitigated because no meaningful changes were needed or made to the Cyber Security Policy, and the duration of the noncompliance was less than three months. 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, Entity:</p> <ol style="list-style-type: none"> 1) obtained CIP Senior Manager review and approval of the revised Cyber Security Policy document; 2) updated a deliverable due date for the next required review and approval to reflect 15 months from the current revision/approval; 3) developed and implemented an identifier/key date field within Compliance Database tasks for updating, reviewing, and approving Cyber Security Policy document; 4) updated the deliverable "Key Date" to reflect the 15-month requirement deadline for future annual review and approval of the Cyber Security Policy; 5) developed a procedure for compliance database tracking to address the approval of the Cyber Security Policy document; and 6) trained applicable personnel on procedure to address out-of-cycle due date management. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017321	CIP-010-2	R1, P1.1.4	[REDACTED]	[REDACTED]	07/01/2016	03/22/2018	Compliance 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 violation.)			<p>During a Compliance Audit conducted from [REDACTED] through [REDACTED], SERC determined that the Entity, as a [REDACTED], [REDACTED] and [REDACTED], was in noncompliance with CIP-010-2 R1, P1.1.4. The Entity failed to include enabled logical network accessible ports in its baseline configuration for [REDACTED] Cyber Assets.</p> <p>SERC identified [REDACTED] devices with baseline documentation that did not match the device configurations. For these devices, the Entity incorrectly assigned the wrong ports. For instance, the Entity utilized its [REDACTED] definition of [REDACTED], which was derived from its [REDACTED] configuration file and was intended to cover all needed ports, and included all ports from [REDACTED]. However, the Entity should have used the Microsoft definition of [REDACTED], which uses the ports between [REDACTED].</p> <p>The Entity’s affected Bulk Electric System (BES) Cyber Systems included [REDACTED] BES Cyber Assets (BCAs), [REDACTED] Protected Cyber Assets (PCAs) and [REDACTED] Electronic Access Control and/or Monitoring Systems (EACMSs) associated with [REDACTED] medium impact BES Cyber Systems.</p> <p>The Entity used its [REDACTED] tool to conduct its extent-of-condition on all Window devices that [REDACTED] monitored. The Entity found no other instances of this issue.</p> <p>This noncompliance started on July 1, 2016, when the standard became mandatory and enforceable, and ended on March 22, 2018, when the Entity updated its baseline configuration to reflect logical network accessible ports.</p> <p>The root cause of this noncompliance was a misinterpretation of what was required for port identification. The Entity erroneously determined that the [REDACTED] definition of [REDACTED] assigned the correct port ranges for the affected Cyber 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. The Entity’s failure to accurately document and track changes that deviate from existing baseline configurations increased the risk that the Entity would not identify authorized changes, which could negatively affect the bulk power system. However, the Entity physically disconnected its [REDACTED] system from its vendor support and would only connect it when the Entity needed outside support, but they still had Inter-Control Center Communications Protocol connectivity, as well as corporate connectivity, through a jump host and firewall. Also, the Entity used a monitoring device to continuously monitor for any changes to its baseline. In addition to its [REDACTED], the Entity also disabled its optical drives and uses physical port blockers used to block access to [REDACTED] system USB ports and open [REDACTED] ports. Also, the Entity’s PACS system is a [REDACTED] system, which is completely isolated and is not provisioned for remote access. 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) discontinued the use of [REDACTED] and updated the Entity’s [REDACTED]; 2) modified the [REDACTED] by adding the statement “nonspecific references, such as the use of the word [REDACTED] are not an acceptable practice”; and 3) trained CIP Compliance personnel on the updated program document. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017018555	CIP-007-6	R5.6	[REDACTED] (the "Entity")	[REDACTED]	10/01/2017	01/19/2018	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 violation.)			<p>On November 2, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-007-3a R5. Specifically, the Entity discovered that passwords for [REDACTED] accounts on a device classified as an Electronic Access Control or Monitoring System associated with a [REDACTED] BES Cyber System had not been changed at least once every 15 calendar months. Texas RE determined that the applicable standard is CIP-007-6 R5.6, as the device was not subject to CIP-007-3a R5 and only became subject to CIP-007 as part of the transition to version five of the CIP standards. As a result, Texas RE determined that [REDACTED] passwords were not changed at least once every 15 calendar months. The Entity determined that it had inadvertently failed to include the accounts in question in its password management report.</p> <p>The root cause for this noncompliance was a lack of preventative controls to verify that all applicable accounts, including accounts from applications, were included in the Entity's password management process.</p> <p>This noncompliance started on October 1, 2017, when the Entity failed to change passwords for accounts on the device 15 calendar months after CIP-007-6 went into effect on July 1, 2016, and ended on January 19, 2018, when the Entity finished changing the passwords for the affected accounts.</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 changed all but one of the passwords within one month of the noncompliance start date and the remaining password within four months of the noncompliance start date, resulting in a short-lived noncompliance. Second, [REDACTED] passwords that were not changed belonged to accounts that had read-only access to the application, greatly limiting the amount of harm that could have resulted from unauthorized access. Third, the accounts only allowed access to a web application and did not allow access to the cyber asset hosting the application. Fourth, the accounts the passwords belonged to had no ability to affect access control and monitoring for the Entity's Electronic Security Perimeter (ESP), further reducing the amount of harm that could have resulted from unauthorized access. No harm is known to have occurred.</p> <p>Texas RE determined that the Entity's compliance history should not serve as a basis for applying a penalty. In [REDACTED], Texas RE determined that the Entity had an instance of noncompliance with CIP-007-3a R5.3.3 and CIP-007-6 R5.6. However, the root cause of that instance is different from the present instance. In the previous instance, the Entity did not have an adequate control to ensure that passwords were changed as required and relied on a manual password review instead. In the present instance, the Entity did not have an adequate control to ensure that all applicable accounts were included in the Entity's password management process.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) changed the passwords for the affected accounts; 2) performed an extent of condition review, which identified [REDACTED] that had not had its password changed at least once every 15 calendar months; the device and account were retired on June 29, 2018, to mitigate the issue; the extent of condition review also identified other application accounts not included in the Entity's password management process, but these accounts were subject to a 90-day password expiration policy, and therefore did not constitute an additional instance of noncompliance; 3) [REDACTED] to prevent recurrence of the root cause; 4) [REDACTED]; 5) [REDACTED]; and 6) implemented process updates and enhancements to controls and trained responsible personnel. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018020401	CIP-005-5	R1; R1.1	[REDACTED] (the "Entity")	[REDACTED]	01/17/2018	06/08/2018	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 violation.)			<p>On September 11, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-005-5 R1. In particular, the Entity failed to ensure that [REDACTED] applicable Cyber Assets connected to a network via a routable protocol resided within a defined Electronic Security Perimeter (ESP).</p> <p>On January 17, 2018, when the Entity was in the process of restructuring an ESP, [REDACTED] workstation Cyber Assets were removed from the ESP because the Entity believed that these devices would no longer be in-scope for the purposes of CIP-005-5 R1. Specifically, the Entity intended for these devices to have view-only access to the Entity's SCADA systems, such that they would no longer be able to control SCADA systems or qualify as BES Cyber Assets. On June 8, 2018, while performing a vulnerability assessment, the Entity discovered that these devices still had some control capabilities [REDACTED], and the Entity removed these control capabilities on the same day when the issue was discovered, ending the noncompliance.</p> <p>The root cause of this issue is that the Entity did not devote sufficient resources to the restructuring of the ESP. Specifically, the Entity stated that the restructuring was performed by a single employee, [REDACTED] before the restructuring was completed. The Entity has since hired additional personnel in order to improve its compliance program.</p> <p>This noncompliance started on January 17, 2018, when the Entity restructured its ESP to exclude the devices with the SCADA control capabilities, and ended on June 8, 2018, when the Entity removed the control capabilities from the devices 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 (BPS). The risk posed by this issue is that an unauthorized individual could gain access to the devices at issue and control SCADA systems, including potentially activating the Entity's breakers. However, the risk posed by this issue was reduced by the following factors. First, the Entity had other controls in place to prevent unauthorized access. Specifically, the devices were located inside a physically secured location, and were automatically monitored by the Entity's change management and baselining software, as well as the Entity's implemented method to detect malicious code. The devices did not have external routable connectivity, and they continued to be included in the Entity's security patching program. Second, the Entity is [REDACTED]. Finally, based on a review of the Entity's logs, the Entity did not detect any unauthorized access to the devices during the noncompliance. No harm is known to have occurred.</p> <p>Texas RE 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) removed the ability for the devices at issue to control SCADA systems; 2) trained applicable users regarding the revised method for accessing SCADA information on the devices at issue; 3) assigned additional personnel to implement the Entity's process for compliance with CIP-005-5 R1; and 4) removed the installation program that had been originally used on the devices at issue from the Entity's network storage and moved the physical installation media [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
TRE2017018659	CIP-007-6	R5.6	[REDACTED] (the "Entity")	[REDACTED]	10/01/2017	01/19/2018	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 violation.)			<p>On November 14, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-007-3a R5. Specifically, the Entity discovered that passwords for [REDACTED] accounts on a device classified as an Electronic Access Control or Monitoring System associated with a [REDACTED] BES Cyber System had not been changed at least once every 15 calendar months. Texas RE determined that the applicable standard is CIP-007-6 R5.6, as the device was not subject to CIP-007-3a R5 and only became subject to CIP-007 as part of the transition to version five of the CIP standards. As a result, Texas RE determined that [REDACTED] passwords were not changed at least once every 15 calendar months. The Entity determined that it had inadvertently failed to include the accounts in question in its password management report.</p> <p>The root cause for this noncompliance was a lack of preventative controls to verify that all applicable accounts, including accounts from applications, were included in the Entity's password management process.</p> <p>This noncompliance started on October 1, 2017, when the Entity failed to change passwords for accounts on the device 15 calendar months after CIP-007-6 went into effect on July 1, 2016, and ended on January 19, 2018, when the Entity finished changing the passwords for the affected accounts.</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 changed [REDACTED] the passwords within one month of the noncompliance start date and [REDACTED] within four months of the noncompliance start date, resulting in a short-lived noncompliance. Second, [REDACTED] passwords that were not changed belonged to accounts that had read-only access to the application, greatly limiting the amount of harm that could have resulted from unauthorized access. Third, the accounts only allowed access to a web application and did not allow access to the cyber asset hosting the application. Fourth, the accounts the passwords belonged to had no ability to affect access control and monitoring for the Entity's Electronic Security Perimeter, further reducing the amount of harm that could have resulted from unauthorized access. No harm is known to have occurred.</p> <p>Texas RE 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) changed the passwords for the affected accounts; 2) performed an extent of condition review, [REDACTED] 3) revised the password management process to prevent recurrence of the root cause; 4) developed a new preventative internal control to identify accounts excluded from the password management process; 5) enhanced the reporting of the existing detective control used to monitor password changes; and 6) implemented process updates and enhancements to controls and trained responsible personnel. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017018671	CIP-008-5	R3.1	[REDACTED] (the "Entity")	[REDACTED]	06/20/2017	11/14/2017	Compliance 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 violation.)			<p>During a Compliance Audit conducted from [REDACTED] Texas RE determined that the Entity, as a [REDACTED] and [REDACTED], was in noncompliance with CIP-008-5 R3. Specifically, the Entity failed to timely update its Cyber Security Incident response plan based on any documented lessons learned associated with the plan within 90 days after the completion of a Cyber Security Incident response plan test, as required by CIP-008-5 R3, Part 3.1.</p> <p>On March 21, 2017, the Entity conducted a Cyber Security Incident response plan test and documented the lessons learned from the exercise. In particular, the Entity's lessons learned noted that the Cyber Security Incident response plan should be revised to [REDACTED]. The 90-day deadline for the Entity to update its Cyber Security Incident response plan based on the documented lessons learned fell on June 19, 2017. However, the Entity's updated Cyber Security Incident response plan did not become effective until November 14, 2017. Accordingly, the duration of this issue is from June 20, 2017, to November 14, 2017.</p> <p>The root cause of this issue is that the Entity did not have a sufficient process for compliance with CIP-008-5 R3. [REDACTED].</p> <p>This noncompliance started on June 20, 2017, which is the first day after the 90-day deadline for the Entity to update its Cyber Security Incident response plan, and ended on November 14, 2017, when the Entity's updated Cyber Security Incident response plan became effective.</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 this issue is that the Entity's Cyber Security Incident response plan would not give adequate instructions in the case of a Cyber Security Incident. However, the risk posed by this issue is reduced by the following factors. First, this issue occurred following a Cyber Security Incident response plan test, rather than an actual event, and the noncompliance was limited to the Entity's documentation only. In addition, the Entity did not experience a Reportable Cyber Security Incident during the noncompliance, meaning that the documentation issue did not have an actual impact on the BPS. Finally, the Entity's extent of condition review determined that this issue was limited to a single instance of noncompliance. No harm is known to have occurred.</p> <p>Texas RE 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) updated its Cyber Security Incident response plan based on the documented lessons learned from the March 21, 2017 response plan test; 2) revised its Cyber Security Incident response plan [REDACTED] regarding the 90-day deadline to update the Cyber Security Incident response plan; 3) communicated by email the revisions to its Cyber Security Incident response plan to the Entity's personnel; and 4) conducted training for the Entity's personnel regarding the Entity's Cyber Security Incident response plan. <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
TRE2017018674	CIP-007-6	R2; R2.1	[REDACTED] (the "Entity")	[REDACTED]	07/01/2016	03/16/2018	Compliance 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 violation.)			<p>During a Compliance Audit conducted from [REDACTED] Texas RE determined that the Entity, as a [REDACTED] and [REDACTED] was in noncompliance with CIP-007-6 R2. Specifically, the Entity's documented patch management process did not include the identification of a source or sources that the Entity tracks for the release of cyber security patches for its Physical Access Control Systems (PACS), as required by CIP-007-6 R2, Part 2.1. On March 16, 2018, the Entity adopted a documented process that identified the sources that the Entity tracks for the release of cyber security patches for its PACS, ending the noncompliance.</p> <p>The root cause of this issue is that the Entity's documentation did not fully describe its process. Specifically, although the Entity's documented process [REDACTED] the documented process did not specifically identify the tracked sources.</p> <p>This noncompliance started on July 1, 2016, when CIP-007-6 R2 became enforceable, and ended on March 16, 2018, when the Entity adopted a revised documented process that identified the sources that the Entity tracks for the release of cyber security patches for its PACS.</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 Entity owns [REDACTED] PACS devices that are associated with [REDACTED] control centers and [REDACTED] substations that contain [REDACTED] BES Cyber Systems. However, this issue was limited to the Entity's documentation only. In particular, although the Entity's documented process did not specifically identify the sources that the Entity tracks, the process for [REDACTED] was stated in more general detail. In addition, the Compliance Audit did not identify any issues regarding the implementation of the Entity's process for compliance with CIP-007-6 R2. Specifically, the Compliance Audit did not identify any late or missing cyber security patches for any of the sampled Cyber Assets, including for any PACS. No harm is known to have occurred.</p> <p>Texas RE 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) adopted a revised documented process that identified the sources that the Entity tracks for the release of cyber security patches for its PACS; and 2) communicated the revised documented process to the Entity's personnel. <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
TRE2017018675	CIP-006-6	R1; R1.2	[REDACTED] (the "Entity")	[REDACTED]	10/18/2017	10/18/2017	Compliance 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 violation.)			<p>During a Compliance Audit conducted from [REDACTED], Texas RE determined that the Entity, as a [REDACTED] and [REDACTED] was in noncompliance with CIP-006-6 R1. Specifically, the Entity failed to implement its physical access control for the applicable Physical Security Perimeter (PSP) at a single substation containing a [REDACTED] BES Cyber System.</p> <p>On [REDACTED] the Compliance Audit team conducted a walkthrough of the [REDACTED], during which the Compliance Audit team identified that a door lock did not properly latch when closed. The failure of this physical access control could have allowed unauthorized physical access to the PSP through the rear door of the substation. Within minutes after the discovery of this issue, the Entity adjusted the door so that the door lock would latch properly.</p> <p>The root cause of this issue is that the physical access control failed due to routine use, which had not been identified by the Entity prior to the Compliance Audit. In order to prevent recurrence of this issue, the Entity performed security reviews of all substations containing [REDACTED] BES Cyber Systems.</p> <p>This noncompliance started and ended on [REDACTED], when the door lock did not properly latch and was subsequently repaired.</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 issue is that an unauthorized individual could obtain physical access to the [REDACTED] BES Cyber System present at the [REDACTED]. However, the risk posed by this issue is reduced by the following factors. First, other physical controls, including Physical Access Control System alarms, were functioning during the noncompliance and alerted the Entity's personnel when the noncompliance occurred. In addition, the issue was quickly corrected after it was discovered. Specifically, the Entity's alarm records indicate that the door was repaired within three minutes of the first alarm triggered by the door lock's failure to properly latch. During this time, no unauthorized individuals accessed the door at issue. Finally, the Entity's extent of condition review determined that this issue was limited to a single instance occurring at the [REDACTED]. No harm is known to have occurred.</p> <p>Texas RE 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) repaired the physical access control at issue; and 2) documented security reviews of all substations containing [REDACTED] BES Cyber Systems, which were performed by a security contractor and which include recommendations to improve physical security for each site. <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
TRE2018020572	CIP-010-2	R4	[REDACTED] (the "Entity")	[REDACTED]	07/16/2018	07/16/2018	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 violation.)			<p>On October 23, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-010-2 R4. In particular, the Entity reported that an escorted individual connected an unauthorized Transient Cyber Asset to a [REDACTED] BES Cyber System. The Entity awarded a work project to perform work at a substation containing [REDACTED] BES Cyber Systems to a third party. This work necessitated connecting a laptop [REDACTED].</p> <p>The root cause of this noncompliance was a lack of a verification process for ensuring work at substations containing [REDACTED] BES Cyber Systems was not assigned to third parties and a misunderstanding of the categorization of the BES Cyber Systems at a particular substation. The Entity's cyber security plan prohibits third parties from being awarded work projects at substations that contain [REDACTED] BES Cyber Systems. The department responsible for assigning contracts to third parties believed that the affected substation only contained [REDACTED] BES Cyber Systems. Due to this misunderstanding and the lack of appropriate oversight, the work was inappropriately awarded to a third party vendor.</p> <p>This noncompliance started on July 16, 2018, when a third party contractor connected their laptop to [REDACTED] that is part of a [REDACTED] BES Cyber System and ended on July 16, 2018, when the contractor disconnected the laptop from [REDACTED].</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 contractor was acting in good faith and performing work that had been assigned by the Entity to their employer.</p> <p>The risk due to this noncompliance is reduced due to the following:</p> <ol style="list-style-type: none"> 1) upon discovering the noncompliance the Entity reviewed logs of actions performed by the contractor and verified that no suspicious activities had occurred; 2) the Entity executed a confidentiality agreement with the contractor, in which the contractor agreed to hold confidential any information concerning the Entity's assets; 3) in addition to the confidentiality agreement between the contractor and the Entity, the contractor's employment contract also prohibits the contractor from divulging information obtained from the Entity; and 4) an escort was present with the contractor at the substation. <p>No harm is known to have occurred.</p> <p>Texas RE 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) the contractor disconnected their laptop from [REDACTED]; 2) verified no other substations containing [REDACTED] BES Cyber Systems were assigned to third party contractors; 3) implemented a process for reviewing and approving third party work schedules to ensure no work is assigned at a substation containing [REDACTED] BES Cyber Systems; and 4) provided reinforcement training reiterating that third party contractors cannot perform work at substations containing [REDACTED] BES Cyber Systems. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019171	CIP-005-5	R1; R1.3	██████████ (the Entity)	██████████	07/01/2016	11/30/2017	Compliance 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 violation.)			<p>During a Compliance Audit conducted from ██████████, Texas RE determined that the Entity, as a ██████████ was in noncompliance with CIP-005-5, R1.3. Specifically, the Entity was missing the justification for the access permissions of one firewall rule.</p> <p>The root cause of the noncompliance was a reliance on one subject matter expert to ensure that access permissions are justified.</p> <p>This noncompliance started on July 1, 2016, when CIP-005-5 R1 became enforceable, and ended on November 30, 2017, when the justification for the access permissions were added to the firewall rule.</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 rule was needed to allow traffic ██████████. No harm is known to have occurred.</p> <p>Texas RE 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) added the justification for the access permissions to the firewall that had been missing justification; and 2) ██████████. <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
TRE2018019175	CIP-010-2	R1; 1.2 and 1.3	██████████ ("the Entity")	██████████	08/01/2016	02/22/2018	Compliance 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 violation.)			<p>During a Compliance Audit conducted from ██████████ Texas RE determined that the Entity, as a ██████████ was in noncompliance with CIP-010-2, R1. Specifically, the Entity did not authorize and document changes that deviated from the existing baseline configurations Cyber Assets, and did not provide evidence updating the baseline configuration within 30 calendar days of completing changes for several Cyber Assets.</p> <p>The root cause of this noncompliance was insufficient communication and coordination from the Entity's compliance specialist to the ██████████ leading to misinterpretation of the standards. Additionally, a lack of NERC CIP training within the ██████████ led to this noncompliance, and some of the Entity's tools that were implemented to support the standard were lacking the needed functionality.</p> <p>This noncompliance started on July 1, 2016, when the revised standard went into effect, and ended on February 22, 2018, when the Entity implemented a tool to enhance reporting ability for changes to existing baselines.</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. Executing changes on CIP assets without authorization and proper documentation reduces the ability to track and mitigate potential failures as well as visibility of the baseline configuration. This reduction can lead to the inability to identify and verify cyber security control modifications, therefore increasing the risk to potential vulnerabilities of the BES Cyber Systems. However, these risks were mitigated by the following factors. By the end of the 12-month audit review period ██████████ for the ██████████, the Entity had properly authorized and documented changes from its existing baseline configurations for all but ██████████, and those ██████████ were shown to be updated appropriately through mitigation activities. Further, Texas RE determined that in 2016 and 2017, all servers were being fully patched based on the screenshots provided during the audit, including on the ██████████ noted above. No harm is known to have occurred.</p> <p>Texas RE 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) updated its baseline configurations; 2) implemented a tool to enhance reporting ability for changes to existing baselines; and 3) held trainings for all affected 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
WECC2018020620	CIP-010-2	R1; P1.4.1	[REDACTED]	[REDACTED]	9/6/2018	9/20/2018	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 October 31, 2018, the entity submitted a self-log stating, as a [REDACTED], it had a potential noncompliance with CIP-010-2 R1 Part 4.1. Specifically, the entity failed to implement one or more of its documented process(es) that collectively included each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management and Table R2 – Configuration Monitoring.</p> <p>On September 6, 2018, the entity initiated a large-scale application installation [REDACTED] that contained both CIP and non-CIP assets. The intended scope of the installation was limited to non-CIP assets with the change authorized through the entity’s change management process. To facilitate the installation effort, a list of assets was created and reviewed by the entity’s personnel to ensure completeness. The review missed [REDACTED] Electronic Access Control or Monitoring Systems (EACMS) associated with its High Impact Bulk Electric System (BES) Cyber System (HIBCS) which resulted in the application being installed on the two Cyber Assets.</p> <p>On September 12, 2018, while performing compliance activities related to CIP-010-2, the entity discovered exceptions to the documented baseline configuration for the [REDACTED] EACMS that resulted from the inadvertent application installation mentioned previously. Upon discovery, the entity launched a change request to uninstall the application. During execution of the workflow associated with the removal of the application, entity personnel performed tasks associated with CIP-010-2 R4 P1.4. The entity identified network accessible ports as the only security control that might be impacted; however, the baseline configuration review associated with the removal of application demonstrated that no network accessible ports were opened because of the application installation. As such, the entity identified noncompliance with CIP-010 R4 P1.4 associated with the application installation on the [REDACTED] EACMS because the entity utilized workflows designed to document the performance of certain requirements of CIP-010-2 during changes to Cyber Assets. More specifically, the workflow included tasks that document the entity’s review and verification of cyber security controls that may be impacted by a change. In this case, because the intended scope of the application installation change did not include Cyber Assets, the entity did not launch those specific workflow tasks.</p> <p>After reviewing all relevant information, WECC determined the entity failed CIP-010-2 R1 Part 1.4. The root cause of the issue was attributed to a lack of internal controls. Specifically, the entity did not have a review process in place to adequately confirm the assets within scope of the change to ensure no CIP assets would be impacted by the change.</p> <p>This issue began on September 6, 2018 when prior to the change that deviated from the existing baseline configuration, the entity should have determined required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change for the [REDACTED] EACMS and ended when the entity completed the removal of the application on the [REDACTED] EACMS on September 20, 2018, for a duration of 15 days.</p>					
Risk Assessment			<p>WECC determined 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, prior to a change that deviated from the existing baseline configuration on [REDACTED] EACMS, the entity failed to determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change as required by CIP-010-2 R1 Part 1.4 sub-part 1.4.1</p> <p>Such failure could potentially affect the security of the Electronic Security Perimeter (ESP) and create vulnerabilities within the HIBCS that if exploited, could ultimately lead to system instability and loss of Load. However, as compensation, the [REDACTED] EACMS were protected by multiple defenses in depth. Specifically, the affected EACMS were located within a Physical Security Perimeter (PSP) and were electronically located within a secure DMZ with restricted access. Additionally, Interactive Remote Access (IRA) to the EACMS required dual factor authentication; logging and alerting were enabled, and the EACMS were monitored for unauthorized access and malware detection. Lastly, during the change, the only security controls that could potentially be impacted were the network accessible ports. After the baseline review, it was determined that no network accessible ports had been opened because of the application installation. No harm is known to have occurred.</p>					

Mitigation	<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none">1. uninstalled the application software from the [REDACTED] EACMS;2. updated its process to include an internal control step to validate the asset list and confirm that no other changes are currently underway that could impact CIP assets;3. evaluated additional documentation and processes associated with mixed environments and updated as needed; and4. provided training to all applicable employees on the updated process and emphasized lessons learned. <p>WECC verified the entity's 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
WECC2018020621	CIP-010-2	R2 P2.1	[REDACTED]	[REDACTED]	1/13/2017	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 violation.)			<p>On October 31, 2018, the entity submitted a Self-Log stating that, as a [REDACTED], it had a potential noncompliance with CIP-010-2 R2 P2.1. Specifically, the entity failed to implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table 2 – Configuration Monitoring.</p> <p>The entity utilized a workflow tool to notify system teams of upcoming work. The workflows allowed the entity to document the performance of CIP activities. On August 1, 2018, the entity discovered one instance when the workflow used to record the monitoring for changes to the baseline configuration of a Cyber Asset associated with a High Impact BES Cyber System (HIBCS) had been marked complete outside of the 35 calendar day window. In a typical baseline configuration monitoring cycle, this workflow would launch every 28 days. System teams then have seven days to review any changes to the applicable Cyber Assets baseline configuration and mark their tasks complete within the 35 calendar day window. The system teams utilized documented Cyber Asset baseline configurations to review for unauthorized changes within the 35 calendar day window. Any changes discovered were investigated, and any unauthorized change were documented and investigated.</p> <p>The entity initiated an extent-of-condition investigation to evaluate the results of all 35 calendar day baseline configuration monitoring workflows completed since July 1, 2016. The investigation identified [REDACTED] additional instances of Cyber Assets associated with a HIBCS where baseline configuration monitoring workflow had been marked complete outside of the 35 calendar day window. As such, the entity determined it did not have evidence to substantiate that it had been monitoring at least once every 35 calendar days for changes to baseline configuration for [REDACTED] Cyber Assets; however, it did have evidence that the [REDACTED] Cyber Assets underwent baseline configuration reviews within two to 10 days after the 35 calendar day window. No unauthorized changes took place on any of the [REDACTED] Cyber Assets in scope. The duration of this issue was 10 days.</p> <p>After reviewing all relevant information, WECC determined the entity failed CIP-010-2 R2 Part 2.1. The root cause of these instances was attributed to a less than adequate baseline monitoring process. There was an oversaturation of notifications from the entity’s workflow tool with no escalation ability for approaching deadlines in baseline monitoring process. The oversaturation of these notifications contributed to the system teams lack of awareness leading to miss the closure windows for their respective workflows.</p> <p>This issue began on June 11, 2018 when monitoring at least once every 35 calendar days for changes to baseline configurations did not occur for the first instance and ended on June 11, 2018 when monitoring resumed in the third instance.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In these instances, the entity failed to monitor at least once every 35 calendar days for changes to baseline configurations for [REDACTED] Cyber Assets, as required by CIP-010-2 R2 Part 2.1.</p> <p>Such failure could result in the Cyber Assets being changed without the entity’s knowledge. Unknown changes could result in the Cyber Asset’s instability, introduction of malicious code, or control of the system operator console resulting in loss of visibility to generation, transmission, and/or balancing that the entity performs. However, as compensation, the Cyber Assets were located within an Electronic Security Perimeter, protected by a Physical Security Perimeter, required dual factor authentication for IRA, logging and alerting were enabled, monitoring for malware was implemented, and access was limited to all identified assets by forcing all IRA through the entity’s Intermediate Systems. Lastly, existing baselines were utilized to determine that no unauthorized changes occurred on any of the [REDACTED] Cyber Assets. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1. completed monitoring of the baseline configurations; 2. required all system teams to complete monitoring tasks within the same seven-day window; 3. modified workflow to include escalation if workflow is not completed in a predefined time frame; and 4. modified content/number of notifications from its change management system to highlight impending deadlines. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018528	CIP-010-2	R3	[REDACTED]	[REDACTED]	7/1/2017	7/24/2017	Self-Report	Completed OR 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 violation.)			<p>On October 27, 2017, the entity submitted a Self-Report stating, as a [REDACTED], it had a potential noncompliance with CIP-010-2 R3. Specifically, on July 3, 2017 the entity discovered through an internal outreach that it had misinterpreted the deadline for conducting a vulnerability assessment (VA). A VA should have been conducted by July 1, 2017, the initial performance date required in the NERC Implementation Plan for Version 5 CIP-010-2 R3. When the entity discovered the noncompliance, it had begun working on completing the required VA for CIP applicable Cyber Assets associated with the High Impact BES Cyber System (HIBCS). However, since the entity originally thought they had more time, it had not yet completed the VA for [REDACTED] Cyber Assets, which included BES Cyber Assets, Protected Cyber Assets, Physical Access Control Systems, and Electronic Access or Monitoring Systems associated with [REDACTED] HIBCS and [REDACTED] Medium Impact BES Cyber Systems.</p> <p>After reviewing all relevant information, WECC determined the entity failed CIP-010-2 R3 Part 3.1. The root cause of the issue was attributed to a less than adequate implementation process that didn't take into consideration any special circumstances. Specifically, the entity was in the process of performing the appropriate VAs as required by Part 3.1, however it did not consider the initial performance dates as stated in the NERC CIP Version 5 Implementation Plan related specifically to Part 3.1 of the Standard and Requirement.</p> <p>This issue began on July 1, 2017 when the Standard and Requirement became mandatory and enforceable and ended on July 24, 2017 when the entity completed the VAs, for a duration of 24 days.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to conduct a VA by the initial performance date required in the NERC CIP Version 5 Implementation Plan for CIP-010-2 R3 Part 3.1, for [REDACTED] applicable Cyber Assets.</p> <p>Such failure could lead to the entity being unaware of vulnerabilities within their system, allowing malicious actors to gain access and potentially cause loss of visibility and control [REDACTED]. However, the entity was working on the VA and had not been able to complete it by the expected due date. Additionally, the entity's VAs resulted in only [REDACTED] Cyber Assets with a potential vulnerability that required an action plan, none of which were high priority or easily exploitable. As compensation, the Cyber Assets were protected with a defense-in-depth strategy consisting of physical, technical, and administrative controls which created multiple layers of systems security significantly decreasing the likelihood of any potential harm from occurring. Specifically, the entity had a patch management program in place which independently assessed and addressed security patches separate from the VA, logging and monitoring of network access was being monitored 24/7, anti-malware prevention as well as network intrusion detection were in place.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1. completed the required VA on the Cyber Assets in scope; 2. updated its procedure to accurately reflect the timeframe requirements; <ol style="list-style-type: none"> a. added calendar invitations to be utilized as an internal control; b. included a timetable for future actions; c. clarified the timing and requirements of the initial performance of the VA as required by the Implementation Plan; d. indicated the group responsible for answering any questions should they arise about the regulatory requirements associated with the VAs; and e. created meeting notices for future performance of VAs; 3. invitations were sent to numerous calendars from different groups to avoid a single point of failure; 4. invitations are spaced for different days to ensure the VAs are completed within the required timeframe; 5. invitations are equipped with notifications alerts which increase in frequency as the deadline nears; and 6. conducted cross-training to increase the number of personnel qualified to perform VAs. <p>WECC verified completion of 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
WECC2018019132	CIP-004-6	R4: P4.1, P4.1.3.	[REDACTED]	[REDACTED]	01/24/2018	01/25/2018	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 violation.)			<p>On February 7, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R4. Specifically, the entity granted one individual unauthorized access to its document management system, a designated storage location for Bulk Electric System (BES) Cyber System Information (BCSI). The entity had implemented an automated process for provisioning access to its BCSI storage location. However, on January 24, 2018, a member of management emailed the database administrator directly and requested, outside of the automated provisioning process, that the administrator grant one individual access to the entity’s document management system. The issue ended on January 25, 2018 when the entity detected that unauthorized access had been granted and ordered the access removed, for a duration of two days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to appropriately perform CIP-004-6 R4 Part 4.1 sub-part 4.1.3. The root cause of the issue was attributed to an incorrect assumption that a correlation existed between two facts; specifically, the administrator that granted unauthorized access to one individual assumed the access was authorized because access had been requested by a member of management.</p>					
Risk Assessment			<p>In this instance, the entity failed to adequately implement its documented access management program to authorize based on need, access to designated storage locations for BCSI when one individual was granted unauthorized access to a designated storage location for BCSI.</p> <p>Failure to properly authorize and manage access to BCSI could have resulted in exposure of sensitive data or improper handling of the BCSI. However, the individual granted unauthorized access was unaware that the access had been granted and therefore did not actually access BCSI. Further, the entity implemented weekly reviews of all access granted in the previous seven days, which is how this issue was discovered. Finally, the individual’s role required access to the BCSI storage location and access was requested, authorized, and granted appropriately a week after the issue. No harm is known to have occurred.</p> <p>WECC 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) removed the employee’s unauthorized access; and 2) required the employees involved in this issue, review and confirm understanding of the access management program documentation and process. <p>WECC 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
WECC2018019302	CIP-002-5.1	R2: P2.1, P2.2	[REDACTED]	[REDACTED]	07/01/2016	02/15/2018	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 violation.)			<p>On February 28, 2018, the entity submitted a Self-Certification stating, as a [REDACTED], it was in potential noncompliance with CIP-002-5.1a R2. Specifically, the entity could not provide evidence sufficient to demonstrate that its Critical Infrastructure Protection (CIP) Senior Manager approved the identification of a single Low Impact BES Cyber System (LIBCS) with External Routable Connectivity made pursuant to its procedures for CIP-002-5.1a R1 by July 1, 2016 when the initial performance of CIP-002-5.1a R2 Part 2.2 should have occurred. Additionally, the entity could not find evidence that it had reviewed the identifications made pursuant to CIP-002-5.1a R1 by October 1, 2017, or within 15 calendar months of the prior identification as required in CIP-005-2.1a R2 Part 2.1. As such, this issue began on July 1, 2016, when the initial performance of CIP-002-5.1a R2 Part 2.2 should have occurred and ended on February 15, 2018, when the entity reviewed the identifications made pursuant to CIP-002-5.1a R1 and its CIP Senior Manager approved those identifications, for a total of 595 days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to appropriately evidence its implementation of CIP-002-5.1a R2 Parts 2.1 and 2.2. The root cause of the issue cannot be fully ascertained as the prior vendor associated with the entity’s CIP-002-5.1a implementation efforts is no longer with the entity and did not adequately respond to the entity’s request for information regarding location of the evidence necessary to demonstrate the entity’s completion of the identifications and approvals required in CIP-002-5.1a R2 Parts 2.1 and 2.2.</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. In this instance, the entity failed to have its CIP Senior Manager perform an initial approval of the identifications made pursuant to Requirement 1 as required in CIP-002-5.1a R2 Part 2.2; additionally, the entity failed to review the identifications made in Requirement 1 and its parts at least every 15 calendar months as required in CIP-002-5.1a R2 Part 2.1</p> <p>Such failures could have resulted in the entity not identifying or mis-categorizing a BES Cyber System, and lead to ineffective or nonexistent protective measures for the Cyber Assets in and associated with the BES Cyber System. However, the entity has [REDACTED] identified LIBCS associated with a [REDACTED] and is not considered a firm resource. Further, the entity’s list of BES Cyber Systems did not change during the noncompliance period therefore, no systems were overlooked and not protected. No harm is known to have occurred.</p> <p>WECC 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) conducted a review of the identifications made pursuant to CIP-002-5.1a R1; 2) had its CIP Senior Manager approve those identifications; and 3) implemented biweekly compliance staff meetings with the CIP Senior Manager to review and prioritize compliance-related activities and tasks. <p>WECC 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
WECC2018019748	CIP-002-5.1a	R2; P2.2	[REDACTED]	[REDACTED]	8/17/2017	10/5/2018	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 violation.)			<p>On May 23, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in potential noncompliance with CIP-002-5.1a R2. Specifically, in February of 2018, the entity hired contractors to complete a gap analysis of its NERC CIP Program. The gap analysis concluded that the initial Bulk Electric System (BES) Cyber System identifications were appropriately reviewed and approved by the CIP Senior Manager on May 17, 2016. However, the entity did not have sufficient evidence of the 15-calendar month CIP Senior Manager approval of the BES Cyber System identifications that should have occurred in 2017.</p> <p>Further analysis determined the entity had an existing employee oversee its NERC compliance when the CIP version 5 Standards were approved, but that person did not have a compliance background. As a result, the entity's compliance program was immature and had gaps. At the time of these issues, the CIP Senior Manager was not aware of the ongoing compliance obligations of CIP-002-5.1a R2. After reviewing all relevant information, WECC determined the entity failed to appropriately perform CIP-002-5.1a R2 Part 2.2.</p> <p>The root cause of this issue was attributed to the individuals responsible for the NERC compliance program not having the necessary skills and background to ensure all compliance obligations were met.</p> <p>This noncompliance started on August 17, 2017, 15 calendar months after the initial identifications had been previously approved, and ended on October 5, 2018, when the identifications were approved, for a total of 415 days.</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. In this instance, the entity failed to have its CIP Senior Manager approve the identifications required by R1, at least once every 15 calendar months, as required by CIP-002-5.1a R2 Part 2.2.</p> <p>Failure to approve the impact evaluations of BES Cyber Systems from R1 could potentially result in mis-categorizing BES Cyber Systems which could lead to inadequate or non-existent cyber security controls. However, as compensation, the entity had implemented all monitoring systems, and physical and electronic access controls required for Low Impact BES Cyber Systems (LIBCS) to the affected Facilities. In addition, considering the entity operates [REDACTED], as such the inherent potential harm has been assessed as minor. No harm is known to have occurred.</p> <p>WECC determined the entity did not have any relevant compliance history for this Standard and Requirement.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) obtained CIP Senior Manager approval of the identifications from by R1; 2) replaced the NERC Compliance Manager with an individual with the appropriate background and knowledge. This individual created a SharePoint site to include tracking of all CIP program documentation, workflows, and important links to prevent gaps in compliance from occurring in the future; and 3) created calendar reminders for the CIP Senior Manager to review and approve identifications made in R1 within the required 15 calendar month timeframe. <p>WECC 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
WECC2018019749	CIP-003-6	R3	[REDACTED]	[REDACTED]	4/14/2017	9/7/2018	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 violation.)			<p>On May 23, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in potential noncompliance with CIP-003-6 R3. Specifically, in February of 2018, the entity hired contractors to complete a gap analysis of its NERC CIP Program. The gap analysis concluded that the entity did not document a change to its CIP Senior Manager within 30 calendar days of the change which occurred in early 2017, as required by CIP-003-6 R3.</p> <p>Further analysis determined the entity had an existing employee oversee its NERC compliance when the CIP version 5 Standards were approved, but that person did not have a compliance background. As a result, the entity's compliance program was immature and had gaps. At the time of these issues, the CIP Senior Manager was not aware of the ongoing compliance obligations of CIP-003-6 R3. After reviewing all relevant information, WECC determined the entity failed to appropriately perform CIP-003-6 R3.</p> <p>The root cause of this issue was attributed to the individuals responsible for the NERC compliance program not having the necessary skills and background to ensure all compliance obligations were met.</p> <p>This noncompliance started on April 14, 2017, 31 days after a change to the CIP Senior Manager that was not documented, and ended on September 7, 2018, when the new CIP Senior Manager was documented, for a total of 512 days.</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. In this instance, the entity failed to document a change to the CIP Senior Manager within 30 calendar days of the change, as required by CIP-003-6 R3.</p> <p>Failure to identify and document a CIP Senior Manager could provide no clear authority and ownership for the entity's CIP program and could result in inadequate strategic planning, lack of executive or board-level awareness, and ineffective overall program governance. However, as compensation, the entity had implemented all monitoring systems, and physical and electronic access controls required for Low Impact BES Cyber Systems (LIBCS) to the affected Facilities. In addition, considering the entity operates [REDACTED], as such the inherent potential harm has been assessed as minor. No harm is known to have occurred.</p> <p>WECC determined the entity did not have any relevant compliance history for this Standard and Requirement.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) documented the change to the CIP Senior Manager; 2) replaced the NERC Compliance Manager with an individual with the appropriate background and knowledge. This individual created a SharePoint site to include tracking of all CIP program documentation, workflows, and important links to prevent gaps in compliance from occurring in the future; and 3) created calendar reminders for the CIP Senior Manager to review and approve identifications made in R1 within the required 15 calendar month timeframe. <p>WECC 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
WECC2018020363	CIP-003-6	R1: P1.2	[REDACTED]	[REDACTED]	07/01/2018	09/07/2018	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 violation.)			<p>On September 7, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in potential noncompliance with CIP-003-6 R1. Specifically, the entity did not review and obtain CIP Senior Manager approval of its cyber security policies for its assets identified in CIP-002 containing Low Impact BES Cyber Systems (LIBCS) within 15 calendar months of conducting the prior review as required by Part 1.2. The entity contracted with a third-party vendor for completion of compliance related activities which included documentation reviews and approvals. At the time, the vendor tracked status of documentation reviews and approvals through SharePoint tasks. In this instance, when the vendor transitioned responsibility for the entity’s compliance related activities internally, neither the entity nor the vendor confirmed all tasks had been completed as indicated by the prior contractor. This issue began on July 1, 2018, when the entity should have completed the review and approval process related to its LIBCS cyber security policies and ended on September 17, 2018, when the entity reviewed and obtained CIP Senior Manager approval of said policies, for a total of 79 days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to adequately perform CIP-003-6 R1 Part 1.2. The root cause of the issue was attributed to a less than adequate process design and oversight. Specifically, the entity managed completion of documentation review and approvals as a SharePoint task without sufficient controls to ensure those tasks were included in SharePoint, and no oversight of completion.</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. In this instance, the entity failed to review and obtain CIP Senior Manager approval at least once every 15 calendar months for its five documented cyber security policies associated with its assets identified as containing LIBCS.</p> <p>Failure to review and obtain approval of cyber security policies could have resulted in distribution of inaccurate guidance or outdated policy. However, this issue was associated with LIBCS and a total of two Bulk Electric System (BES) Cyber Assets (BCA). Additionally, no inaccurate or outdated information was identified that required updating when the review was conducted. No harm is known to have occurred.</p> <p>WECC 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 obtained CIP Senior Manager approval for its cyber security policies associated with its LIBCS; 2) automated tracking of compliance related tasks by expanding the functionality of their compliance software to track document review and approval processes; and 3) established an escalation process to provide additional oversight of completion of documentation reviews. <p>WECC 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
WECC2018020445	CIP-004-6	R4: P4.1, P4.1.1.	[REDACTED]	[REDACTED]	05/04/2018	08/14/2018	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 violation.)			<p>On September 26, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R4. Specifically, the entity commissioned [REDACTED] workstations classified as Physical Access Control System (PACS) without disabling the device’s default access configuration which allowed unauthorized access to the PACS workstations, not the security software, to all employees in the remote users Active Directory group. During the commissioning process for the new workstations, the default access configuration allowing the access should have been disabled. As a result, an individual remotely accessed one of the PACS; however, the individual was not able to access the security software which was protected by two-factor authentication. This issue began on May 4, 2018, when the PACS were commissioned and ended on August 14, 2018, when unauthorized access for the individual in scope was revoked, for a duration of 103 days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to adequately perform CIP-004-6 R4 Part 4.1 subpart 4.1.1. The root cause of the issue was attributed to less than adequate process documentation. Specifically, the entity’s documented process did not include steps to remove the default configuration that granted unauthorized access to members of the remote users Active Directory group.</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. In this instance, the entity failed to adequately implement its documented process to authorize electronic access based on need as required by CIP-004-6 R4 Part 4.1 subpart 4.1.1 when members of the remote users Active Directory group, [REDACTED] employees, were allowed remote access to [REDACTED] new PACS workstations.</p> <p>Failure to properly manage electronic access could have resulted in a malicious actor granting unauthorized physical access to a Physical Security Perimeter protecting access to the Medium Impact Bulk Electric System (BES) Cyber Systems located in both its primary and backup Control Centers. However, the entity had implemented two-factor authentication on the security software installed on the [REDACTED] PACS; although an individual could have gained unauthorized access to the workstation itself, the security software required separate BES Cyber System authorization. No harm is known to have occurred.</p> <p>WECC considered the Entity’s compliance history and determined that there are no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) revoked the default unauthorized electronic access by reconfiguring the [REDACTED] PACS; and 2) changed its desktop imaging procedure for PACS to require removal of default access permissions to prevent a reoccurrence. <p>WECC 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
WECC2018018941	CIP-010-2	R1: P1.1, P1.1.1.	[REDACTED]	[REDACTED]	07/01/2016	11/10/2017	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 January 8, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in potential noncompliance with CIP-010-2 R1. The entity submitted the Self-Report to WECC under an existing multi-region registered entity agreement. Specifically, the entity incorrectly documented the baseline configuration of three Bulk Electric System (BES) Cyber Assets (BCA) associated with its Medium Impact BES Cyber Systems (MIBCS) without External Routable Connectivity located at [REDACTED] different substations. The operating system version and firmware documented by the entity was different than the baseline configurations on the BCAs. The entity identified the issue during an internal training session on how to properly document a baseline configuration. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity and ended on November 10, 2017, when the entity correctly documented the baseline configurations of the three BCAs, for a total of 498 days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to adequately implement CIP-010-2 R1 Part 1.1.1. The root cause of this issue was attributed to less than adequate training for personnel responsible for documenting 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. In this instance, the entity failed to adequately implement its documented process to develop a baseline configuration which included the operating system or firmware as required by CIP-010-2 R1 Part 1.1.1 for three BCAs.</p> <p>Failure to properly document a baseline configuration could have resulted in a failure to identify security patches that required evaluation for applicability. Additionally, failure to have the baseline properly documented could have hindered system restoration. However, the BCAs used custom firmware and the entity would have been contacted directly by the vendor if an update was necessary and the entity confirmed that no updates were released by the vendor for the operating system or firmware during the period at issue. Additionally, this issue was discovered because of training the entity implemented for employees as to how to properly document a baseline configuration. No harm is known to have occurred.</p> <p>WECC 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) updated the baseline configuration documentation for the three BCAs; and 2) conducted training on proper documentation of a baseline configuration. <p>WECC 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
WECC2018019685	CIP-010-2	R1: P1.2	[REDACTED]	[REDACTED]	08/31/2017	05/01/2018	Compliance 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 violation.)			<p>During a Compliance Audit conducted [REDACTED], WECC determined the entity, as a [REDACTED], had a potential noncompliance with CIP-010-2 R1 Part 1.2. The entity submitted the Self-Report to WECC under an existing multi-region registered entity agreement. Specifically, in two instances, the entity failed to authorize changes that deviated from the existing baseline configuration of a single BCA associated with its MIBCS. This issue began on August 31, 2017, when the entity made the first unauthorized change to the BCA and ended on May 1, 2018, when the entity's change management procedure and process documentation were updated, for a duration of 244 days.</p> <p>After reviewing all relevant information, WECC Enforcement concurred with the audit finding as stated above. The root cause of the issue was attributed to a less than adequate process design and documentation. Specifically, the entity had documented a change management process; the entity's process utilized a task checklist for employees to reference as work-level instructions and to document completion of activities while completing a change. However, the entity's process did not account for unplanned changes, and as such, the entity had not identified or documented how unplanned changes could be authorized.</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. In two instances, the entity failed to implement a documented process to authorize and document changes that deviated from the baseline configuration as required by CIP-010-2 R1 P1.2 for a single BCA.</p> <p>Failure to implement a change management process that details how to obtain authorization of unplanned changes could have resulted in delay of necessary changes to Cyber Assets; individuals may have hesitated to implement a change without prior approval. Additionally, a lack of oversight in the process could result in unforeseen adverse consequences to the BES if the appropriate individuals were not evaluating the impact of the change to the system. However, in each instance, entity personnel utilized the task checklist while completing the change. Therefore, for each change, personnel documented the following actions: an emergency change was determined necessary; confirmed that the prior version was available to revert to; verified that the change had not impacted security controls; notified management of the change; and documented changes to the baseline. No harm is known to have occurred.</p> <p>WECC 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) updated the configuration change management procedure to address authorization of unplanned changes; 2) created a task checklist for unplanned changes that includes a step for authorization of the change; and 3) notified responsible personnel of the updated procedure documentation. <p>WECC 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
WECC2018020041	CIP-004-6	R3: P3.5	[REDACTED]	[REDACTED]	02/13/2017	08/31/2018	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 violation.)			<p>On July 18, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in potential noncompliance with CIP-004-6 R3. Specifically, in two instances, the entity did not ensure that personnel with authorized unescorted physical access had a personnel risk assessment (PRA) completed within the last 7 years prior to expiration of their existing PRA. In the first instance, on February 13, 2017, an employee with authorized unescorted physical access to a Medium Impact Bulk Electric System (BES) Cyber System (MIBCS) with External Routable Connectivity (ERC) did not have a PRA completed within the last 7 years prior to expiration of their existing PRA. This instance ended on September 29, 2017 when the entity completed the individual’s PRA for a total of 299 days. The second instance began on February 10, 2018 and involved three personnel with authorized unescorted physical access to a MIBCS with ERC that did not have a PRA completed within the last 7 years prior to expiration of their existing PRA. This instance ended on August 31, 2018 when all three personnel had a PRA completed or their authorization for unescorted physical access removed for a total of 203 days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to adequately perform CIP-004-6 R3 Part 3.5. The root cause of these instances was attributed to a less than adequate process and lack of management oversight. Specifically, the entity’s PRA review process was not well-documented and did not incorporate management oversight of the process or work product.</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. In these instances, the entity failed to adequately implement its process to ensure that four individuals with authorized electronic or authorized unescorted physical access had a PRA completed within the last seven years, prior to expiration of their existing PRA, as required by CIP-004-6 R3 Part 3.5.</p> <p>Failure to periodically conduct a PRA could result in the entity failing to identify personnel whose risk profile has changed over time and who may have developed the motivation to cause harm to the BES. With unescorted physical access to a MIBCS and its associated BCAs, PACS, and EACMS, a malicious actor could cause physical damage to the assets making them inoperable, resulting in disruptions to security at the facility. However, as compensation, the personnel in scope for this issue had an initial PRA performed and had been provisioned authorized access based on requirements of their role. As current personnel, the individuals were less likely to have malicious intent to cause harm to or disrupt the BES resulting from access to one generating facility. Additionally, the individuals did not have electronic access to the MIBCS or its associated BCAs, PACS, or EACMS. No harm is known to have occurred.</p> <p>WECC considered the Entity’s compliance history and determined that there are no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed a PRA for three of the personnel and removed access for one personnel who no longer required the access; 2) reviewed personnel access lists to verify personnel with authorized unescorted physical access have an active PRA; 3) updated and documented the access verification process to include a monthly review of PRA expiration dates and to alert of PRAs that expire within 180 days and those that have already expired; 					

<p>4) provided training to personnel on the monthly PRA review; and 5) implemented management oversight of the process by requiring manager approval of the monthly review. WECC has verified the completion of all mitigation activity.</p>

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 Exception 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	MRO2018020157			Yes	Yes					Yes				Category 2 – 12: 2 years
2	MRO2019021425			Yes	Yes					Yes				Category 2 – 12: 2 years
3	MRO2019021530			Yes	Yes					Yes				Category 2 – 12: 2 years
4	MRO2019021499			Yes	Yes									Category 2 – 12: 2 years
5	MRO2018020844			Yes	Yes									Category 2 – 12: 2 years
6	MRO2018020837			Yes	Yes					Yes				Category 2 – 12: 2 years
7	MRO2019021365	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
8	MRO2018019555			Yes	Yes									Category 2 – 12: 2 years
9	MRO2018020831			Yes	Yes									Category 2 – 12: 2 years
10	MRO2018020838			Yes	Yes									Category 2 – 12: 2 years
11	MRO2017017815			Yes	Yes						Yes			Category 2 – 12: 2 years
12	MRO2019021191			Yes	Yes					Yes				Category 2 – 12: 2 years
13	MRO2017018866	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
14	MRO2018018954			Yes	Yes					Yes				Category 2 – 12: 2 years
15	MRO2018019231	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
16	MRO2018019584			Yes	Yes					Yes				Category 2 – 12: 2 years
17	MRO2019020945			Yes	Yes					Yes				Category 2 – 12: 2 years
18	MRO2019021359			Yes	Yes					Yes				Category 2 – 12: 2 years
19	MRO2019021391			Yes	Yes					Yes				Category 2 – 12: 2 years
20	MRO2019021448	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
21	MRO2019021450		Yes	Yes	Yes					Yes				Category 2 – 12: 2 years
22	MRO2019021451			Yes	Yes					Yes				Category 2 – 12: 2 years
23	MRO2019021267			Yes	Yes					Yes				Category 2 – 12: 2 years
24	MRO2018020161	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
25	NPCC2019021754			Yes	Yes		Yes		Yes					Categories 3 – 4: 2 years Category 6: 3 years
26	NPCC2019021756			Yes	Yes		Yes		Yes					Categories 3 – 4: 2 years Category 6: 3 years
27	RFC2018019969	Yes		Yes	Yes	Yes	Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 years
28	RFC2018020579	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 years
29	RFC2017018304	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 years
30	RFC2017017652	Yes		Yes	Yes					Yes				Category 1: 3 years; 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)
31	RFC2017018562	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
32	RFC2018018986	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
33	RFC2017017843	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
34	RFC2018019771	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 years
35	RFC2018019383	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
36	RFC2017018257	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
37	RFC2017017412	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
38	RFC2017018256	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
39	RFC2019021106	Yes					Category 1: 3 years; Category 2 – 12: 2 years							
40	RFC2019021107	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
41	RFC2018019401	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
42	RFC2017018258	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
43	RFC2017017414	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
44	RFC2017018259	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
45	RFC2017018254	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
46	RFC2017017417	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
47	RFC2017018255	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
48	RFC2019021893	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 years
49	RFC2019021894	Yes	Yes	Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
50	RFC2019021895	Yes	Yes	Yes	Yes	Yes	Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 years
51	RFC2019021904	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 years
52	RFC2019021905	Yes	Yes	Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
53	SERC2017017763			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
54	SERC2017017762			Yes	Yes				Yes					Category 2 – 12: 2 year
55	SERC2017017761	Yes		Yes	Yes					Yes				Category 2 – 12: 2 year
56	SERC2016016719			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
57	SERC2017017663			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
58	SERC2017018496			Yes	Yes				Yes	Yes	Yes		Yes	Category 2 – 12: 2 year

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)
59	TRE2019021507			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
60	TRE2019021295	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
61	TRE2019021333	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
62	TRE2019021578	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
63	TRE2018019729	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
64	WECC2018020117			Yes	Yes									Category 2 – 12: 2 year
65	WECC2018020415			Yes	Yes									Category 2 – 12: 2 year
66	WECC2017018399			Yes	Yes									Category 2 – 12: 2 year
67	WECC2017018400			Yes	Yes									Category 2 – 12: 2 year
68	WECC2018019195			Yes	Yes									Category 2 – 12: 2 year
69	WECC2018020113			Yes	Yes					Yes				Category 2 – 12: 2 year
70	WECC2018019482			Yes	Yes					Yes				Category 2 – 12: 2 year
71	WECC2018019548			Yes	Yes						Yes			Category 2 – 12: 2 year
72	WECC2018019552			Yes	Yes						Yes			Category 2 – 12: 2 year
73	WECC2017018614	Yes		Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 year
74	WECC2018019294			Yes	Yes				Yes					Category 2 – 12: 2 year

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
MRO2018020157	CIP-006-6	R2	[REDACTED] (the Entity)	[REDACTED]	04/11/2018	04/11/2018	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 violation.)			<p>On July 10, 2018, the Entity submitted a Self-Log stating that as a [REDACTED], it was in noncompliance with CIP-006-6 P2.1. [REDACTED]</p> <p>[REDACTED] The noncompliance [REDACTED] An employee with authorized access to a Physical Security Perimeter (PSP) failed to continuously escort three visitors (contractors) who were doing work within the PSP. Per the Entity, the escort was distracted from escort duties while reviewing results of work that had been performed in the PSP.</p> <p>The cause of the noncompliance is that the Entity failed to follow its documented processes related to performing an escort.</p> <p>The issue began on April 11, 2018, when the employee stopped continuously escorting the contractors, and ended thirteen minutes later when the employee resumed the escort.</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 the Entity, the duration of the noncompliance was limited to 13 minutes. Also, the Entity reports that BES Cyber Assets within the PSP are housed in card access controlled cabinets and none of the visitors had a badge for these cabinets. Lastly, the Entity states that security cameras monitored the visitors while they were within the PSP and security personnel confirmed that no attempts were made to access BES Cyber Assets. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) had its employee resume the continuous escort; 2) directed the employee escort to notify the appropriate manager and Compliance staff; 3) revised annual SME training to add emphasis to the visitor control program; 4) required the employee escort to review Visitor Control Program policies; 5) posted an entry to its intranet security weblog outlining key responsibility for escorting visitors; 6) distributed an urgent email to employees with PSP access describing the incident and reinforcing key responsibilities for escorting visitors in restricted areas; and 7) modified their policy regarding Restricted Area Visitor Escorting and Access which included providing specific responsibilities for escort personnel and to require an escort signature in the visitor log. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021425	CIP-004-6	R5	[REDACTED] (the Entity)	[REDACTED]	12/27/2018	02/12/2019	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 10, 2019, the Entity, submitted a Self-Log stating that as a [REDACTED], it was in noncompliance with CIP-004-6 R5. [REDACTED]</p> <p>[REDACTED] The noncompliance [REDACTED] The Entity stated that on February 12, 2019, it conducted a quarterly access review follow-up investigation, and the assessment identified account passwords on shared accounts that were not changed within 30 days of one individual no longer needing access, as required by CIP-004-6 P5.5. The noncompliance occurred when the Entity was implementing a new access management tool and the normal workflow to remove access during the new access management tool implementation process was not used. The user transitioned to a new role within the Entity.</p> <p>The cause of the noncompliance was the entity did not follow its access management process for access removal.</p> <p>The issue began on December 27, 2018, 31 days after the individual no longer needed access, and ended on February 12, 2019 when the account password was 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 the Entity, the user was a trusted employee whose transfer was voluntary and not for cause. The Entity also stated that during the noncompliance, the user did not utilize the shared account to access any BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems (EACMS). No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) changed passwords for 158 shared accounts; 2) conducted an extent of condition analysis to review all users moved to the new access management tool and verified that no other new access requests were rejected during the cutover to the new tool; 3) conducted a lessons learned meeting regarding the new access management tool, reinforcing the need to use the new access management tool for access removals; and 4) sent communications to supervisors of personnel with NERC CIP access to reinforce that all NERC CIP access removals must go through the formal access removal 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
MRO2019021530	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	01/04/2019	01/07/2019	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 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-010-2 R1. [REDACTED]</p> <p>The Entity reported that it made a baseline configuration change on one virtual server before having assessed the configuration change for possible security impact as required by CIP-010-2 R1. The nature of the change was installation of a (commercially available) backup software agent for SQL databases with the intent of facilitating backups. The noncompliance was discovered when an administrator, who had made the baseline configuration change on the virtual server, recognized the issue and took corrective action.</p> <p>The cause of the noncompliance was that the Entity failed to follow its documented processes regarding making baseline changes without prior assessment of the possible impact of those changes as detailed in CIP-010-2 R1.</p> <p>This noncompliance started on January 4, 2019, when the Entity made a change to the baseline configuration without performing the impact assessment required by P1.4, and ended on January 7, 2019, when it performed the required impact 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 (BPS). The issue resulted from installation of a commercially available backup software agent for SQL databases on a virtual device. The agent had previously been installed on 69 other hosts without incident. Had the issue not been discovered and corrected by the administrator, it would have been discovered by an internal control that employs an automated baseline monitoring system to detect and log baseline changes. These log events are reviewed manually as part of a scheduled review process and cause a ticket to be automatically generated, which instructs a review of baseline changes to be performed on the first calendar day of the following month. The Entity conducted a "post implementation risk assessment" of potential CIP-005 and CIP-007 effects of the baseline change was conducted and the results of the assessment was that no CIP-005 or CIP-007 controls were affected. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) created a change control ticket to document configuration change activities, track authorization, and perform an impact assessment of CIP-005 and CIP-007 controls which were potentially impacted; and 2) sent a message to personnel responsible for change control to emphasize and set expectations for managing change control as directed by training and 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
MRO2019021499	CIP-006-6	R1	[REDACTED] (the Entity)	[REDACTED]	02/13/2019	02/13/2019	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 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-006-6 R1. The Entity reported that on February 13, 2019, a person with authorized unescorted physical access to the Entity's Primary Control Center (PCC) entered the PCC's Physical Security Perimeter (PSP) without utilizing two-factor authentication as required by P1.3. The Entity's Physical Access Control System (PACS) requires a person to scan a badge and enter a pin to enter the PCC's PSP. The individual followed another authorized person that properly authenticated and entered the PSP without allowing the door to close (tailgating). The Entity states that the individual scanned their badge but did not and was not required to enter the PIN due to the tailgating. The Entity reports that a third party observed this and immediately reported the matter to security staff; security staff responded and intervened appropriately.</p> <p>The cause of the noncompliance was that the Entity's employee failed to follow the Entity's access control program, which requires use of two-factor authentication when entering the PCC PSP.</p> <p>The issue began on February 13, 2019, when the individual entered the PSP without being granted access by the PACS, and ended later when persons involved left and re-entered the PSP following correct procedures.</p>					
Risk Assessment			The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The individual had authorized access; further, the noncompliance was detected and reported by a peer, which demonstrates a strong culture of compliance. No harm is known to have occurred.					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) required the individual involved to leave and re-enter the PSP following the correct procedure; and 2) sent a memo to all persons with authorized unescorted physical access to PSPs to reinforce access management procedures, including ensuring that doors are closed prior to attempting to gain 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
MRO2018020844	CIP-004-6	R5	[REDACTED] (the Entity)	[REDACTED]	08/05/2018	08/07/2018	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 October 3, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. The Entity reported that an individual's job duties changed and it was determined that the individual no longer required electronic access to an individual account. The effective date of the employee's transfer was August 3, 2018, such that his access was to be removed by the end of the following calendar day as required by P5.2. During a review of changes to the individual's accounts on August 6, 2018, it was discovered that the SME responsible for revoking access had failed to revoke access for one individual account on four medium impact CAs.</p> <p>The cause of the noncompliance was the Entity failed to follow its process for access revocation upon reassignment or transfer.</p> <p>This noncompliance began on August 5, 2018, which was the day after the access was to be revoked, and ended on August 7, 2018, when the final 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 (BPS). The issue was limited to one user account on four Cyber Assets. The employee, who was being transitioned to a new role, retained the 'acting' title of his old role, and it would have been reasonable for the Entity to determine that the employee should have still retained the access. Further, the date of the change in access was determined to coincide with the termination of another employee with similar access to gain efficiencies in doing both at the same time, rather than revoking the employee's access after his 'acting' role concluded. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked the remaining access; and 2) performed training for its SMEs on CIP-004-5 R5.2. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020837	CIP-011-2	R1	[REDACTED] (the Entity)	[REDACTED]	10/30/2018	10/30/2018	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 violation.)			<p>On November 20, 2018, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-011-2 R1. Per the Entity, it failed to follow its procedures for protecting the transmission of BES Cyber System Information (BES CSI). This occurred when an individual emailed an attachment with BES CSI to an authorized recipient, but failed to follow the Entity's procedures for protecting BES CSI in transit. Specifically, this individual failed to encrypt the email along with password protecting it per the Entity's procedure. The issue was immediately identified by the individual who sent the email and reported it to the Entity's Compliance office.</p> <p>The cause of the noncompliance was the Entity failed to follow its process for protecting the transit and use of BES CSI, resulting in BES CSI not being protected in transit.</p> <p>The issue started October 30, 2018 when BES CSI was not protected in transit and ended later that day when the BES CSI was no longer being transmitted.</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 the Entity, the email attachment with BES CSI did not include Cyber Asset IP addresses, hostnames, or locations, limiting the misuse to non-access oriented BES CSI. [REDACTED] Finally, the Entity states that the recipient of the email was intended and authorized to use the BES CSI. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) stopped transmitting the BES CSI; 2) retrained the individual who emailed the BES CSI on the protection procedures for BES CSI; 3) distributed a security awareness bulletin to all staff that focused on protections for BES CSI; and 4) created and distributed a BES CSI desktop reference card to staff that details the process for determining and handling BES CSI. 					

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
MRO2019021365	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	09/26/2018	12/20/2018	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 9, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-007-6 R2. The Entity failed to identify a source to track for the release of cyber security patches for new software installed on one BES Cyber Asset as required by P2.1</p> <p>The cause of the noncompliance was that the Entity failed to follow its CIP-007-6 process to identify and track cyber security patch sources at time of installation, and not at the time of first use.</p> <p>This issue began on September 26, 2018, when the Entity failed to identify a source to track for new software installed on one BES Cyber Asset, and ended on December 20, 2018, when the source was identified and evaluated for cyber security patches.</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 Entity reported that this issue only impacted a single patch source on a single medium impact BES Cyber Asset. Further, physical access to the device is protected [REDACTED] which is above that which is required for a medium impact BES Cyber System. Additionally, there is no Internet access to this device, which further limits the attack vectors available to this device. The Entity reports that the patch source only released a single patch during the noncompliance and that patch was evaluated within 36 days of its release. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) identified the patch source and evaluated the cyber security patches released by the source (one patch); 2) trained the impacted staff member on identifying the source at the time of software installation and not at the time of first use; and 3) updated its CIP change management training to explicitly require the identification of patch sources at time of software installation. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019555	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	01/04/2018	01/08/2018	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 4, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>The Entity determined that new biometric software was installed on a PACS server without authorization. The unauthorized software installation was a deviation from baseline, and the baseline scanning software (which runs nightly) detected the issue.</p> <p>The cause of the noncompliance was that the importance of authorization prior to a baseline change was insufficiently reinforced.</p> <p>The noncompliance started January 4, 2018, when biometric software was installed on the PACS server without authorization, and ended on January 8, 2018, when the software installation was authorized.</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 biometric software was needed and ultimately authorized. Further, the individual who installed the software without authorization had electronic access permissions, and was current on CIP training. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) authorized the software installation; 2) created a new user profile for PACS users that utilized greater access restrictions to the PACS server. The increased access restrictions are intended to prevent non-administrative users from performing administrative functions (such as installing software) going forward; and 3) revised and reinforced CIP Electronic Access Training course across the organization. The training was specifically reinforced with the employee responsible for the software installation to emphasize the importance of authorization prior to baseline changes. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020831	CIP-004-6	R4	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	04/27/2018	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 violation.)			<p>On October 10, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R4. On April 26, 2018, the Entity discovered that there were four Security Administrators who held an electronic access privilege, which permitted them to update the firmware on Physical Security Perimeter (PSP) terminal controllers (Physical Access Control Systems (PACS)), but were not authorized to perform that activity on those Cyber Assets. The issue involved two PSP terminal controllers at the Entity's primary Control Center and one at the Entity's backup Control Center. In addition, the issue involved one PSP terminal controller at each of the Entity's substations that contain medium impact BES Cyber Systems.</p> <p>The cause of the noncompliance was that the Entity was unaware of an electronic access privilege built into the Security Administrator user type, its process failed to account for those types of users, resulting in those users being given the ability to update firmware without authorization.</p> <p>The noncompliance began on July 1, 2016 when the requirement went into effect and ended on April 27, 2018, when the four administrators were authorized for electronic access to the terminal controllers.</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 scope of the issue was limited to four users and the noncompliance was resolved by authorizing access to the users. The Entity stated that these users could not perform other common system administrator functions, such as managing ports and services. Lastly, the Entity reported no instances of PACS firmware updates being performed without proper authorization. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) authorized electronic access to the terminal controllers for the four Security Administrators; and 2) revised its process for onboarding Security Administrators to include authorizing electronic access to terminal controllers for such personnel. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020838	CIP-004-6	R5	[REDACTED] (the Entity)	[REDACTED]	12/10/2017	12/20/2017	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 October 10, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R5. On December 20, 2017, the Entity discovered that an individual with authorized electronic access had been transferred elsewhere in the company and no longer needed that authorized electronic access, but that electronic access had not been revoked within one calendar day. The electronic access was to one medium impact BES Cyber System (BCS) located at three substations.</p> <p>The cause of the noncompliance was the Entity's process for notifying internal transfers was designed to occur at varying number of days after the transfer was completed, putting it in conflict with the timing element of the requirement.</p> <p>The noncompliance began on December 10, 2017, one working day following the transfer, and ended on December 20, 2017, 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. The transferred individual had an active Personal Risk Assessment and current CIP training. The issue was Self-Reported and was limited in duration to 11 days. Additionally, the transferred individual did not access the system after the date of the transfer. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked the access in question; and 2) added a new email notification, timed to occur at the start of the HR transfer process, notifying the affected supervisors and the Entity's Security Administration group about the upcoming transfer, these new notifications serve to trigger the individuals responsible for initiating access revocation requests. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2017017815	CIP-007-6	R4	[REDACTED] (the Entity)	[REDACTED]	07/1/2016	[REDACTED]	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 June 23, 2017, the Entity submitted a Self-Report stating that as a [REDACTED], it had an issue of noncompliance with CIP-007-6, R4. A second instance of noncompliance was detected during a Compliance Audit conducted from [REDACTED].</p> <p>The first instance of noncompliance was discovered during an internal review which discovered gaps in evidence supporting the reviews required by CIP-007-6 P4.4. Investigation showed that one gap occurred from July 16, 2016 (the day after the first review was required to have been performed) to August 16, 2016. The Entity states that it identified a second gap that occurred from October 14, 2016 to March 27, 2017. The cause of the noncompliance is that the Entity failed to follow its documented process to review a summarization or sampling of recorded logged events. The cause of the noncompliance was that the Entity failed to follow its documented process to review a summarization or sampling of recorded logged events at intervals no greater than 15 calendar days as required by CIP-007-6 R4. The noncompliance was noncontiguous; the noncompliance began on July 1, 2016, when the obligation under P4.4 in the Standard and Requirement became enforceable, and ended on March 27, 2017 when the Entity conducted a review of logs.</p> <p>The second instance of noncompliance was discovered in preparation for a Compliance Audit conducted from [REDACTED] of [REDACTED] sampled Cyber Assets was not configured to issue an alert upon detection of malicious code as required by P4.2.1. Per the Entity, the Electronic Access Control or Monitoring System (EACMS) device is not capable of directly issuing such an alert but is able to generate (syslog) messages to a Security Information and Event Management System (SIEM) which can be configured to act as a proxy to generate the alert. The cause of the noncompliance was that the entity failed to follow its documented process regarding alerts to be generated upon detection of malicious code. The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on [REDACTED] when the Entity configured the device.</p> <p>The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on [REDACTED] when the Entity re-configured the device in the second instance.</p> <p>The Entity does not have any relevant history of 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 (BPS). For instance one, per the Entity, an additional control which generates alerts that are monitored by a third party was in place during the noncompliance. Additionally, no information was lost. For the second instance, the evidence indicates that log reviews for the impacted device were being appropriately conducted. Additionally, the device was an EACMS and not a BES Cyber Asset. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) conducted and completed a retroactive review of logged events; 2) updated relevant EMS Procedures Document and SCADA System Support documentation; and 3) conducted training on 15 and 35-day review processes for relevant personnel. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) configured a SIEM to issue an alert if the device’s logs indicate the detection of malicious code; and 2) updated the onboarding section of the applicable Device Management policy to include steps to configure the SIEM to alert for malicious code in similar situations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021191	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	11/30/2018	02/07/2019	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 February 27, 2019, the Entity submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-007-6 R2. [REDACTED] The Entity states that it discovered that it had not included its "manual" patch sources in its patch evaluations in P2.2 that occurred in November, December, and January.</p> <p>The cause of the noncompliance was that the Entity's implementation of its process was insufficient in ensuring that manual patch sources were assessed.</p> <p>The noncompliance started on November 30, 2018, 36 days after its last complete P2.2 evaluation, and ended on February 7, 2019, when patches released by its "manual" sources were evaluated.</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 Entity reports that the noncompliance was limited to the manual patch sources consisting of five applications from two vendors (applications were for security monitoring). The Entity also states that only one applicable patch was released from a manual source during the period of noncompliance and that patch had a low impact and exploitability score; the patch was for a vulnerability in an embedded library that does not actually affect the product. Upon discovery of the issue, the patch was evaluated and applied on the same day, limiting the duration. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) evaluated and applied the patch; and 2) updated the monthly ticket to specifically call out manually reviewed sources and enhanced its security patch management document to more clearly identify manual sources. <p>MRO 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
MRO2017018866	CIP-007-6	R5	[REDACTED] (the Entity)	[REDACTED]	7/1/2016	3/29/2018	Compliance 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 violation.)			<p>During a Compliance Audit conducted from [REDACTED] MRO determined that the Entity, [REDACTED] was in noncompliance with CIP-007-6 R5. NSP, [REDACTED]. The Compliance Audit discovered three instances of noncompliance.</p> <p>The first instance of noncompliance involved an enabled default/generic account on a single BES Cyber Asset that was not documented as required by P5.2. The BES Cyber Asset was located at an [REDACTED] substation. The Entity states that the account was created when new software was installed on the device. The Entity reports that it documented the accounts that the vendor identified in its documentation, but did not verify what accounts were enabled on the device; the account was not included in the documentation. The cause of the noncompliance was that the Entity failed to follow its documented process to identify and inventory all enabled default or other generic accounts. The noncompliance began on July 1, 2016 when the Standard and requirement became enforceable, and ended on November 9, 2017, when the account was inventoried and identified.</p> <p>The second instance of noncompliance involved a Protected Cyber Asset (PCA) in the [REDACTED] Control Center. The PCA did not enable controls to technically enforce password complexity, and the Entity had failed to produce evidence of how the complexity was procedurally enforced. The cause of the noncompliance was that the Entity failed to follow its processes for enforcing password complexity. The noncompliance began on July 1, 2016 when the Standard and requirement became enforceable, and ended on November 9, 2017, when password complexity controls were enabled.</p> <p>The third instance of noncompliance involved [REDACTED] Physical Access and Control System (PACS) (PACS panels) devices for which the Entity could not demonstrate a method for either limiting unsuccessful authentication attempts, or issuing an alert on exceeding a threshold as required by P5.7. The cause of the noncompliance was that the Entity failed to follow its process to file a Technical Feasibility Exception (TFE) when a device cannot either limit or alert regarding unsuccessful authentication attempts. The final PACS device was removed from service and replaced with another PACS device that was added to an existing TFE. The noncompliance began on July 1, 2016 when the Standard and requirement became enforceable, and ended on March 29, 2018, when the last device was added to an existing TFE.</p> <p>The noncompliance began on July 1, 2016 when the Standard and Requirement became enforceable and ended on March 29, 2018, when the final device was added to an existing TFE.</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 Entity states that the device in the first instance was located in functioning Physical Security Perimeters (PSPs) during the noncompliance. The Entity reports that the second instance involved some password complexity controls not being implemented, but the password was being changed with the required frequency. For the third instance, individual PACS panels are unable to generate alerts for unsuccessful authentication attempts, [REDACTED]. [REDACTED] the noncompliance was resolved with a TFE. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p> <p>While the noncompliance is being fully mitigated, the Entity has protected against reoccurrence by modifying applicable procedures and by providing additional training.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) inventoried and identified the account; 2) conducted an extent of conditions analysis on devices with this software installed; 3) developed a process and form for field personnel to use in identifying generic and default accounts; and 4) updated the account management tool and determined password capabilities for newly identified generic/default accounts. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) configured the controls for password complexity; and 2) implemented a software controlled enforcement for password complexity. 					

To mitigate the third instance of noncompliance, the Entity:

- 1) added the devices to existing TFEs; and
- 2) now collects device statistics regarding unsuccessful attempts and alerts are issued by the syslog server.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018018954	CIP-004-6	R4	[REDACTED] (the Entity)	[REDACTED]	07/01/2017	08/07/2017	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 October 16, 2017, the Entity submitted a Self-Log stating that as a [REDACTED] it was in noncompliance with CIP-004-6 R4. [REDACTED]</p> <p>[REDACTED] The noncompliance impacted [REDACTED]</p> <p>The Entity failed to verify, [REDACTED] security groups, at least every 15 calendar months, that access to the designated storage locations for BES Cyber System Information (BES CSI) were correct and were determined by the Responsible Entity to be necessary for performing the assigned work functions as required by P4.3 and P4.4.</p> <p>The cause of the noncompliance was that the Entity failed to follow its processes related to verification of user accounts/groups and their privileges to access designated BES CSI storage locations were correct and necessary.</p> <p>The noncompliance began on July 1, 2017, when the obligation became mandatory under the Standard and Requirement, and ended on August 4, 2017 when the verification was complete.</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 (BPS). The duration of the noncompliance was limited to 35 days. The Entity reports that the users in the affected security groups did not have direct access to any systems, which operate or monitor the BPS. The Entity states that the security groups that had been created were valid groups with a legitimate need, and retained their access after the review. 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 access for all [REDACTED] groups; 2) defined a process for confirming server and entitlement names associated with BES CSI information repositories; and 3) added all BESCSI information repository security groups and entitlements to their Identity Management System. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019231	CIP-007-6	R5	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	12/13/2018	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 January 10, 2018, the Entity submitted a Self-Log stating that, as [REDACTED] it was in noncompliance with CIP-007-6 R5. [REDACTED]</p> <p>[REDACTED] The Self-Log contained three instances of noncompliance.</p> <p>The first instance of noncompliance involved BES Cyber Assets and Protected Cyber Assets (PCAs) that did not have their passwords changed within the 15-month requirement in P5.6. The noncompliance impacted [REDACTED] account passwords on [REDACTED] BES Cyber Assets and [REDACTED] accounts on [REDACTED] PCAs that were located in [REDACTED] substations and [REDACTED] accounts that were on [REDACTED] BES Cyber Assets in [REDACTED] substations. The Entity reports that the passwords were not timely changed because of communication errors in scripts used to automate password changes and a lack of field resources to perform updates at remote locations. The noncompliance began on October 1, 2017, when the obligation to change a password under the Standard and Requirement became enforceable and ended on October 27, 2017, when the passwords were changed.</p> <p>The second instance of noncompliance involved a nested account password that did not have its default password changed. A nested account is an account that can only be accessed after a user has successfully authenticated into another account. The Entity reports that this is a calibration account that the vendor intends to be used by its field staff. The Entity estimated that the noncompliance impacted approximately [REDACTED] devices across [REDACTED]. The cause of the noncompliance was a failure to follow the Entity’s documented processes regarding password changes. The noncompliance began on July 1, 2016 when the Standard and Requirement became enforceable and ended on December 13, 2018, when the default passwords were changed.</p> <p>The third instance of noncompliance involved default passwords on [REDACTED] BES Cyber Assets (each a different model) located in substations [REDACTED]. The Entity reports that it conducted an extent of conditions analysis on all devices of the same device type and did not find any additional instances of noncompliance. The noncompliance was discovered while conducting vulnerability assessments. The cause of the noncompliance was a failure to follow the Entity’s documented processes regarding password changes. The noncompliance began on July 1, 2016 when the Standard and Requirement became enforceable and ended on July 19, 2017, when the default passwords were changed.</p> <p>The noncompliance began on July 1, 2016 when the Standard and Requirement became enforceable and ended on December 13, 2018, when all the default passwords in instance two had been 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. The Entity reports that each of the devices impacted by the noncompliance was located in a substation and not in a Control Center and all were afforded all the other required Cyber Security Controls including being located within a functioning Physical Security Perimeter (PSP) and Electronic Security Perimeter (ESP). Additionally, regarding the second instance, the Entity states that the calibration account could only be accessed after successfully authenticating into one of the device’s other accounts; an account with a password that met the complexity requirements of R5. Further, regarding the third instance, the Entity reports that the [REDACTED]</p> <p>[REDACTED] No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) changed the passwords; 2) scheduled password changes to coincide with the cyber vulnerability assessment; 3) increased the robustness of its SharePoint site and added references change control and vulnerability assessment forms; and 4) enhanced required training for engineering staff and new employees and enhanced job aids. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019584	CIP-002-5.1	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	3/30/2019	Self-Log	9/30/2019
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 violation.)			<p>On April 10, 2018, the Entity submitted a Self-Log stating that as a [REDACTED] it was in noncompliance with CIP-002-5.1a R1. [REDACTED]</p> <p>[REDACTED] The self-log contained four instances of noncompliance.</p> <p>In the first instance of noncompliance, the Entity states that it failed to identify each medium impact BES Cyber System as required by P1.2. The Entity states that during a cyber vulnerability assessment of an [REDACTED] substation, it discovered that a relay was not correctly identified during the CIP-002-5 inventorying that occurred during CIP v5 transition. The Entity reports that the relay did not have External Routable Connectivity (ERC) or Interactive Remote Access (IRA). The noncompliance was caused by the Entity not correctly following its documented process. The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on December 22, 2017, when the BES Cyber System documentation was updated.</p> <p>In the second instance of noncompliance, the Entity states that it failed to identify each medium impact BES Cyber System as required by P1.2. The Entity states that during a cyber vulnerability assessment, it discovered there were [REDACTED] relays, located in a [REDACTED] substation, which were not correctly identified during the CIP-002-5 inventorying that occurred during CIP v5 transition. The Entity reports that the relays were identified in the Electronic Security Perimeter (ESP) diagram and did not have ERC or IRA. The noncompliance was caused by the Entity not correctly following its documented process. The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on June 23, 2017, when the BES Cyber System documentation was updated.</p> <p>In the third instance of noncompliance, the Entity states that in preparation for the 2017 Compliance Audit, it completed a review [REDACTED]. The review identified [REDACTED] BES Cyber Assets located in substations that were not correctly identified during the CIP-002-5 inventorying that occurred during CIP v5 transition; the BES Cyber Assets did not have ERC or IRA. The noncompliance was caused by the Entity not correctly following its documented process. The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on March 23, 2018, when the BES Cyber System documentation was updated.</p> <p>In the fourth instance of noncompliance, the Entity states that it conducted an extent of conditions analysis after discovering instances one through three. During that analysis, the Entity discovered [REDACTED] Annunciators and [REDACTED] Programmable Logic Controllers (PLCs), located in [REDACTED] substations, that were not correctly identified as medium impact BES Cyber Assets, during the CIP-002-5 inventorying that occurred during CIP v5 transition. The Entity failed to apply the required Cyber Security protections to the PLCs after determining they met the criteria of BES Cyber Asset, and then subsequently determined that the PLCs did not meet the criteria of BES Cyber Asset. The cause of the noncompliance was that the Entity inaccurately understood the equipment functionality and, as a result, the Entity failed to follow its process for identifying the BES Cyber Assets. The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on March 30, 2019, when the BES Cyber System documentation was updated to remove the PLCs from the list of BES Cyber Assets.</p> <p>The noncompliance began on July 1, 2016 when the substation was required to be identified, and ended on March 30, 2019 when the PLCs were removed from the BES Cyber System documentation.</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. Per the entity, this issue was limited to a single substation. None of the devices had ERC or IRA. Additionally, for the BES Cyber Assets in instances one through three, the Entity was providing the BES Cyber Assets with the required Cyber Security controls including logging, account inventorying, complex passwords, patching, storage information and recovery plans. For the fourth instance of noncompliance, the Entity was protecting the devices above the requirements of the CIP Standards by placing the devices in a Physical Security Perimeter; further, the use of the annunciators is limited to situational awareness purposes and if disabled, the Entity can utilize a transient device. No harm is known to have occurred.</p> <p>While the noncompliance is being fully mitigated, the Entity has protected against reoccurrence by modifying its cyber vulnerability assessment process and providing additional training.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) added the BES Cyber Assets in instances one through three and the annunciators in instance four to the BES Cyber System documentation; 2) removed the PLCs in instance four from the BES Cyber System documentation; 3) to address the PLCs in instance four, it discussed with its protection engineering and communication engineering teams the necessity to obtain device functional capacity during the BES Cyber Asset determination; 					

- 4) to address the Annunciators in instance four, worked with its vendor to develop a white paper summarizing the devices contained in its closed-loop system and how security controls should be managed in that system; and
- 5) augmented its vulnerability process to include a panel-by-panel and end-to-end inventory process.

To mitigate the noncompliance, the Entity will, by September 30, 2019:

- 1) will be developing a new “device lifecycle process” which is an improved process to address device onboarding, baseline, testing, and other security commissioning requirements; and
- 2) implement the cyber security controls identified in the white paper for closed-loop systems.

The length of the mitigating activities is due to the creation of a new “device life cycle process” that needs to be scoped and then fully developed prior to completing the activity and the implementation of the security controls for the closed-looped system could only begin after the white paper was completed which was completed on or around June 30, 2019.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019020945	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	7/1/2016	6/30/2019	Self-Log	November 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 violation.)			<p>On January 10, 2019, the Entity submitted a Self-Log stating that, as [REDACTED] it was in noncompliance with CIP-010-2 R1. [REDACTED] The Self-Log contained three instances of noncompliance.</p> <p>The first instance of noncompliance involved [REDACTED] BES Cyber Assets that were located in [REDACTED] substations [REDACTED] While conducting vulnerability assessments, the Entity discovered that these devices did not have the correct firmware version documented in the device’s baseline as required by P1.1. The cause of the noncompliance was two distinct deficiencies in the Entity’s processes; most of the BES Cyber Assets did not have their baselines correctly documented due to a lack of sufficient detail that resulted in inadequate preparations during device commissioning, the remaining BES Cyber Assets did not have their baselines correctly documented due to insufficient instructions on how to determine the correct firmware version for a particular device model. The noncompliance began on July 1, 2016 when the Standard and Requirement became enforceable and ended on June 30, 2019, when the baselines were updated.</p> <p>The second instance of noncompliance involved [REDACTED] BES Cyber Assets that were located in [REDACTED] substation [REDACTED] The Entity received change control documentation from substation technicians on November 1, 2018 regarding BES Cyber Assets that had a change applied on September 27, 2018. The baselines were not updated within 30 days of a change as required by P1.2. The cause of the noncompliance was that due to a lack of training, substation engineers and contract engineering resources failed to follow the Entity’s processes. The noncompliance began on October 27, 2018, 31 days after the changes were made, and ended on November 14, 2018, when the baselines were updated.</p> <p>The third instance of noncompliance involved [REDACTED] BES Cyber Assets that were located in [REDACTED] substations [REDACTED] While conducting vulnerability assessments, the Entity discovered that these devices had the required information recorded in the relay engineering department, but a formal baseline was not created for these devices as required by P1.1. Additionally, the Entity discovered that [REDACTED] of the devices did not have their default passwords changed as required by CIP-007-6 P5.4. The cause of the noncompliance were deficiencies in the Entity’s processes that failed to ensure that baselines were created. The noncompliance began on June 7, 2018 when the first device was deployed, ended on October 26, 2018, when the baselines were updated.</p> <p>The noncompliance began on July 1, 2016 when the Standard and Requirement became enforceable and ended on June 30, 2019, when the baselines in instance one 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 Entity states that the devices were located in functioning Physical Security Perimeters (PSPs) and Electronic Security Perimeters (ESPs) during the noncompliance. The Entity reports that the devices were afforded the required Cyber Security protections (except for the subset of devices in instance three that did not have their default passwords changed). Finally, the devices were located in the substation environment and not in a Control Center. No harm is known to have occurred.</p> <p>While the noncompliance is being fully mitigated, the Entity has protected against reoccurrence by modifying applicable procedures and by providing additional training.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the firmware version for the BES Cyber Assets in the baseline documentation; and 2) contacted the vendor for the one model and requested instructions for retrieving information regarding the firmware version. <p>To mitigate the first instance of noncompliance, the Entity will be developing a new “device lifecycle process” which is an improved process to address device onboarding, baseline, testing, and other security commissioning requirements. This mitigating activity is expected to be completed by November 30, 2019.</p> <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the baseline documentation; and 2) conducted additional training sessions for field technicians, substation engineering resources, and project management resources regarding CIP deliverable due dates and in-service dates. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021359	CIP-002-5.1	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	02/11/2019	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 10, 2019, the Entity submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-002-5.1a R1. [REDACTED]</p> <p>[REDACTED] The noncompliance occurred in the operating area of [REDACTED]</p> <p>On December 19, 2018, during a biannual review of its low impact BES Cyber Asset list (P1.3), the Entity identified that a substation containing low impact BES Cyber Systems was not included in the list. The substation is jointly owned, and the Entity did not own any of the BES Cyber Assets that were located at the substation. The Entity's guidelines did not provide clear guidance to the engineering staff regarding the need to classify this as a substation containing low impact BES Cyber Systems.</p> <p>The cause of the noncompliance was that the Entity's documented BES substation guidelines did not provide clear definition and guidance to include jointly owned substations on the low impact list when the Entity did not own any BES Cyber Asset, but where the jointly owned substation contained low impact BES Cyber Systems.</p> <p>The noncompliance began on July 1, 2016 when the substation was required to be identified, and ended on February 11, 2019 when the low impact list was updated to correctly identify the substation.</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. Per the entity, this issue was limited to a single substation. Additionally, the other joint-owner owned all the Cyber Assets associated with the low impact BES Cyber Systems and that registered entity was maintaining and protecting those Cyber Assets. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) correctly identified and included the jointly owned substation in the low impact asset list; 2) revised the BES substation guidelines to provide clear definitions to identify jointly owned substations; and 3) finalized the low impact asset list based on the new revised guidelines during the next scheduled biannual 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
MRO2019021391	CIP-004-6	R5	[REDACTED] (the Entity)	[REDACTED]	11/10/2018	2/19/2019	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 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R5. [REDACTED] The noncompliance impacted [REDACTED] The Self-Log contained three instances of noncompliance.</p> <p>The first instance of noncompliance involved unescorted physical access to a jointly owned [REDACTED] substation by a joint owner's employee. As part of its quarterly review process, the Entity contacts the joint owners to confirm the ongoing need of individuals with physical access to jointly owned medium impact substations. The Entity states that during this process, the joint owner reported that an employee with physical access had resigned effective November 9, 2018. The cause of the noncompliance was that the joint owner did not inform the Entity of the resignation within 12 hours as required by their agreement. The noncompliance began on November 10, 2018, 24 hours after the termination action and ended on January 8, 2019 when physical access was removed.</p> <p>The second instance of noncompliance involved unescorted physical access to [REDACTED] assets. The employee resigned with an effective date of February 2, 2019. The employee's manager was on vacation when the resignation became effective and did not submit the removal request until February 4, 2019. The cause of the noncompliance was that the Entity failed to follow its process for removal. The noncompliance began on February 3, 2019, 24 hours after the termination action and ended on February 4, 2019 when physical access was removed.</p> <p>The third instance of noncompliance involved unescorted physical access to [REDACTED] assets. The employee retired with an effective date of February 16, 2019. The employee's manager was on vacation when the resignation became effective and did not submit the removal request until February 19, 2019. The cause of the noncompliance was that the Entity failed to follow its process for removal. The noncompliance began on February 17, 2019, 24 hours after the termination action and ended on February 19, 2019 when physical access was removed.</p> <p>The noncompliance was noncontiguous; the noncompliance began on November 10, 2018, 24 hours after the termination action in instance one and ended on February 19, 2019 when the access in instance three was removed.</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. In all three instances, the Entity states that the employee's did not have electronic access and the badges were surrendered upon resignation and were secured during the period of noncompliance. Additionally, the Entity reports that it confirmed that none of the badges were used during the noncompliance. Finally, the Entity states that none of the instances of noncompliance involved a termination for cause. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) removed the physical access; and 2) reinforced the joint owners contractual obligation to promptly report a termination. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) removed the physical access; 2) sent the responsible manager a counseling letter to educate the manager on the importance and responsibilities of timely CIP access removal and how to ensure the process is initiated during periods of time that the manager will be out of the office; and 3) had its Vice-President of Human Resources send a communication reinforcing the company's policies on submitting access removal forms prior to the employee's last working day. <p>To mitigate the third instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) removed the physical access; and 2) sent the responsible manager a counseling letter to educate the manager on the importance and responsibilities of timely CIP access removal and how to ensure the process is initiated during periods of time that the manager will be out of the office. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021448	CIP-006-6	R2	[REDACTED] (the Entity)	[REDACTED]	01/4/2019	01/4/2019	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 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-006-6 R2. [REDACTED]</p> <p>The Entity reports that a substation construction employee had previously been granted unescorted physical access to a [REDACTED] substation. The Entity states that the employee changed job assignments, and due to an error during that process, the employee's physical access was inadvertently removed. On January 4, 2019, the employee was not able to enter the substation control house with his badge. A co-worker used his badge to allow the employee to enter the control house and did not escort during the employee for the 13 minutes that the employee was in the control house. This was in violation of the Entity's visitor escort policy. After exiting the control house, the employee called security personnel to inquire as to why his security badge did not work. [REDACTED]</p> <p>The cause of the noncompliance was the Entity failed to follow its process regarding maintaining a continuous escort.</p> <p>The noncompliance began on January 4, 2019, when the employee was not escorted in the control house and ended on 13 minutes later when the employee exited the control house.</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 Entity states that the employee had prior unescorted physical access and should have had unescorted physical access during the time of the noncompliance. [REDACTED] No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) had its employee leave the control house; and 2) instructed both employees that they have violated the Entity's policies and reinforced the policies regarding continuous escorts and that prohibit badge sharing. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021450	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	01/18/2019	01/29/2019	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 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-007-6 R2. [REDACTED] The noncompliance impacted [REDACTED]</p> <p>On January 23, 2019, during an internal patch coordination meeting (an internal control held twice monthly to review the status of security patch assessments and implementation), the Entity discovered that [REDACTED] security patches were not evaluated within 35 days of the last security patch review. The release of these four patches coincided with another set of [REDACTED] patches. The team focused on the second set of patches and as a result, failed to complete their evaluation of the first set within 35 days of the last security patch review.</p> <p>The cause of the noncompliance was the Entity failed to follow its process regarding evaluating patches within 35 calendar days from the last security patch review.</p> <p>The noncompliance began on January 18, 2019, which was one day after the 35-day window and ended on January 29, 2019 when the patches were evaluated.</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. Per the Entity, the patches were evaluated and applied within the seventy day time frame that is allowed under CIP-007-6 R2 (35 days in P2.2 and 35 days in P2.3). No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) evaluated and applied the security patches; 2) reinforced the importance of timely evaluation to the team; 3) reviewed the patching spreadsheet filter to remove confusion caused by multiple patch evaluations; and 4) modified the patching process to review the patching spreadsheet weekly. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021451	CIP-011-2	R2	<div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> (the Entity)	<div style="background-color: black; width: 100%; height: 15px;"></div>	12/18/2018	01/2/2019	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 10, 2019, the Entity submitted a Self-Log stating that, as <div style="background-color: black; width: 100%; height: 15px; display: inline-block;"></div> it was in noncompliance with CIP-0011-2 R2. <div style="background-color: black; width: 100%; height: 15px; display: inline-block;"></div></p> <p>The noncompliance involved a Protected Cyber Asset (PCA) that was temporarily installed at an <div style="background-color: black; width: 100%; height: 15px; display: inline-block;"></div> substation. The PCA was temporarily installed for testing purposes and was removed from service on December 18, 2018 and returned to the service center. The PCA was not reset to factory defaults prior to returning the device to the service center as required by P2.1. The Entity reports that the noncompliance was discovered by a compliance engineer during a review of the PCA’s change control documentation, who promptly reset the PCA to its factory default settings.</p> <p>The cause of the noncompliance was the Entity failed to follow its process to reset the device to factory settings prior to returning the device to the service center.</p> <p>The noncompliance began on December 18, 2019, when the device was removed from the substation and ended on January 2, 2019 when the device was reset to its factory settings.</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. During the period of the noncompliance, the Entity states that the PCA was secured in the service center in a location that was controlled by badge access. Further, all the required Cyber Security controls were applied to the device. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) reset the device to factory defaults; 2) conducted training for its transmission construction team on the importance of change control requirements; and 3) conducted refresher training for its substation engineering team on its change control requirements. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021267	CIP-002-5.1	R2	[REDACTED] (the Entity)	[REDACTED]	12/01/2016	07/25/2017	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 January 24, 2019, the Entity submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-002-5.1 R2. [REDACTED]</p> <p>[REDACTED] Per the Entity, a contractor performing operational and compliance services missed the 15-month requirement to review and approve the list of assets and BES Cyber Systems.</p> <p>The cause of noncompliance is the Entity did not have enough controls in place to ensure the contractor completed the required review and approval of BES cyber assets in the designated time period of 15 months.</p> <p>The noncompliance began on December 1, 2016, which was 15 months after the lists had been previously reviewed, and ended on July 25, 2017 when the list of BES Cyber Systems in CIP-002-5.1a R1 was reviewed and approved.</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 nameplate capability of the windfarms are 150 MW and 200 MW respectively. Due to their relatively small size and non-dispatchable nature, the potential adverse impact to the BES from the loss, compromise, or misuse of these two wind facilities is limited. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) reviewed and approved the list of BES Cyber Systems for CIP-002-5.1a R1 as required by CIP-002-5.1a R2; 2) created a NERC Compliance department with professionals dedicated to review and help SMEs develop controls to reduce the risk of noncompliance; and 3) implemented the use of "GenSuite" which is a scheduling application that sends reminders to multiple personnel when a task needs to be performed. The application also has escalation capabilities when a task is incomplete and approaching its due date. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020161	CIP-011-2	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	04/26/2019	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 June 28, 2018, the Entity submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-011-2 R1. The Self-Report included five issues.</p> <p>For the first issue, the Entity discovered that network configurations, which they consider as being BES Cyber System Information (BCSI), were being stored on a specific server that was not a BCSI designated storage location. This instance began on July 1, 2016, when the requirement went into effect, and ended on May 9, 2018, when the BCSI was moved to a designated storage location for BCSI. After the first issue was discovered, the Entity’s contractor filled a new position of “Lead Network Administrator” for management of the Entity’s SCADA Network and the Entity’s CIP V5 implementation procedures. The new Lead Network Administrator conducted an extent of conditions review to seek out additional instances of noncompliance.</p> <p>For the second issue, discovered during an extent of condition review, an Entity Information Security Officer (ISO) determined that the Entity’s change management ticketing system which includes the application, database, and two index servers should have been identified as BCSI electronic storage locations when CIP-011-2 became effective. This issue began on July 1, 2016, when CIP-011-2 became effective and ended on April 26, 2019, when the servers were designated as BCSI storage locations.</p> <p>For the third instance, discovered during the same extent of condition review, an Entity ISO determined that a system used for e-discovery processes allowed users to pull BCSI information from other existing designated storage locations to be stored on the system. The system database consists of three servers having direct-attached storage, which should have been identified, as BCSI electronic storage locations when CIP-011-2 became effective. This issue began on July 1, 2016, when CIP-011-2 became effective and ended on April 26, 2019, when the servers were designated as BCSI storage locations.</p> <p>For the fourth issue, discovered during the same extent of condition review, an Entity ISO discovered that BCSI such as groupings of IP addresses used by System and Network Administrators was stored in a folder in SharePoint and that folder was not in a designated storage location. This issue began on July 1, 2016, when CIP-011-2 became effective and ended on February 5, 2019, when folders were moved into a designated BCSI storage location.</p> <p>For the fifth issue, discovered during the same extent of condition review, an Entity ISO discovered that the folder which was intended to be used by the CIP V5 implementation team to review potential BES Cyber Assets still contained the Cyber Asset list and associated IP addresses. The folder contained BCSI-related files used by Network and System Administrators, but was not deleted once the transition project was completed. Also, the folder was not contained in an identified BCSI electronic storage location when CIP-011-2 became effective. This issue began on July 1, 2016, when the requirement became effective, and ended on January 16, 2019, when the folder containing the Cyber Asset list and associated IP addresses was deleted.</p> <p>The cause of the noncompliance was the Entity had an incomplete understanding of what constituted BCSI, which resulted in a lack of training and guidance for the personnel involved in transition activities and deficiency in the transition planning process for the CIP Version 5 implementation.</p> <p>The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on April 26, 2019, when the servers were designated as BCSI storage locations.</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 the Entity, the first issue was minimal because the server where the BCSI was stored resides within the SCADA system Electronic Security Perimeter (ESP), so it was protected accordingly by protections which exceeded those required for BCSI alone. Additionally, logical access to the servers hosting the BCSI was restricted to a smaller number of personnel than access to general BCSI storage locations due to the server being within an ESP. All employees with logical access to the servers already had authorized access to the BCSI storage location. The Entity also states that all the issues were minimal because the risk of misuse by the BCSI information was mitigated by protections including: [REDACTED] is prohibited; the [REDACTED] and are reviewed annually reducing the threat vector; network devices within the ESP would have alerted the Administrator and Information Security Officers in the event of unauthorized access attempts; and the data was not accessible [REDACTED] and although the servers were not designated BCSI storage locations, [REDACTED].</p> <p>No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					

Mitigation	To mitigate the noncompliance, the Entity: 1) moved the data in the first and fourth instance to an existing designated BCSI storage location; 2) designated the servers in instance two and three as BCSI storage location; 3) deleted the BSCI data in instance five; and 4) had its contractor fill a new position of "Lead Network Administrator" for management of the Entity's SCADA Network and the Entity's CIP V5 implementation procedures.
-------------------	---

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021754	CIP-007-6	R5. (5.2)	[REDACTED]	[REDACTED]	7/1/2016	5/23/2019	Self-Report	12/23/2019
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 June 28, 2019, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-007-6 R5 (5.2).</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and the entity failed to identify and inventory all known enabled default or other generic account types. The noncompliance ended on May 23, 2019, when the entity combined the application level and OS level accounts. The merged accounts were included in the entity's inventory of accounts.</p> <p>On March 27, 2019, an issue was discovered when a subject matter expert (SME) was working with the [REDACTED] team to transition access due to a change in responsibilities. They discovered that a single application level account was not inventoried. The account is used to [REDACTED].</p> <p>The account predated the transition of cyber assets to the NERC CIP V5 program (the account was not in previous Version 3 program) and was not inventoried during the onboarding of new assets.</p> <p>The entity failed to inventory the account because of a misunderstanding surrounding the account names. The application level account shares a name with an Operating System (OS) level account. The OS level account was properly inventoried leading the entity to incorrectly assume that the application level account with the same name was also inventoried, when it was not actually properly inventoried.</p> <p>The root cause of this noncompliance was lack of proper controls and specifically a weakness in the verification control used by the entity to verify that all accounts were inventoried.</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>Specifically, failing to inventory an account could result in a lack of protection to accounts that could lead to compromise of applicable Cyber Assets rendering them unavailable, degraded, or misused. However, the administrators of the system were aware of the account and did not realize it was not properly inventoried from a CIP program perspective.</p> <p>Additionally, the account was only accessible through a server controlled through [REDACTED]. All personnel with access to the account password have current Personnel Risk Assessments (PRA), CIP training, and a business need for the access. The account is a service account that can only be used to [REDACTED] can be performed with this account.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>The entity has relevant compliance history. However, NPCC determined that the entity's compliance history should not serve as a basis for applying a penalty because this noncompliance is minimal risk and the relevant compliance history does not indicate a broad programmatic failure.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) transferred the authentication method from the application level account to the Operating System account that is included in the entity account inventory; and 2) linked the access and authentication method for both accounts. <p>To mitigate this noncompliance, the entity will by December 23, 2019, obtain certification from role owners through verification that all access is accounted for during the [REDACTED]. The amount of time required to complete this final mitigation activity is related to an annual review.</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
NPCC2019021756	CIP-007-6	R5. (5.3)	[REDACTED]	[REDACTED]	7/1/2016	4/18/2019	Self-Report	12/23/2019
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 June 28, 2019, New York Independent System Operator (the entity) submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-007-6 R5. (5.3.)</p> <p>This noncompliance began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and the entity failed to identify all individuals who had authorized access to shared accounts. The noncompliance ended on April 18, 2019, when the entity provided proper authorization for the shared account access within the Identity and Access Management System.</p> <p>During a review of access by the [REDACTED], the entity determined that a Subject Matter Expert (SME) knew the password to a shared account. The SME had a business need for the access, but authorization for the access was not documented in the entity's [REDACTED].</p> <p>The root cause of this issue was ineffective documentation controls. Specifically, access was never onboarded into the SME's role. The SME had been an administrator of the system and had access prior to the account being in the CIP program. The account was brought into the CIP program during the CIP V5 transition, but the SME's authorization was not properly documented in the [REDACTED]. It was incorrectly assumed that the SME was authorized for the role due to the SME being authorized for a role with similar access.</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>Specifically, failing to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. However, the entity has processes that reduce the risk and operate as preventative controls. All employees receive proper CIP training, Personnel Risk Assessments (PRAs), and there are multiple layers of authentication on CIP assets along with an annual password change.</p> <p>This noncompliance was largely a documentation issue. The SME involved was authorized and had been an administrator since before the account was included in the CIP program as part of the CIP V5 transition. The account was used to [REDACTED] and would not allow a user to modify [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 prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) properly authorized the SME for shared account access within the [REDACTED]; and 2) focused its [REDACTED] awareness campaign on proper [REDACTED] (sending emails company-wide and posters placed at key locations). <p>To mitigate this noncompliance, the entity will by December 23, 2019, obtain certification from role owners through verification that all access is accounted for during the [REDACTED]. The amount of time required to complete this final mitigation activity is related to an annual review.</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
RFC2018019969	CIP-011-2	R2	[REDACTED]	[REDACTED]	10/11/2017	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 June 20, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-011-2 R2.</p> <p>In October 2017 and January 2018, the entity gave two relays to [REDACTED] employees for reuse. (All employees that handled the relays had approved CIP access, valid Personnel Risk Assessments, and current NERC CIP training.) The entity removed one relay from the [REDACTED] station (on October 11, 2017) and the other relay from the [REDACTED] station (on January 2, 2018). The entity employees that removed the relays did not complete the necessary disposal/reuse paperwork before giving the relays to the [REDACTED] employees. By not completing the necessary disposal/reuse paperwork, the employees did not follow the correct protocol for removing relays and giving them to [REDACTED] employees for reuse.</p> <p>While the relays remained in the [REDACTED] employees' possession and the relay passwords were changed, the entity had no documentation that identified the custodian for the data storage media while the data storage media was outside of the station Physical Security Perimeter (PSP) as required under CIP-011-2.</p> <p>This noncompliance involves the management practices of workforce management and work management. A contributing cause of this noncompliance is that the [REDACTED] employees that received the relays did not understand the necessary paperwork and protocol that had to be followed when removing and reusing a Cyber Asset from a PSP to prevent the unauthorized retrieval of Bulk Electric System (BES) Cyber System Information (BCSI). That lack of understanding arose from ineffective training. The root cause, however, is a lack of an effective internal control to ensure that entity employees follow the entity's CIP-011 BES Cyber Asset Reuse and Disposal Program.</p> <p>This noncompliance started on October 11, 2017, when the entity employees who removed the relays did not complete the necessary disposal/reuse paperwork before giving the relays to [REDACTED] employees and ended on January 18, 2018, when the entity completed the proper custodial documentation for both instances.</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 arises from potentially allowing unauthorized access to BCSI that is stored on the relays by not following protocol when removing a Cyber Asset from a PSP. The risk is minimized because the relays can only be accessed locally by individuals that have authorized logical access and knowledge of the relay passwords. Additionally, the passwords on both relays had been properly changed, which reduced the risk of an unauthorized individual accessing the relays. Lastly, the employees that handled the relays had approved CIP access, valid Personnel Risk Assessments, and current NERC CIP training. 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) took custody of the relays and the passwords were returned to factory settings; 2) had the four employees that were involved in this noncompliance take targeted NERC CIP Information Protection training; 3) met with the relevant group to remind and inform employees of their responsibilities regarding disposal and use and a review of CIP-011; 4) sent a "Did You Know Reminder" to all Transmission personnel reinforcing the fact that the CIP-011 BES Cyber Disposal/Reuse Policy must be followed; 5) incorporated the "NERC CIP Important Items" Job Aid into TFS Safety Briefings at Medium Impact Substations; and 6) formalized its existing detective control. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020579	CIP-007-6	R1	[REDACTED]	[REDACTED]	5/31/2018	7/31/2018	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 19, 2018, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-007-6 R1.</p> <p>On June 18, 2018, as part of the entity's bi-weekly review of its baseline deviations, the entity discovered one service on one device [REDACTED] which was not necessary. The one device involved is a [REDACTED]. The unnecessary service [REDACTED]. The entity investigated to determine how the service got enabled and discovered no apparent reason (e.g. a patch or a software upgrade) which caused the service to be enabled.</p> <p>The entity determined that [REDACTED] had been incorrectly enabled on the one device beginning on May 30, 2018. [REDACTED] Additionally, during mitigation, the entity determined that [REDACTED] was enabled again on this one device on June 4, 2018. Both times [REDACTED] got enabled unintentionally and incorrectly. The entity determined that the [REDACTED] service provided minimal value and disabled the [REDACTED] service on July 31, 2018.</p> <p>The root cause of this noncompliance is that the expected list of ports and services for this device was incorrectly constructed due to ineffectively trained employees. Specifically, the expected list was based on the history of detected listening services rather than the population of ports and services required by the device's operating system.</p> <p>This noncompliance involves the management practices of verification and workforce management. Verification is involved because the entity failed to confirm that the affected device was operating only necessary services. Workforce management is involved because the root cause of the noncompliance stemmed from ineffective training.</p> <p>This noncompliance started on May 31, 2018, when the unnecessary [REDACTED] service began showing up on the device intermittently and ended on July 31, 2018, when the entity disabled the [REDACTED] service.</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 risk posed by this instance of noncompliance is the potential for a bad actor to access Bulk Electric System Cyber Systems through unidentified open communication channels resulting in harm to the BPS. The risk is minimized because the [REDACTED] service [REDACTED] is not known to cause any harm. The entity determined that the service provided minimal value and then disabled the service. Additionally, the noncompliance was detected through the use of an internal control (an internal bi-weekly review). For the duration of the noncompliance, the device was protected within an Electronic Security Perimeter (ESP) and a Physical Security Perimeter. Any access to the device must be authorized and requires the use of an intermediate system, which enforces two factor authentication and encryption. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disabled the [REDACTED] service on all [REDACTED] devices in the domain; 2) performed an Extent of Condition review and no additional instances were discovered. (The entity did not detect any additional instances of noncompliance with CIP-007-6 R1 while performing the extent of condition in Milestone 2. Although the entity did not identify any additional instances of noncompliance, the entity did identify differences between the entity's population of necessary ports and services as required by the [REDACTED] System [REDACTED]. As a result, completion of Milestone 3 aligned the entity's population of necessary ports and services required by the [REDACTED] System [REDACTED].) 3) based on the results of the extent of condition, the entity made any necessary adjustments to the approved ports and services for the device taxonomies; 4) created and implemented a preventative control as a part of the change management process to identify new ports and services caused by the introduction or modification of a device. (For new devices, the population of necessary ports and services will be identified and supported with valid justifications prior to placing new devices into an ESP. For modifications to existing devices, changes will be tested on representative test systems to identify any new ports and services caused by the change. Any new ports and services identified will be evaluated for necessity and supported with valid justifications.); and 5) conducted training on the new preventative control. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018304	CIP-004-6	R4	[REDACTED]	[REDACTED]	6/22/2017	6/23/2017	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 September 1, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance with CIP-004-6 R4.</p> <p>On June 22, 2017, a contractor who had not yet been provided a computer or account access began working at the entity. On that same day, another entity contractor logged in to an entity network laptop using their own credentials so that the new contractor could work on that laptop. The new contractor was left unsupervised to work on a spreadsheet that was opened on the laptop. The user account of the contractor who logged in had read/write access to the [REDACTED] on the shared network, which contains Bulk Electric System (BES) Cyber System Information (CSI).</p> <p>The root cause of this noncompliance was inadequate training for individuals with access to BES Cyber System Information access which resulted in the decision of an entity contractor to use their credentials to log in to a BES Cyber Asset and provide unsupervised access to another contractor.</p> <p>This noncompliance involves the management practice of workforce management because the contractors integrated into the entity's workforce were not properly trained on internal access procedures.</p> <p>The noncompliance began on June 22, 2017, the date the contractor used his login credentials to provide unsupervised access to another contractor. The violation ended on June 23, 2017, the date the entity provided the new contractor with properly authorized 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 (BPS) based on the following factors. The risk posed by this noncompliance is that an unauthorized actor could utilize NERC CIP information or a BES Cyber Asset to adversely impact the BPS. The risk is minimized because the contractor who received access was from a trusted vendor and the contractor was ultimately given authorized access. Upon review, the contractor erroneously provided access to the laptop did not access the BES CSI information. Thus, the risk posed to the bulk power system was minimal. 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) changed the contractor's password for the corporate account; 2) retrained individuals with access to BES Cyber System Information on the Information Protection Procedures; and 3) reviewed access levels for everyone with access to BES Cyber System Information to ensure they only have access to the specific folders that they need. <p>ReliabilityFirst 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
RFC2017017652	CIP-007-6	R2	[REDACTED]	[REDACTED]	3/3/2017	3/8/2017	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 May 24, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance with CIP-007-6 R2.</p> <p>In order to comply with CIP-007-6 R2, and its patch assessment requirements, the entity's 35 day deadline to review and assess certain patches was March 2, 2017. However, the entity did not complete these patch assessments until March 8, 2017.</p> <p>The entity failed to assess the patches within the time required by CIP-007-6 due to staffing issues as a result of two CIP employees departing just before the assessment was due. More specifically, the root cause was the exit of two CIP subject matter experts assigned to the monthly patching cycle who left the entity on February 15, 2017, and additional staff could not cover the patch management responsibility due to a prioritized review [REDACTED]. This noncompliance involves the management practices of workforce management because the entity was understaffed as a result of two employees leaving the entity and not having sufficient processes and resources to ensure timely coverage of their responsibilities.</p> <p>The noncompliance began on March 3, 2017, the date by which the entity was required to assess patches, and ended on March 8, 2017, the date the entity assessed the patches for implementation.</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 risk posed by this noncompliance is the opportunity for a bad actor to infiltrate the Electronic Security Perimeter (ESP) and associated systems when security patches and upgrades are not installed on Cyber Assets within the ESP, thereby adversely impacting the reliability of the BPS. The risk is minimized in this noncompliance because although the patch assessment process was untimely, the entity quickly identified and corrected the issue and the patch installation was timely. Thus, the risk posed to the bulk power system was minimal. 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 there were different root causes than in the corresponding current violation.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the monthly patch discovery to get back into compliance; 2) trained internal personnel to fulfill the role of the subject matter experts that left; and 3) contracted with consultants with CIP compliance experience to assist in the day-to-day CIP tasks. <p>ReliabilityFirst 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
RFC2017018562	CIP-007-6	R2	[REDACTED]	[REDACTED]	8/11/2017	8/26/2017	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 25, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance with CIP-007-6 R2.</p> <p>In order to comply with CIP-007-6 R2, and its patch assessment requirements, the entity's 35 day deadline to review and assess certain patches was August 11, 2017. However, the entity did not complete these patch assessments until August 26, 2017.</p> <p>The root cause of this noncompliance related to staff unavailability [REDACTED]. The entity used most of its workforce resources to review [REDACTED], demonstrating insufficient workforce management processes.</p> <p>The noncompliance began on August 11, 2017, the date by which the entity was required to assess patches, and ended on August 26, 2017, the date the entity assessed the patches for implementation.</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 risk posed by this noncompliance is the opportunity for a bad actor to infiltrate the Electronic Security Perimeter (ESP) and associated systems when security patches and upgrades are not installed on Cyber Assets within the ESP, thereby adversely impacting the reliability of the BPS. The risk is minimized because the entity quickly identified and corrected the noncompliance (within 15 days). Further minimizing the risk, the patches for that period were installed within the required timeframe. Thus, the risk posed to the bulk power system was minimal. 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 there were different root causes than in the corresponding current violation.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the late patch evaluations; 2) completed the patching from the August patching cycle; 3) completed the following months patch evaluations; 4) created a detailed Patching Process Runbook allowing for unscheduled issues during patching process; and 5) cross-trained personnel on patching run book. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018018986	CIP-007-6	R2	[REDACTED]	[REDACTED]	11/25/2017	12/22/2017	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 8, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that [REDACTED] it was in noncompliance with CIP-007-6 R2.</p> <p>The entity failed to perform patch assessments every 35 days as required by CIP-007-6 R2.2. Specifically, the entity completed a patch discovery and assessment process on October 20, 2017. Therefore, the next patch assessment process was due to be processed on November 25, 2017. However, the patch assessment was not completed until December 22, 2017 (26 days late).</p> <p>The entity's failure to comply with CIP-007-6 R2.2 was the result of three different internal issues: 1) [REDACTED] 2) there were formatting issues with the entity's patch assessment spreadsheet; and 3) the integration of new personnel unfamiliar with the process, which involves workforce management.</p> <p>The noncompliance began on November 25, 2017, the date the entity was required to comply with CIP-007-6 R2. The noncompliance ended on December 22, 2017, the date 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 (BPS) based on the following factors. The risk posed by this noncompliance is the opportunity for a bad actor to infiltrate the Electronic Security Perimeter (ESP) or associated systems when security patches and upgrades are not installed on Cyber Assets within the ESP, thereby adversely impacting the reliability of the BPS. The risk is minimized because the entity quickly identified and corrected the violation (within 27 days). Further minimizing the risk, the patches for that period were installed within the required timeframe. Thus, the risk posed to the bulk power system was minimal. 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 there were different root causes than in the corresponding current violation.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the monthly patch discovery for all items; 2) instituted a process to have a person not involved in the patch evaluations execute a final review of the work completed on or before the due date to allow any missing items to be completed; 3) instituted a peer review/cross check process as part of the patch evaluation process to ensure every discovery is reviewed by a peer; 4) created a static list for each team member for patch evaluations to more evenly distribute work; 5) completed security patching from the November Cycle; and 6) completed the following month patch discovery on time within original dates. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017017843	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/1/2016	11/30/2017	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 June 22, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>A Cyber Asset used for Interactive Remote Access to a Medium Impact Bulk Electric System (BES) Cyber System was not identified and evaluated as an Electronic Access Control or Monitoring Systems (EACMS) device. Since the Cyber Asset was not identified and classified as an EACMS device, no documented baseline configuration was maintained for the Cyber Asset in accordance with CIP-010-2 R1.1.</p> <p>The root cause of this noncompliance was the entity's failure to properly apply its internal EACMS identification and evaluation process. Specifically, entity employees failed to properly evaluate firewall rule sets to identify which of the network zones are authorized for inbound or outbound communications to BES Cyber Assets or Protected Cyber Assets within the ESP which resulted in the entity's failure to identify the EACMS involved in this violation.</p> <p>This noncompliance involves the management practices workforce management and asset and configuration management. Workforce management is involved in this noncompliance because entity employees were not properly trained to fulfill CIP-010-2 requirements adequately. Asset and configuration management is involved in this noncompliance because the entity failed to identify a Cyber Asset used as for Interactive Remote Access as an EACMS, and therefore a Cyber Asset resulted a failure to document the baseline configuration as required by CIP-010-2.</p> <p>The noncompliance began on July 1, 2016, the date the entity was required to comply with CIP-010-2 R1. The noncompliance ended on November 30, 2017, the date 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 (BPS) based on the following factors. The risk posed by this noncompliance is that failing to establish baselines for one EACMS device could result in the entity failing to detect and track both authorized and unauthorized changes to these devices; thereby adversely impacting the BPS. The risk is minimized here because the EACMS device was patched, and protected by anti-virus software at all relevant times. Further minimizing the risk, systems security practices were applied to the EACMS device, including user authorization and account management practices. Thus, the risk posed to the bulk power system was minimal. 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 there were different root causes than the corresponding current violation.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) added devices to the [REDACTED] and assigned it the classification of an EACMS or Physical Access Control Systems (PACS) device respectively; 2) performed deployment activities for Interactive Remote Access and PACS devices (validate the necessity of enabled logical network ports; validate authorization of physical ports; validate installed software including all security patch levels; validate communication and logging by the Security Information and Event Management (SIEM); validate Antivirus (AV) server communications and AV updates; validate successful backup reporting; validate backup and restore processes; validate individuals with access to individual and shared accounts; validate authentication practices; validate documented configuration baseline; validate addition to monthly patch discovery, assessment and installation process; and validate addition to network diagram); 3) made editorial improvements to the documented process for identifying and evaluating potential EACMS and PACS devices deemed appropriate by management; 4) developed and provided training to subject matter experts on how to apply the documented process for identifying and evaluating potential EACMS and PACS devices; 5) reapplied the EACMS and PACS identification process; 6) conducted a compliance review of EACMS and PACS identification process; and 7) reviewed evidence of completion and submitted evidence of completion to ReliabilityFirst. <p>ReliabilityFirst 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
RFC2018019771	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/1/2016	5/16/2018	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 May 18, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>The entity had two data collection file scripts ([REDACTED]) that they failed to include in their internal software inventory and thereby failed to establish baselines for as required by CIP-010-2 R1 from July 1, 2016 until January 8, 2018. These scripts' purpose is to passively collect system information.</p> <p>The [REDACTED] was installed on three servers classified as Electronic Access Control or Monitoring Systems (EACMS) devices. The [REDACTED] was installed on twenty-eight applicable Cyber Assets. Of the [REDACTED] Cyber Assets with the [REDACTED], [REDACTED] were Bulk Electric System Cyber Assets, [REDACTED] were EACMS [REDACTED] were Physical Access Control Systems, and two were Protected Cyber Assets.</p> <p>The root cause of this noncompliance is that entity employees misidentified the two custom scripts involved above. The misidentification was discovered by an independent contractor and reflects that entity employees misidentified the two custom scripts because of a lack of understanding of CIP standards.</p> <p>This noncompliance involves the management practices workforce management and asset and configuration management. Workforce management is involved in this noncompliance because entity employees were not properly trained and did not fully understand CIP-010-2. Asset and configuration management is involved in this noncompliance because the entity failed to identify an Interactive Remote Access (IRA) as an EACMS, and therefore a Cyber Asset resulted a failure to document the baseline configuration as required by CIP-010-2.</p> <p>The noncompliance began on July 1, 2016, the date the entity was required to comply with CIP-010-2 R1. The noncompliance ended on May 16, 2018, the date 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 (BPS) based on the following factors. The risk posed by this issue is that failing to establish baselines for two custom software scripts could result in the entity failing to detect and track both authorized and unauthorized changes to these scripts; thereby adversely impacting the BPS. The risk is minimized because the custom scripts were merely performing data collection and did not offer any other functionality. Further minimizing the risk, the omission of the data collection scripts from the baseline software inventory did not cause any security patch to be overlooked. Thus, the risk posed to the bulk power system was minimal. 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 there were different root causes than corresponding current violation.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) added the two scripts names to [REDACTED]; 2) developed and distributed awareness communications about baseline requirements, including but not limited to follow configuration change management processes for custom scripts installed on applicable Cyber Assets; 3) conducted a review of all applicable Cyber Assets for any other scripts that may be eligible for inclusion in the baseline for custom software; 4) revised training for applicable personnel on the requirements for configuration change management, including but not limited to the need to update the software inventory for custom scripts installed on applicable Cyber Assets; and 5) reported the results of the review of the scripts that needed to be added to the Baselines to management. <p>ReliabilityFirst 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
RFC2018019383	CIP-004-6	R1	[REDACTED]	[REDACTED]	8/30/2017	8/31/2017	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 March 1, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-004-6 R1. (This noncompliance was also resolved in the [REDACTED] Region.)</p> <p>On August 30, 2017, the entity's [REDACTED] group inadvertently provided a new contractor, who was not authorized or trained, with electronic access to NERC data. On August 31, 2017, [REDACTED] internal control process identified the noncompliance. [REDACTED] then notified [REDACTED] which removed the access on August 31, 2017.</p> <p>As background, the [REDACTED] security analyst had mistakenly added the new Database Administrator (DBA) contractor to a [REDACTED] group for which access had not been requested or approved. The requests and approval are submitted and completed via a workflow tool that does not communicate with the [REDACTED] group itself. The [REDACTED] security analyst must search for the requested access group in [REDACTED] where authorization is granted, but the large number of [REDACTED] groups and similar nomenclature make it difficult to confirm that the right [REDACTED] group is selected.</p> <p>The root cause of this noncompliance was that the security analyst completing the work inadvertently selected the wrong [REDACTED] group due to the [REDACTED] group naming similarities discussed above, and an insufficient process that allowed the error to occur without detection.</p> <p>This noncompliance involves the management practices of information management and verification. Information management is involved because the entity's [REDACTED] failed to properly protect information by providing a contractor with access to a Physical Access Control Systems Database (PACS) which supported facilities containing High and Medium Impact BCS. Verification management is involved because the entity's process for verifying and adding members to the [REDACTED] group was the central cause of this noncompliance.</p> <p>The noncompliance began on August 30, 2017, the date the entity inadvertently provided a new not authorized and untrained contractor with electronic access to NERC data, and ended on August 31, 2017, the date the entity removed the DBA 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 instance of noncompliance is the provision of electronic access to an unauthorized and untrained individual, potentially resulting in an unintentional or malicious action with operational impacts. This risk is minimized because the entity discovered and remediated the issue within only 24 hours, demonstrating strong internal controls. Additionally, the contractor had a current background check and had recently completed NERC CIP training. Thus, the risk posed to the Bulk-Power System was minimal. No harm is known to have occurred. ReliabilityFirst also notes that the entity's review of the end user's data indicates that the contractor did not access NERC data during the period for which authorized access was granted.</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) removed unauthorized access from contractor's account; 2) added an enhancement to the workflow tool to initiate a pop-up alert when completing a NERC request. To continue with the process, the security analyst requests a peer review and the peer reviewer notes their review in [REDACTED]; and 3) instituted a process improvement to prevent vaulting certain user accounts until [REDACTED] notifies [REDACTED] that the Compliance Process is complete. <p>ReliabilityFirst 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
RFC2017018257	CIP-004-6	R4	[REDACTED]	[REDACTED]	1/5/2017	4/13/2017	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 August 22, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-004-6 R4. (This noncompliance was also resolved in the SERC Region.)</p> <p>On January 5, 2017, an [REDACTED] (an employee) coordinated multiple changes to the entity's Physical Security Perimeters (PSP). Specifically, the entity's employee had interior fencing removed which had separated the [REDACTED] and the [REDACTED] both PSPs from each other as well as separating the [REDACTED] a non-NERC asset. The removal of the fencing shifted the space into one, larger, PSP. The reconfiguration also included the removal of the [REDACTED], leaving only the two PSP access doors remaining. The result of the change was that any individual who was authorized to enter one of the PSPs was able to access both PSPs. The entity's employee incorrectly believed that because both were NERC PSPs every party who had access to either PSP was covered because they had completed Learning Management System training. The entity's employee failed to consider that an individual employee may have authorization to enter one PSP but not the other. Therefore, the entity's employee erroneously applied internal procedures because the employee did not believe certain procedures were applicable in this instance. The result was that the noncompliance allowed 18 unauthorized individuals to have access to 17 Physical Access Control System Cyber Assets within the merged cage. On March 31, 2017, the entity discovered the noncompliance while conducting an extent-of-condition review relating to another noncompliance.</p> <p>The root cause of this noncompliance was the employee's erroneous interpretation of internal CIP procedures resulting from insufficient training and ineffective controls.</p> <p>This noncompliance involves the management practices of implementation and workforce management. Implementation management is involved because the entity failed to comply with CIP-004-6 R4 as a result of their incorrect implementation of changes to multiple PSPs. Workforce management is involved because the employee was not properly trained on how to interpret the entity's policy and procedure regarding PSP access changes.</p> <p>The noncompliance began on January 5, 2017, the date the entity made changes to the layout of two PSPs, and ended on April 13, 2017, the date the entity corrected the relevant access authorizations.</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 instance of noncompliance is the opportunity for unauthorized personnel at the entity to access Bulk Electric System (BES) Cyber Systems and their associated Electronic Access Control and Monitoring and Physical Access Control Systems which could result in harm to the integrity of the BES Cyber Systems and the reliability of the BPS as a result of intentional compromise or misuse. The risk is minimized because all card holders with access to either PSP were NERC trained employees with valid Personal Risk Assessments. Further minimizing the risk, the facility is manned by security officers 24 hours per day, 7 days per week. Finally, the duration was limited to just 13 weeks and access was restricted to the same personnel that were originally using card readers. Thus, the risk posed to the Bulk-Power System was minimal. 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) sent email communication to all Area Owners reminding them not to make changes to a PSP without following the Corporate Security's change control process; 2) created new PSP in the access control system and obtained authorizations; 3) completed PSP inspection; 4) created a Configuration Item for changes to a PSP; 5) created a Job aid which will direct individuals to use the Configuration Item and posted in the data center PSPs; and 6) trained impacted personnel on the [REDACTED]. <p>ReliabilityFirst 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
RFC2017017412	CIP-006-6	R1	[REDACTED]	[REDACTED]	12/8/2016	12/8/2016	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 April 11, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-006-6 R1.</p> <p>On December 8, 2016, just after 12:30 P.M., the entity was notified via a Physical Access Control System alarm that there was an unsecured door to a Physical Security Perimeter (PSP) at the [REDACTED] within a corporate office building. The unsecured door occurred when an employee working in the PSP left the PSP through the third door and an alarm was generated because that door would not remain latched. This unsecured door allowed access to a Medium Impact Bulk Electric System (BES) Cyber system without need for a cardkey at the access control device. The lead security officer was deployed to look at the door causing the alarms and confirmed that the door would not stay closed. The lead security officer then returned to the [REDACTED] with two authorized employees alone in the PSP. The two employees soon finished their work and left. There was no human observation of the unsecured door.</p> <p>The [REDACTED] then deployed the Lead Technician to see if the door issue had been addressed. The Lead Technician arrived 15 minutes after the two employees vacated the PSP. The Lead Technician informed the [REDACTED] that he could not fix the door. The Lead Technician then left the PSP area at 1:32 P.M., leaving the door unsecured for an additional 65 minutes.</p> <p>At 2:36 P.M., two more employees arrived at the door and the programming issue was corrected soon thereafter. The door was programmed incorrectly in December 2014, prior to commissioning and the cage was still empty. The PSP to which this door provided access was not brought into scope until CIP-006-6 V5, beginning July 1, 2016. Finally, the entity Technical Security determined that the door was not unlocked manually by anyone who had the ability to do so. On the day of December 8, 2016, the door was unsecured and unobserved for approximately 80 minutes.</p> <p>The root cause of this noncompliance was that the entity's staff overlooked programming of the door which resulted in the error in programming; as well as numerous procedural and training deficiencies which resulted in the entity's failure to observe the door continuously while it was not secured.</p> <p>This noncompliance involves the management practices of workforce management and validation. Workforce management is implicated because the Lead Technician was not properly trained to remain at the unsecured door until it was either fixed or another authorized individual arrived to observe the door. Validation management is involved because the door was improperly programmed and validation of the program would have uncovered the programming issues.</p> <p>The noncompliance began on December 8, 2016, the date the door was opened without the capacity for lockout. The noncompliance ended on later on December 8, 2016, when the entity fixed the programming 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 based on the following factors. The risk posed by this noncompliance is the opportunity for unauthorized physical access to Cyber Assets or Cyber System(s) which could result in harm to the integrity of the BES Cyber Systems or the reliability of the BPS as a consequence of intentional compromise or misuse. The risk is minimized because the PSP was within a limited-access controlled area within an access controlled facility. Further minimizing the risk, while the PSP itself was unmanned, the PSP is within a controlled access facility which is manned by security guards 24 hours a day, 7 days a week. Finally, the duration of the noncompliance, approximately 80 minutes, limits the risk. Thus, the risk posed to the Bulk-Power System was minimal. 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) corrected the programming issue the same day the PSP door became unsecured; 2) reviewed and revised Corporate Security CIP-006 procedure to prevent a recurrence; 3) sent communication to the [REDACTED] and Technical Security regarding the updated CIP-006 procedure; and 4) conducted training with the [REDACTED] and Technical Security. <p>ReliabilityFirst 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
RFC2017018256	CIP-007-6	R2	[REDACTED]	[REDACTED]	1/17/2017	1/19/2017	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 22, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-007-6 R2. (This noncompliance was also resolved in the SERC Region.)</p> <p>On January 19, 2017, the entity discovered that three security patches were evaluated for installation 37 calendar days after being released from their monitored source, exceeding the patch deadline in CIP-007-6 R2 by two days. The patches which were not assessed in time included three patches for eight [REDACTED] servers classified as Electronic Access Control or Monitoring Systems (EACMS) supporting eight Bulk Electric System (BES) Cyber Systems. The entity's personnel overlooked the assessment during a period of heavy workload.</p> <p>The root cause of this noncompliance was inadequate internal workforce controls. High workloads and planned absences were managed ineffectively resulting in the entities being unable to complete the patch evaluation in time.</p> <p>This noncompliance involves the management practice of workforce management. Workforce management is implicated because the entity's employees were overburdened with work as a result of poor management practices which included granting planned absences during elevated workflow periods, thereby causing human performance errors.</p> <p>The noncompliance began on January 17, 2017, the date the entity was required to comply with CIP-007-6 R2. The noncompliance ended January 19, 2017, when the entity evaluated the patches for applicability.</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 failure to evaluate patches in a timely manner can expose BES Cyber Systems to cyber security vulnerabilities such as the introduction of malicious code or infiltration of a bad actor into BES Cyber Systems. The risk is minimized because the delay only impacted the assessment and the patches themselves were installed in a timely manner in accordance with CIP-007-6-R2.3. Specifically, CIP-007-6 R2 provides 35 days for patch assessment and an additional 35 days for implementation for a total of 70 days; here it took only 44 days to complete both steps. Further minimizing the risk, the BES Cyber Assets impacted, resided within a Physical Security Perimeter where the assets received all applicable logical and physical controls. Finally, this noncompliance only impacted three security patches specific to EACMS. Thus, the risk posed to the Bulk-Power System was minimal. 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) evaluated missed security patches for applicability; 2) added CIP-007-6 R2.2 task to the Executive Dashboard; 3) addressed human performance; 4) implemented additional controls around [REDACTED] patching to ensure patches are assessed and implemented; and 5) conducted training to ensure patches are assessed and implemented. <p>ReliabilityFirst 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
RFC2019021106	CIP-006-6	R2	[REDACTED]	[REDACTED]	November 30, 2018	April 29, 2019	Self-Report	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 February 15, 2019, April 30, 2019, and June 28, 2019 the entity submitted Self-Reports stating that, [REDACTED] it was in noncompliance with CIP-006-6 R2. The entity identified four issues relating to continuous escorting of visitors inside a Physical Security Perimeter (PSP).</p> <p>In the first instance, on November 30, 2018, an entity employee (Employee 1) who had authorized unescorted access to the [REDACTED] Physical Security Perimeter ([REDACTED] PSP), escorted another entity employee (Employee 2) who did not have authorized unescorted access into the [REDACTED] PSP in order to use the restroom. After entering the [REDACTED] PSP together at 07:57, Employee 1 instructed Employee 2 to call him when he needed to leave the [REDACTED] PSP and return to his work area. Employee 1 then exited the [REDACTED] PSP leaving Employee 2 unescorted within the [REDACTED] PSP. At approximately 08:08, Employee 2 called Employee 1 and asked him to open the [REDACTED] PSP door. Employee 2 exited the [REDACTED] PSP after 11 minutes of being unescorted.</p> <p>The root cause of this first instance was ineffective communication and ineffective training as both employees were mistakenly told by their supervisor that they each had authorized unescorted access to the [REDACTED] PSP. Neither the supervisor nor the employees involved confirmed that assumption, and only Employee 1 actually had been authorized for unescorted access into the [REDACTED] PSP. When Employee 2 tried to access the [REDACTED] PSP using his own credentials, the secure door would not open because he had not been granted unescorted access. The employees involved assumed this was a system error and Employee 1 provided access to the [REDACTED] PSP for Employee 2 to use the restroom. Based on the assumption that Employee 2 was authorized to be in the [REDACTED] PSP, Employee 1 left the POC PSP with Employee 2 being unescorted.</p> <p>This first instance involves the management practices of workforce management and verification as the employees were ineffectively trained on what to do when a secure door would not open and they did not verify that they each had authorized unescorted access to the [REDACTED] PSP.</p> <p>This first instance started on November 30, 2018, when Employee 1 left Employee 2 unescorted inside the [REDACTED] PSP and ended 11 minutes later on November 30, 2018 when Employee 2 left the [REDACTED] PSP.</p> <p>In the second instance, on December 6, 2018, an entity employee (Escort) logged a visitor (Visitor) with the Security Office to enter the [REDACTED] PSP ([REDACTED] PSP) at 11:11.</p> <p>On the same day, an entity security officer who was reviewing exit door procedures discovered that the Escort had left the [REDACTED] PSP with the Visitor still inside. More specifically, the security officer reviewed exit door video and saw that a few minutes prior to the arrival of another visitor, the Escort had left the Visitor unescorted inside the [REDACTED] PSP while he retrieved a chair from outside of the secure area. The exit door video shows that the Escort left the Visitor unescorted in the [REDACTED] PSP for approximately 17 seconds.</p> <p>The second instance involves the management practice of workforce management and the root cause was ineffective training as the Escort momentarily forgot to continuously escort the Visitor while he left the secure area to get a chair. (The Escort was fully aware of the Visitor Control Program and had properly followed the procedure while escorting the Visitor into the [REDACTED] PSP and later when exiting the [REDACTED] PSP with the Visitor while retrieving another Visitor.)</p> <p>This second instance started on December 6, 2018, when the Escort left the Visitor unescorted inside the PSP and ended 17 seconds later on December 6, 2018 when the Escort rejoined the Visitor inside the [REDACTED] PSP.</p> <p>In the third instance, on March 25, 2019, the entity did not continuously escort two visitors inside of the entryway of a PSP for approximately 30 seconds. The two visitors were logged with entity security as visitors to the PSP by an entity escort (Escort 1) and were in the process of being transferred to a new escort (Escort 2).</p> <p>During the transfer of escorting privileges, Escort 1 met Escort 2 and the two visitors at the entrance to the PSP. Escort 2 took the visitors into the PSP while Escort 1 proceeded to the security office outside of the PSP in order to communicate the transfer of visitor escort responsibilities. However, instead of waiting for Escort 1 to enter the PSP and hand-off the escort badge to Escort 2, Escort 2 exited the PSP to retrieve the escort badge from Escort 1 thus leaving the visitors unescorted for approximately 30 seconds before reentering with the escort badge.</p> <p>The third instance involves the management practice of workforce management and the root cause was ineffective training as Escort 2 momentarily failed to continuously escort the visitors while he left to get the escort badge.</p> <p>This third instance started on March 25, 2019, when Escort 2 left the visitors unescorted inside the PSP and ended approximately 30 seconds later on March 25, 2019, when Escort 2 rejoined the visitors inside the PSP with the escort badge.</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
RFC2019021106	CIP-006-6	R2	[REDACTED]	[REDACTED]	November 30, 2018	April 29, 2019	Self-Report	Completed
			<p>In the fourth instance, on April 29, 2019, an entity employee (Escort) properly logged two visitors (Visitor 1 and Visitor 2) with entity Security to access a PSP. The two visitors were onsite with the Escort to conduct testing and an inspection of the fire alarm system for the facility. As the Escort and the two visitors were relocating from one test location to another, the Escort proceeded through an interior secured door thinking both visitors were following. The Escort then recognized that only Visitor 1 had come through the door before it closed and Visitor 2 remained on the other side of the door working on the fire panel and not visible to the Escort.</p> <p>The Escort and Visitor 1 then returned to the original location where Visitor 2 was still located, along with another entity employee that had just arrived. This second entity employee immediately recognized the situation and began to continuously escort Visitor 2 until the Escort returned to that location. As a result, Visitor 2 was not continuously escorted within a PSP for approximately 20 seconds, from the time the door closed until the other entity employee arrived on the scene.</p> <p>The fourth noncompliance involves the management practices of workforce management and verification. The root cause was ineffective training as the Escort momentarily forgot to ensure that he continuously escorted the two visitors at all times when within a PSP. The Escort did not verify that both Visitors had followed him through the interior secured door.</p> <p>This fourth instance started on April 29, 2019, when the Escort left Visitor 2 unescorted inside the PSP and ended approximately 20 seconds later on April 29, 2019, when the other entity employee arrived and began escorting Visitor 2 until the Escort returned to the location where Visitor 2 was working on the fire panel.</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 both instances is permitting unauthorized individuals to access Bulk Electric System (BES) Cyber Systems without supervision. The risk is minimized because in the first instance, Employee 2 had a current background check and up to date annual CIP training and he remains an entity employee in good standing. In the second instance, the entity had implemented internal controls within the [REDACTED] PSP to prevent unauthorized access to BES Cyber Assets. [REDACTED] The second instance also had a short duration of just 17 seconds. In the third instance, the visitors were unescorted for only approximately 30 seconds inside the PSP. Both remained in the PSP entry hallway on the inside of the PSP glass door while not being escorted. In the fourth instance, Visitor 2 was only left unescorted for approximately 20 seconds inside the PSP and was found standing where he was left when the door closed. Therefore, he did not have the opportunity to access any CIP Cyber Assets because the assets are not located within close proximity to the fire panel. 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. Although the current noncompliance involves conduct that is arguably similar to the previous noncompliances, 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 noncompliances. Additionally, the instant noncompliance does not indicate a systemic or programmatic issue.</p>					
Mitigation			<p>To mitigate this noncompliance (first and second instance), the entity:</p> <ol style="list-style-type: none"> 1) retrained and disciplined Employee 1 and Employee 2; 2) administered retraining on entering/exiting and escorting to the entire group of [REDACTED] supervisors and employees from the impacted work location; 3) coached and disciplined the escort; 4) posted a new sign on the interior side of the [REDACTED] Physical Security Perimeter door used for visitor access to remind escorts that anytime they exit the secure area their visitor(s) must exit with them; and 5) provided retraining on entering/exiting and escorting to the [REDACTED] supervisor and his direct reports including the escort. <p>To mitigate this noncompliance (third instance), the entity:</p> <ol style="list-style-type: none"> 1) terminated Escort 1 (an entity contractor) and all access was revoked. (The termination was not directly related to this instance.); 2) immediately retrained Escort 2 (an entity employee) on entity practices concerning escorting in restricted areas (PSPs), and received discipline from his supervisor; 3) posted a visible Security Officer at the primary entrance to this PSP during normal business hours for this location (7:30 am – 3:30 pm). This Security Officer will serve as an additional resource for providing instruction for proper ingress and egress of the PSP. <p>To mitigate this noncompliance (fourth instance), the entity:</p> <ol style="list-style-type: none"> 1) counseled and coached the Escort involved as to the proper procedure for maintaining continuous visual and auditory contact with visitors when escorting; 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021106	CIP-006-6	R2	[REDACTED]	[REDACTED]	November 30, 2018	April 29, 2019	Self-Report	Completed
			<p>2) made physical changes to the access point to create a designated visitor access door [REDACTED]. The entity now requires all visitors to this PSP to be escorted through the new visitor access door which will improve visitor management;</p> <p>3) conducted training with entity personnel with authorized unescorted access to this PSP, concerning the proper escorting practices;</p> <p>4) prepared a computer based training program to provide instruction on proper escorting practices that will be required for new personnel being granted unescorted access to this PSP and for periodic training to be completed at least every 15 calendar months by all personnel with authorized unescorted access to any PSPs. The entity has prepared a new [REDACTED] "Guide" that will be used by Security Officers to provide escorts and visitors instructions for proper escorting immediately prior to them entering any entity PSP;</p> <p>5) prepared a new [REDACTED] " form for the particular PSP involved in this instance [REDACTED] that will be signed by escorts and visitors; and</p> <p>6) implemented for all other PSPs, a new process that will require documented acknowledgment of escorts and visitors after receiving instructions for proper escorting immediately prior to them entering the PSP.</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
RFC2019021107	CIP-010-2	R1	[REDACTED]	[REDACTED]	11/21/2018	11/27/2018	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 15, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>On November 21, 2018, the entity installed a computer workstation (Cyber Asset) on the [REDACTED] production environment at the entity [REDACTED] following approval of a configuration management expedited change request. [REDACTED]. Although the expedited change request was properly reviewed and processed per the entity's expedited change request practices, it did not accurately reflect the status of the Cyber Asset involved.</p> <p>The expedited change request indicated a location move for an existing Bulk Electric System (BES) Cyber Asset, which should have been preconfigured with an established and approved baseline configuration for the production environment. The entity employee that entered the change request incorrectly assumed that the workstation he was connecting was a BES Cyber Asset without performing any verification. As a result, a non-BES Cyber Asset workstation from within the Physical Security Perimeter (PSP) was connected to the production environment.</p> <p>The workstation was not preconfigured with an established and approved baseline configuration. After connecting the workstation, the employee recognized that it did not have an operating system and made additional changes to the Cyber Asset in order for it to function as planned and established the approved baseline configuration for that BES Cyber Asset type. These additional changes were not identified as part of the planned work included in the expedited change request, the original change request was not updated, and an additional change request was not submitted.</p> <p>The entity discovered this noncompliance [REDACTED], during a regularly scheduled [REDACTED] meeting w [REDACTED] [REDACTED]. After discovery and out of an abundance of caution, the entity removed the Cyber Asset from the [REDACTED] Electronic Security Perimeter (ESP) and entity cyber security staff performed a vulnerability analysis of the Cyber Asset, as well as an analysis of malware scans, intrusion detection alerts, network firewall logs, security logs and local firewall logs. This analysis revealed no anomalies.</p> <p>This noncompliance involves the management practices of workforce management through ineffective training, work management, and verification. The entity employee who entered the expedited change request incorrectly indicated on the request that the change involved moving an existing BES Cyber Asset from the [REDACTED] production environment to the [REDACTED] production environment. Ineffective training that led the employee to make this mistake is a root cause of this noncompliance. Another contributing cause of this noncompliance is the limitations of the entity expedited change request process, because such requests do not undergo the same level of scrutiny and review as a normal change request. As a result, details of the change were not thoroughly vetted by a larger group of entity technical resources as would have occurred for a normal change. As part of a normal change request, the [REDACTED] would have reviewed the request in more detail prior to granting approval to place the asset in production.</p> <p>This noncompliance started on November 21, 2018, when a non-BES Cyber Asset workstation from within the Physical Security Perimeter (PSP) was incorrectly connected to the production environment without a correct and updated change request [REDACTED].</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 making undocumented and unapproved changes when installing a Cyber Asset, which could introduce vulnerabilities into the system. The risk is minimized because the entity's configuration monitoring system is deployed to other Cyber Assets [REDACTED] in the [REDACTED] network, and the system did not detect or alert to any unexpected new software (or malware) installed, or any configuration changes to these systems because the change request to install a Cyber Asset on the [REDACTED] environment at the [REDACTED] had been approved via an expedited change request. (The entity also monitors the configuration of network devices as well as collects security log files, and no configuration changes or security events were detected due to this instance.) The [REDACTED] production ESP is segmented via firewalls from the [REDACTED] ESP. During the noncompliance, the [REDACTED] on the [REDACTED] production network did not detect or alert on any vulnerabilities or communication attempts into or out of the ESP due to this instance. [REDACTED]. The noncompliance only lasted six days. Lastly, the entity conducted a vulnerability analysis on the Cyber Asset involved after discovering this noncompliance and no anomalies were detected. 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) removed the Cyber Asset involved from the entity [REDACTED] production network and conducted a vulnerability analysis of the Cyber Asset. No anomalies were detected; 2) gave a verbal and written reprimand to the [REDACTED] involved for not following established entity procedures; 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021107	CIP-010-2	R1	[REDACTED]	[REDACTED]	11/21/2018	11/27/2018	Self-Report	Completed
			3) provided retraining to the [REDACTED] involved, as well as other entity personnel responsible for making similar infrastructure changes to the entity production environment, on the procedures for making such changes and requesting changes via the normal and expedited change request process; 4) revised the entity change request process to include additional internal controls to ensure that expedited change requests are accurately submitted, reviewed and approved prior to implementation of the change: (i) expedited change requests to be submitted by entity Subject Matter Experts must be approved based on a valid need for the expedited change by their Manager or above; (ii) expedited change requests will undergo a pre-evaluation to ensure accuracy, completeness and operational appropriateness (similar to a "normal" change request), and then be reviewed and approved by an [REDACTED] conference call scheduled as soon as practical after the request is submitted; and 5) provided training on the revised procedure to entity personnel responsible for submitting expedited change requests.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019401	CIP-004-6	R1	[REDACTED]	[REDACTED]	8/30/2017	8/31/2017	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 March 7, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-004-6 R1. (This noncompliance was also resolved in the [REDACTED] Region.)</p> <p>On August 30, 2017, the entity's [REDACTED] group inadvertently provided a new contractor, who was not authorized or trained, with electronic access to NERC data. On August 31, 2017, [REDACTED] internal control process identified the noncompliance. [REDACTED] then notified [REDACTED] which removed the access on August 31, 2017.</p> <p>As background, the [REDACTED] security analyst had mistakenly added the new Database Administrator (DBA) contractor to a [REDACTED] group for which access had not been requested or approved. The requests and approval are submitted and completed via a workflow tool that does not communicate with the [REDACTED] group itself. The [REDACTED] security analyst must search for the requested access group in [REDACTED] where authorization is granted, but the large number of [REDACTED] groups and similar nomenclature make it difficult to confirm that the right [REDACTED] group is selected.</p> <p>The root cause of this noncompliance was that the security analyst completing the work inadvertently selected the wrong [REDACTED] group due to the [REDACTED] group naming similarities discussed above, and an insufficient process that allowed the error to occur without detection.</p> <p>This noncompliance involves the management practices of information management and verification. Information management is involved because the entity's [REDACTED] failed to properly protect information by providing a contractor with access to a Physical Access Control Systems Database (PACS) which supported facilities containing High and Medium Impact BCS. Verification management is involved because the entity's process for verifying and adding members to the [REDACTED] group was the central cause of this noncompliance.</p> <p>The noncompliance began on August 30, 2017, the date the entity inadvertently provided a new not authorized and untrained contractor with electronic access to NERC data, and ended on August 31, 2017, the date the entity removed the DBA 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 instance of noncompliance is the provision of electronic access to an unauthorized and untrained individual, potentially resulting in an unintentional or malicious action with operational impacts. This risk is minimized because the entity discovered and remediated the issue within only 24 hours, demonstrating strong internal controls. Additionally, the contractor had a current background check and had recently completed NERC CIP training. Thus, the risk posed to the Bulk-Power System was minimal. No harm is known to have occurred. ReliabilityFirst also notes that the entity's review of the end user's data indicates that the contractor did not access NERC data during the period for which authorized access was granted.</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) removed unauthorized access from contractor's account; 2) added an enhancement to the workflow tool to initiate a pop-up alert when completing a NERC request. To continue with the process, the security analyst requests a peer review and the peer reviewer notes their review in [REDACTED]; and 3) instituted a process improvement to prevent vaulting certain user accounts until [REDACTED] notifies [REDACTED] that the Compliance Process is complete. <p>ReliabilityFirst 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
RFC2017018258	CIP-004-6	R4	[REDACTED]	[REDACTED]	1/5/2017	4/13/2017	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 August 22, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-004-6 R4. (This noncompliance was also resolved in the SERC Region.)</p> <p>On January 5, 2017, an [REDACTED] (an employee) coordinated multiple changes to the entity's Physical Security Perimeters (PSP). Specifically, the entity's employee had interior fencing removed which had separated the [REDACTED] and the [REDACTED] both PSPs from each other as well as separating the [REDACTED], a non-NERC asset. The removal of the fencing shifted the space into one, larger, PSP. The reconfiguration also included the removal of the [REDACTED], leaving only the two PSP access doors remaining. The result of the change was that any individual who was authorized to enter one of the PSPs was able to access both PSPs. The entity's employee incorrectly believed that because both were NERC PSPs every party who had access to either PSP was covered because they had completed Learning Management System training. The entity's employee failed to consider that an individual employee may have authorization to enter one PSP but not the other. Therefore, the entity's employee erroneously applied internal procedures because the employee did not believe certain procedures were applicable in this instance. The result was that the noncompliance allowed 18 unauthorized individuals to have access to 17 Physical Access Control System Cyber Assets within the merged cage. On March 31, 2017, the entity discovered the noncompliance while conducting an extent-of-condition review relating to another noncompliance.</p> <p>The root cause of this noncompliance was the employee's erroneous interpretation of internal CIP procedures resulting from insufficient training and ineffective controls.</p> <p>This noncompliance involves the management practices of implementation and workforce management. Implementation management is involved because the entity failed to comply with CIP-004-6 R4 as a result of their incorrect implementation of changes to multiple PSPs. Workforce management is involved because the employee was not properly trained on how to interpret the entity's policy and procedure regarding PSP access changes.</p> <p>The noncompliance began on January 5, 2017, the date the entity made changes to the layout of two PSPs, and ended on April 13, 2017, the date the entity corrected the relevant access authorizations.</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 instance of noncompliance is the opportunity for unauthorized personnel at the entity to access Bulk Electric System (BES) Cyber Systems and their associated Electronic Access Control and Monitoring and Physical Access Control Systems which could result in harm to the integrity of the BES Cyber Systems and the reliability of the BPS as a result of intentional compromise or misuse. The risk is minimized because all card holders with access to either PSP were NERC trained employees with valid Personal Risk Assessments. Further minimizing the risk, the facility is manned by security officers 24 hours per day, 7 days per week. Finally, the duration was limited to just 13 weeks and access was restricted to the same personnel that were originally using card readers. Thus, the risk posed to the Bulk-Power System was minimal. 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) sent email communication to all Area Owners reminding them not to make changes to a PSP without following the Corporate Security's change control process; 2) created new PSP in the access control system and obtained authorizations; 3) completed PSP inspection; 4) created a Configuration Item for changes to a PSP; 5) created a Job aid which will direct individuals to use the Configuration Item and posted in the data center PSPs; and 6) trained impacted personnel on the [REDACTED]. <p>ReliabilityFirst 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
RFC2017017414	CIP-006-6	R1	[REDACTED]	[REDACTED]	12/8/2016	12/8/2016	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 April 11, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-006-6 R1.</p> <p>On December 8, 2016, just after 12:30 P.M., the entity was notified via a Physical Access Control System alarm that there was an unsecured door to a Physical Security Perimeter (PSP) at the [REDACTED] within a corporate office building. The unsecured door occurred when an employee working in the PSP left the PSP through the third door and an alarm was generated because that door would not remain latched. This unsecured door allowed access to a Medium Impact Bulk Electric System (BES) Cyber system without need for a cardkey at the access control device. The lead security officer was deployed to look at the door causing the alarms and confirmed that the door would not stay closed. The lead security officer then returned to the [REDACTED] with two authorized employees alone in the PSP. The two employees soon finished their work and left. There was no human observation of the unsecured door.</p> <p>The [REDACTED] then deployed the Lead Technician to see if the door issue had been addressed. The Lead Technician arrived 15 minutes after the two employees vacated the PSP. The Lead Technician informed the [REDACTED] that he could not fix the door. The Lead Technician then left the PSP area at 1:32 P.M., leaving the door unsecured for an additional 65 minutes.</p> <p>At 2:36 P.M., two more employees arrived at the door and the programming issue was corrected soon thereafter. The door was programmed incorrectly in December 2014, prior to commissioning and the cage was still empty. The PSP to which this door provided access was not brought into scope until CIP-006-6 V5, beginning July 1, 2016. Finally, the entity Technical Security determined that the door was not unlocked manually by anyone who had the ability to do so. On the day of December 8, 2016, the door was unsecured and unobserved for approximately 80 minutes.</p> <p>The root cause of this noncompliance was that the entity's staff overlooked programming of the door which resulted in the error in programming; as well as numerous procedural and training deficiencies which resulted in the entity's failure to observe the door continuously while it was not secured.</p> <p>This noncompliance involves the management practices of workforce management and validation. Workforce management is implicated because the Lead Technician was not properly trained to remain at the unsecured door until it was either fixed or another authorized individual arrived to observe the door. Validation management is involved because the door was improperly programmed and validation of the program would have uncovered the programming issues.</p> <p>The noncompliance began on December 8, 2016, the date the door was opened without the capacity for lockout. The noncompliance ended on later on December 8, 2016, when the entity fixed the programming 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 based on the following factors. The risk posed by this noncompliance is the opportunity for unauthorized physical access to Cyber Assets or Cyber System(s) which could result in harm to the integrity of the BES Cyber Systems or the reliability of the BPS as a consequence of intentional compromise or misuse. The risk is minimized because the PSP was within a limited-access controlled area within an access controlled facility. Further minimizing the risk, while the PSP itself was unmanned, the PSP is within a controlled access facility which is manned by security guards 24 hours a day, 7 days a week. Finally, the duration of the noncompliance, approximately 80 minutes, limits the risk. Thus, the risk posed to the Bulk-Power System was minimal. 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) corrected the programming issue the same day the PSP door became unsecured; 2) reviewed and revised Corporate Security CIP-006 procedure to prevent a recurrence; 3) sent communication to the [REDACTED] and Technical Security regarding the updated CIP-006 procedure; and 4) conducted training with the [REDACTED] and Technical Security. <p>ReliabilityFirst 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
RFC2017018259	CIP-007-6	R2	[REDACTED]	[REDACTED]	1/17/2017	1/19/2017	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 22, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-007-6 R2. (This noncompliance was also resolved in the SERC Region.)</p> <p>On January 19, 2017, the entity discovered that three security patches were evaluated for installation 37 calendar days after being released from their monitored source, exceeding the patch deadline in CIP-007-6 R2 by two days. The patches which were not assessed in time included three patches for eight [REDACTED] servers classified as Electronic Access Control or Monitoring Systems (EACMS) supporting eight Bulk Electric System (BES) Cyber Systems. The entity's personnel overlooked the assessment during a period of heavy workload.</p> <p>The root cause of this noncompliance was inadequate internal workforce controls. High workloads and planned absences were managed ineffectively resulting in the entities being unable to complete the patch evaluation in time.</p> <p>This noncompliance involves the management practice of workforce management. Workforce management is implicated because the entity's employees were overburdened with work as a result of poor management practices which included granting planned absences during elevated workflow periods, thereby causing human performance errors.</p> <p>The noncompliance began on January 17, 2017, the date the entity was required to comply with CIP-007-6 R2. The noncompliance ended January 19, 2017, when the entity evaluated the patches for applicability.</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 failure to evaluate patches in a timely manner can expose BES Cyber Systems to cyber security vulnerabilities such as the introduction of malicious code or infiltration of a bad actor into BES Cyber Systems. The risk is minimized because the delay only impacted the assessment and the patches themselves were installed in a timely manner in accordance with CIP-007-6-R2.3. Specifically, CIP-007-6 R2 provides 35 days for patch assessment and an additional 35 days for implementation for a total of 70 days; here it took only 44 days to complete both steps. Further minimizing the risk, the BES Cyber Assets impacted, resided within a Physical Security Perimeter where the assets received all applicable logical and physical controls. Finally, this noncompliance only impacted three security patches specific to EACMS. Thus, the risk posed to the Bulk-Power System was minimal. 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) evaluated missed security patches for applicability; 2) added CIP-007-6 R2.2 task to the Executive Dashboard; 3) addressed human performance; 4) implemented additional controls around [REDACTED] patching to ensure patches are assessed and implemented; and 5) conducted training to ensure patches are assessed and implemented. <p>ReliabilityFirst 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
RFC2017018254	CIP-004-6	R4			1/5/2017	4/13/2017	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 August 21, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-004-6 R4. (This noncompliance was also resolved in the SERC Region.)</p> <p>On January 5, 2017, an [REDACTED] (an employee) coordinated multiple changes to the entity's Physical Security Perimeters (PSP). Specifically, the entity's employee had interior fencing removed which had separated the [REDACTED] and the [REDACTED] both PSPs from each other as well as separating the [REDACTED], a non-NERC asset. The removal of the fencing shifted the space into one, larger, PSP. The reconfiguration also included the removal of the [REDACTED], leaving only the two PSP access doors remaining. The result of the change was that any individual who was authorized to enter one of the PSPs was able to access both PSPs. The entity's employee incorrectly believed that because both were NERC PSPs every party who had access to either PSP was covered because they had completed Learning Management System training. The entity's employee failed to consider that an individual employee may have authorization to enter one PSP but not the other. Therefore, the entity's employee erroneously applied internal procedures because the employee did not believe certain procedures were applicable in this instance. The result was that the noncompliance allowed 18 unauthorized individuals to have access to 17 Physical Access Control System Cyber Assets within the merged cage. On March 31, 2017, the entity discovered the noncompliance while conducting an extent-of-condition review relating to another noncompliance.</p> <p>The root cause of this noncompliance was the employee's erroneous interpretation of internal CIP procedures resulting from insufficient training and ineffective controls.</p> <p>This noncompliance involves the management practices of implementation and workforce management. Implementation management is involved because the entity failed to comply with CIP-004-6 R4 as a result of their incorrect implementation of changes to multiple PSPs. Workforce management is involved because the employee was not properly trained on how to interpret the entity's policy and procedure regarding PSP access changes.</p> <p>The noncompliance began on January 5, 2017, the date the entity made changes to the layout of two PSPs, and ended on April 13, 2017, the date the entity corrected the relevant access authorizations.</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 instance of noncompliance is the opportunity for unauthorized personnel at the entity to access Bulk Electric System (BES) Cyber Systems and their associated Electronic Access Control and Monitoring and Physical Access Control Systems which could result in harm to the integrity of the BES Cyber Systems and the reliability of the BPS as a result of intentional compromise or misuse. The risk is minimized because all card holders with access to either PSP were NERC trained employees with valid Personal Risk Assessments. Further minimizing the risk, the facility is manned by security officers 24 hours per day, 7 days per week. Finally, the duration was limited to just 13 weeks and access was restricted to the same personnel that were originally using card readers. Thus, the risk posed to the Bulk-Power System was minimal. 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) sent email communication to all Area Owners reminding them not to make changes to a PSP without following the Corporate Security's change control process; 2) created new PSP in the access control system and obtained authorizations; 3) completed PSP inspection; 4) created a Configuration Item for changes to a PSP; 5) created a Job aid which will direct individuals to use the Configuration Item and posted in the data center PSPs; and 6) trained impacted personnel on the [REDACTED]. <p>ReliabilityFirst 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
RFC2017017417	CIP-006-6	R1	[REDACTED]	[REDACTED]	12/8/2016	12/8/2016	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 April 11, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-006-6 R1.</p> <p>On December 8, 2016, just after 12:30 P.M., the entity was notified via a Physical Access Control System alarm that there was an unsecured door to a Physical Security Perimeter (PSP) at the [REDACTED] within a corporate office building. The unsecured door occurred when an employee working in the PSP left the PSP through the third door and an alarm was generated because that door would not remain latched. This unsecured door allowed access to a Medium Impact Bulk Electric System (BES) Cyber system without need for a cardkey at the access control device. The lead security officer was deployed to look at the door causing the alarms and confirmed that the door would not stay closed. The lead security officer then returned to the [REDACTED] with two authorized employees alone in the PSP. The two employees soon finished their work and left. There was no human observation of the unsecured door.</p> <p>The [REDACTED] then deployed the Lead Technician to see if the door issue had been addressed. The Lead Technician arrived 15 minutes after the two employees vacated the PSP. The Lead Technician informed the [REDACTED] that he could not fix the door. The Lead Technician then left the PSP area at 1:32 P.M., leaving the door unsecured for an additional 65 minutes.</p> <p>At 2:36 P.M., two more employees arrived at the door and the programming issue was corrected soon thereafter. The door was programmed incorrectly in December 2014, prior to commissioning and the cage was still empty. The PSP to which this door provided access was not brought into scope until CIP-006-6 V5, beginning July 1, 2016. Finally, the entity Technical Security determined that the door was not unlocked manually by anyone who had the ability to do so. On the day of December 8, 2016, the door was unsecured and unobserved for approximately 80 minutes.</p> <p>The root cause of this noncompliance was that the entity's staff overlooked programming of the door which resulted in the error in programming; as well as numerous procedural and training deficiencies which resulted in the entity's failure to observe the door continuously while it was not secured.</p> <p>This noncompliance involves the management practices of workforce management and validation. Workforce management is implicated because the Lead Technician was not properly trained to remain at the unsecured door until it was either fixed or another authorized individual arrived to observe the door. Validation management is involved because the door was improperly programmed and validation of the program would have uncovered the programming issues.</p> <p>The noncompliance began on December 8, 2016, the date the door was opened without the capacity for lockout. The noncompliance ended on later on December 8, 2016, when the entity fixed the programming 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 based on the following factors. The risk posed by this noncompliance is the opportunity for unauthorized physical access to Cyber Assets or Cyber System(s) which could result in harm to the integrity of the BES Cyber Systems or the reliability of the BPS as a consequence of intentional compromise or misuse. The risk is minimized because the PSP was within a limited-access controlled area within an access controlled facility. Further minimizing the risk, while the PSP itself was unmanned, the PSP is within a controlled access facility which is manned by security guards 24 hours a day, 7 days a week. Finally, the duration of the noncompliance, approximately 80 minutes, limits the risk. Thus, the risk posed to the Bulk-Power System was minimal. 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) corrected the programming issue the same day the PSP door became unsecured; 2) reviewed and revised Corporate Security CIP-006 procedure to prevent a recurrence; 3) sent communication to the [REDACTED] and Technical Security regarding the updated CIP-006 procedure; and 4) conducted training with the [REDACTED] and Technical Security. <p>ReliabilityFirst 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
RFC2017018255	CIP-007-6	R2	[REDACTED]	[REDACTED]	1/17/2017	1/19/2017	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 21, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-007-6 R2. (This noncompliance was also resolved in the SERC Region.)</p> <p>On January 19, 2017, the entity discovered that three security patches were evaluated for installation 37 calendar days after being released from their monitored source, exceeding the patch deadline in CIP-007-6 R2 by two days. The patches which were not assessed in time included three patches for eight [REDACTED] servers classified as Electronic Access Control or Monitoring Systems (EACMS) supporting eight Bulk Electric System (BES) Cyber Systems. The entity's personnel overlooked the assessment during a period of heavy workload.</p> <p>The root cause of this noncompliance was inadequate internal workforce controls. High workloads and planned absences were managed ineffectively resulting in the entities being unable to complete the patch evaluation in time.</p> <p>This noncompliance involves the management practice of workforce management. Workforce management is implicated because the entity's employees were overburdened with work as a result of poor management practices which included granting planned absences during elevated workflow periods, thereby causing human performance errors.</p> <p>The noncompliance began on January 17, 2017, the date the entity was required to comply with CIP-007-6 R2. The noncompliance ended January 19, 2017, when the entity evaluated the patches for applicability.</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 failure to evaluate patches in a timely manner can expose BES Cyber Systems to cyber security vulnerabilities such as the introduction of malicious code or infiltration of a bad actor into BES Cyber Systems. The risk is minimized because the delay only impacted the assessment and the patches themselves were installed in a timely manner in accordance with CIP-007-6-R2.3. Specifically, CIP-007-6 R2 provides 35 days for patch assessment and an additional 35 days for implementation for a total of 70 days; here it took only 44 days to complete both steps. Further minimizing the risk, the BES Cyber Assets impacted, resided within a Physical Security Perimeter where the assets received all applicable logical and physical controls. Finally, this noncompliance only impacted three security patches specific to EACMS. Thus, the risk posed to the Bulk-Power System was minimal. 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) evaluated missed security patches for applicability; 2) added CIP-007-6 R2.2 task to the Executive Dashboard; 3) addressed human performance; 4) implemented additional controls around [REDACTED] patching to ensure patches are assessed and implemented; and 5) conducted training to ensure patches are assessed and implemented. <p>ReliabilityFirst 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
RFC2019021893	CIP-010-2	R1; Part 1.2	[REDACTED]	[REDACTED]	12/14/2017	12/21/2017	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 March 31, 2018, the entity submitted a self-log stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.2.</p>							
	<p>On December 21, 2017, the entity discovered a change to the authorized baseline for 39 [REDACTED] (Electronic Access Control or Monitoring System (EACMS)) as a part of the monthly baseline monitoring process. [REDACTED] planned an upgrade [REDACTED] and the entity performed Cyber Security Testing (CST) in the development environment on December 7, 2017. During the upgrade in the development environment, a [REDACTED] technician identified an issue, i.e. unneeded opened ports on the device. The [REDACTED] technician ran a script in development to close the ports; however, the technician did not communicate the need for the script to the entity and thoroughly within [REDACTED] upgraded the devices in the production environment on December 14, 2017. This upgrade did not include the script resulting in unneeded ports being left open. [REDACTED] provided a post upgrade report to the entity on December 15, 2017, which showed the opened ports; however, the entity did not complete a full review report and did not identify the open ports.</p>							
	<p>This noncompliance involves the management practices of external interdependencies and verification as the [REDACTED] upgrade incorrectly left unneeded ports being open. The failure to verify that the upgrade included the necessary script to ensure unneeded ports were not left open is a root cause of this noncompliance.</p> <p>Other contributing causes included that [REDACTED] upgrade code contained an error that enabled a service that was not necessary. While [REDACTED] identified the code error, they did not properly communicate the issue internally and externally to ensure it was corrected. The entity [REDACTED] did not identify security concerns or unintended deviations from the baseline as [REDACTED] installed the upgrade and code fix in the development environment. The entity identified the enabled service and open port with the monthly baseline report rather than with the post upgrade report.</p> <p>This noncompliance began on December 14, 2017 when the entity first left the unneeded ports open, and ended on December 21, 2017, when the entity disabled the unneeded open ports.</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 leaving unneeded ports open provides an additional attack vector for a bad actor to attempt to access and compromise Bulk Electric System Cyber Assets (BCAs). The risk is minimized because the enabled service and open ports could not have been used to compromise the BCAs as there is no enabled network path from the EACMS to the BCAs. Additionally, the enabled service and open ports could not be used to compromise the EACMS unless the [REDACTED] network was already compromised and there is no indication this has occurred. If the EACMS was compromised, [REDACTED] would have alerted the entity. The EACMS have event and health monitoring and any loss of monitoring would be detected. The EACMS have a local firewall which prevents the communication with other devices on entity networks, including BCAs. No harm is known to have occurred.</p>							
<p>Mitigation</p>	<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) instructed [REDACTED] to run the script in production environment to disable the services and ports; 2) updated [REDACTED] job aid to perform a full review of post upgrade report for changes; 3) improved their process and communication on upgrades and baseline review by adding a second person to verify baselines are complete and accurate before sending to the entity; 4) implemented a bi-weekly technician meeting with the entity to discuss device management issues, enhancements and documentation to improve communication at the technician level of support; and 5) implemented a new [REDACTED] check that will identify unintended changes to ports, services, [REDACTED] and custom software during the testing processes as new software is developed. 							

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021894	CIP-010-2	R1; Part 1.1	[REDACTED]	[REDACTED]	7/1/2016	2/23/2018	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 March 31, 2018, the entity submitted a self-log stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.1.</p> <p>On December 18, 2017, the entity was performing a firmware upgrade on a relay (Bulk Electric System Cyber Asset (BCA)) at a substation and identified an enabled logical port. The entity consulted with Relay Engineering and then disabled the port by applying updated settings. Relay Engineering determined the port was enabled as a result of the setting applied during the entity's NERC CIP V5 preparations. [REDACTED] Relay Engineering intended the port to be disabled. Since the baseline for the BCA indicated the port was disabled and the port was enabled; the baseline was incorrect and not corrected within 30 calendar days.</p> <p>This noncompliance involves the management practices of asset and configuration management and verification as the entity incorrectly enabled the port as a result of an applied setting. The entity did not verify that the port was disabled. The root cause of this noncompliance was that the entity process for issuing settings does not include a review of ports and services for all types of setting changes. [REDACTED]</p> <p>This noncompliance began on July 1, 2016 when the entity was required to comply with CIP-010-2 R1.1, and ended on February 23, 2018, when the entity updated asset inventory with the correct BCA baseline.</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 leaving an unneeded port open because of an incorrect asset inventory list provides an additional attack vector for a bad actor to attempt to access and compromise BCAs. The risk is minimized because even though there was an unneeded enabled port, the BCA did not have [REDACTED]. The BCA received firmware updates, was located inside a Physical Security Perimeter and had account password controls in place. The enabled port could only be accessed by being physically present at the BCA. There were no unauthorized physical access attempts at the substation. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disabled the port. Evidence "as left" file in asset inventory database; 2) updated asset inventory with the correct BCA baseline; and 3) updated the procedure for issuing and finalizing settings to include baseline and port confirmation 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021895	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/1/2016	1/29/2018	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 March 31, 2018, the entity submitted a self-log stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>On November 30, 2017, the entity was performing a field review of all devices at a substation and discovered there were devices not accurately identified. The entity identified 8 devices [REDACTED] that were not identified as Protected Cyber Assets (PCAs) and did not have appropriate NERC CIP protections, e.g. patching, malicious code detection, logging, and alerting. These eight devices should have been identified as PCAs. The eight devices were physically protected and did not allow remote access and were not providing any reliability operating services, including visibility or control.</p> <p>[REDACTED]</p> <p>The eight PCAs were connected to a Bulk Electric System (BES) Cyber Asset (BCA), [REDACTED], which was connected to other BCAs. All BCAs were properly protected via the CIP Standards including account management, password management, patching, etc.</p> <p>This noncompliance involves the management practice of asset and configuration management as the entity did not accurately identify eight devices. The root cause of this noncompliance is the entity classified the Cyber Assets based on a future state but the anticipated change was not implemented prior to the NERC CIP V5 enforcement date. When the entity conducted the final reconciliation prior to the NERC CIP V5 enforcement date, they compared the [REDACTED] diagram to the system and the [REDACTED] diagram reflected the future state.</p> <p>This noncompliance began on July 1, 2016 when the entity was required to comply with CIP-010-2 R1, and ended on January 29, 2018, when the entity disconnected the 8 PCAs as they were not needed.</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 failing to identify assets that contain low impact BES Cyber Systems which can lead to the entity not properly securing those assets due to lack of awareness. The risk is minimized because the PCAs were not providing any reliability operating services, including visibility or control. The PCAs were physically protected and did not have [REDACTED]. The BCAs that the PCAs were connected to were protected via the CIP standards, including account management, password management, patching, etc. Lastly, there was no physical compromise to the substation Physical Security Perimeter. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disconnected the 8 PCAs as they were not needed; 2) reviewed the asset commissioning procedure with all stakeholders; 3) performed an extent of condition via a walk down at all [REDACTED] Substations; 4) implemented any corrective actions if required from the extent of condition; and 5) updated [REDACTED] with an attachment detailing how a walk down will be performed including controls to ensure completeness and accuracy. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021904	CIP-010-2	R1; Part 1.4	[REDACTED]	[REDACTED]	3/13/2018	7/13/2018	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 June 30, 2018, the entity submitted a self-log stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.4</p> <p>On April 2, 2018, IT [REDACTED] identified a change to the baseline for [REDACTED] Electronic Access Control or Monitoring System (EACMS), [REDACTED] On March 13, 2018, IT [REDACTED] coordinated with the [REDACTED] to implement a code upgrade for log collectors and inspector devices. As part of the upgrade on March 13, 2018, the [REDACTED] devices automatically updated a module without change management and [REDACTED] Testing [REDACTED] After further research, the update is designed to be automatic to ensure communications between devices.</p> <p>On May 29, 2018, IT [REDACTED] identified a change to the baseline on [REDACTED] EACMS, [REDACTED] On May 4, 2018, [REDACTED] inadvertently upgraded software on EACMS during a planned deployment of a software upgrade. The upgrade was done without change management, [REDACTED] and the baseline was not updated within the required 35 days.</p> <p>Both changes are required and will remain installed on the EACMS.</p> <p>This noncompliance involves the management practices of asset and configuration management and verification as a code upgrade resulted in baseline changes but the baselines were not timely updated with those changes. The root cause of this noncompliance is a lack of understanding that the code upgrade would require baseline changes.</p> <p>This noncompliance began on March 13, 2018 when the entity implemented the code upgrade without updating the baselines and ended on July 13, 2018, when the entity updated the missed baselines.</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 that future changes may be made based on outdated or incorrect information because the baselines were not updated. The risk is minimized because although the EACMS Cyber Assets were changed prior to approval by IT [REDACTED] review and approval, the change in both instances were tested by the [REDACTED] and ultimately accepted by IT [REDACTED] The change was required and done automatically by the [REDACTED] as the change was required to ensure the EACMS Cyber Assets functioned. The EACMS Cyber Asset functioned as expected. Lastly, the entity quickly identified and corrected this noncompliance. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) submitted an Emergency Change Request and performed [REDACTED]; 2) submitted Emergency Change Request, [REDACTED]; and 3) reviewed and revised the approach to coordinate and test changes performed by the [REDACTED] on EACMS 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
RFC2019021905	CIP-007-6	R4; Part 4.4	[REDACTED]	[REDACTED]	4/11/2018	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 June 30, 2018, the entity submitted a self-log stating that, [REDACTED] it was in noncompliance with CIP-007-6 R4.4.</p> <p>While completing the log review on April 12, 2018, IT [REDACTED] identified the log review passed the 15 day requirement. While the log review is required every 15 days, [REDACTED] The log review was completed on March 27, 2018 and again on April 12, 2018; therefore, missing the required completion date of April 11, 2018.</p> <p>This noncompliance involves the management practices of verification and work management as the entity did not verify that it had timely performed its 15 day log review. The root cause was the entity's process lacked an escalation and automatic alerting mechanism to ensure log reviews are completed within the 15 day requirement.</p> <p>This noncompliance began on April 11, 2018 when the entity should have completed the 15 day log review, and ended on April 12, 2018, when the entity completed the overdue 15 day log review.</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 that performing a late log review could result in ongoing undetected activity. The risk is minimized because the 15 day log review was only performed one day late. The entity quickly identified, assessed, and corrected this noncompliance. Additionally, IT Security had logging and monitoring in place for the duration of the noncompliance. No security alerts were identified during the noncompliance. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the log review; and 2) researched, documented and implemented the [REDACTED] to review and report log anomalies to fulfill the 15 day log 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
SERC2017017763	CIP-006-6	R2, P2.2	██████████	██████████	12/12/2016	12/12/2016	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 violation.)			<p>On June 16, 2017, the Entity submitted a Self-Report stating that, as a ██████████, ██████████, ██████████, ██████████, ██████████, and ██████████, it was in noncompliance with CIP-006-6 R2, P2.2. The Entity failed to record all required details in a visitor log entry for one Physical Security Perimeter (PSP).</p> <p>On March 22, 2017, a consultant reviewed the Entity's CIP Program and noticed an incomplete log for one visitor who visited the primary control center PSP. On December 12, 2016, although the Entity manually logged the date and time of the visitor's entry and exit of the PSP and the visitor's name, the Entity failed to include the name of the visitor's escort. The affected PSP contained ██████████ medium-impact Bulk Electric System Cyber Assets.</p> <p>The Entity conducted an extent-of-condition analysis by reviewing all visitor logs for both the primary and backup control centers. The Entity found no other instances of noncompliance.</p> <p>This noncompliance started on December 12, 2016, when the Entity failed to include the name of the visitor's escort in the log entry, and ended on December 12, 2016, when the visitor's exited the PSP.</p> <p>The root cause of the non-compliance was insufficient training.</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 maintain a complete visitor log could impede an investigation in the event a cyber security incident occurs while a visitor was inside the PSP. However, a review of the surveillance video revealed that the visitor was escorted throughout the length of the visit, and a review of existing manual logs revealed no other instances of noncompliance. No harm is known to have occurred.</p> <p>The Entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) reviewed other logs to determine the extent of condition and did not find any other errors; 2) sent an email to ██████████ that alerted them of the incident and reminded them of their responsibilities to escort individuals; and 3) modified annual CIP training for authorized employees to utilize video and quiz-scored computer-based training to improve understanding of responsibilities as an escort to visitors. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017762	CIP-009-6	R3 P3.1.3	[REDACTED]	[REDACTED]	11/10/2016	06/14/2017	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 June 16, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED], it was in noncompliance with CIP-009-6 R3, P3.1.3. The Entity did not notify each person or group, with a defined role in the recovery plan, of updates within 90 calendar days of the completion of the recovery plan test.</p> <p>On August 11, 2016, the Entity performed a paper drill of the CIP-009 recovery plan. On August 30, 2016, the Entity made changes to the recovery plan in response to the lessons learned from the paper drill. The changes were minor, such as, updating a link and removing a reference to a resource that was no longer in service. On that same day, the Entity sent an email to three individuals notifying them of the changes to the recovery plan.</p> <p>On March 30, 2017, a consultant reviewed the Entity's CIP program and discovered that the notification email was not sent to all required recipients. In addition, to the three individuals who did receive the email, the notification email should have also been sent to all members of the [REDACTED] and [REDACTED], the [REDACTED], [REDACTED], and the [REDACTED].</p> <p>On June 14, 2017, the Entity sent the notification of the changes to the remaining affected parties. By August 30, 2017, the Entity developed a checklist designed to ensure that all affected parties are notified, as part of the notification process, of changes to the recovery plan.</p> <p>The extent-of-condition was performed by confirming that the aforementioned change was the only change that had been made to the recovery plan based on lessons learned from the paper drill.</p> <p>The noncompliance started on November 10, 2016, 91 days after the recovery plan test was completed, and ended on June 14, 2017, when the remaining affected parties were notified.</p> <p>The root cause of the noncompliance was lack of an internal control, e.g., a checklist, to ensure that all parties are notified.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a minimal or substantial risk to the reliability of the bulk power system. The Entity's failure to notify all affected individuals of changes to the recovery plan could have delayed its recovery of reliability functions performed by the Bulk Electric System Cyber Systems. However, the differences between the prior and updated versions of the recovery plan were minor, such as updating a link and removing a reference to a resource that was no longer in service, and did not represent changes to actual actions required of responders. Furthermore, although not formally communicated, the changes to the recovery plan were made available to all affected individuals via a network folder. 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) updated the recovery plan procedure to simplify the roles of responders and make staff aware of the need to communicate the plan to all of those individuals identified in the plan; 2) developed a checklist to ensure that all parties are notified; and 3) significantly reduced the number of responders in the plan to include only functional responder roles. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017761	CIP-007-6	R3, P3.3	[REDACTED]	[REDACTED]	07/01/2016	02/06/2018	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 violation.)			<p>On June 16, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED], it was in noncompliance with CIP-007-6 R3, P3.3. The Entity did not have a documented process for the testing of malware signatures or patterns.</p> <p>On March 30, 2017, a consultant examined the Entity’s CIP Version 5 Compliance Program and discovered that the Entity did not implement a documented process for malware signature testing specific to the Physical Access Control System (PACS). Although the Entity did not have a documented process for malware signature testing, the Entity still performed the testing. On February 6, 2018, the Entity implemented a new process document that detailed the PACS-specific steps for malware signature testing.</p> <p>The affected asset included [REDACTED] Cyber Asset, the [REDACTED] associated with [REDACTED] [REDACTED] impact Bulk Electric System Cyber System.</p> <p>An extent-of-condition analysis (EOC) was conducted by examining the current effective process documents. The Entity confirmed that the [REDACTED] was the only applicable Cyber Asset not covered by a documented malware signature testing process.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on February 6, 2018, when the Entity implemented its new process document that detailed the PACS-specific steps for malware signature testing.</p> <p>The root cause of this noncompliance was an insufficient documentation process. The Entity was following a process for malware signature testing for the PACS Cyber Asset in question, however, the process just wasn’t documented.</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 documenting a process for testing malware signatures, the Entity risked the installation of untested malware signatures on the PACS server. There was a possibility that installation of untested malware signatures could have caused instability on the PACS server, which could have led to a failure of physical access control functionality. However, this was a documentation deficiency, as testing of the malware signature for the PACS server was being conducted even though a documented testing process had not been implemented. No harm is known to have occurred.</p> <p>The Entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) implemented a documented process for testing and updating malware definitions, which includes the use of the change management ticket system; 2) improved the PACS validation procedures associated with malware definition updates and the patching cycle that was accomplished by testing the alarm delivery function of the PACS application by incorporating the use of emails as evidence to prove testing; and 3) trained applicable staff on the procedural improvements that consisted of reviewing the procedure and discussing the effectiveness of key changes. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016719	CIP-006-6	R2, P2.2	██████████	██████████	07/06/2016	08/26/2016	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 violation.)			<p>On December 28, 2016, the Entity submitted a Self-Report to SERC stating that, as a ██████████, it was in violation of CIP-006-6 R2, P2.2. The Entity had 19 instances where it did not log all required information for visitors who accessed a Physical Security Perimeter (PSP).</p> <p>Beginning August 1, 2016, during the performance of an annual internal cyber security audit, the Entity discovered 19 instances incomplete access logs associated with 18 visitors who accessed the primary control center PSP. Specifically, from July 6, 2019 through August 15, 2016, the Entity failed to log the names of the escorts (16 instances); entry time (1 instance); and exit time (2 instances) of visitors who accessed the PSP.</p> <p>The affected Cyber Assets included ██████ medium impact Bulk Electric System (BES) Cyber System, the energy management system, containing ██████ BES Cyber Assets and ██████ Protected Cyber Assets.</p> <p>The Entity assessed the extent-of-condition by reviewing all the in-scope manual visitor logs as part of the annual internal security audit and discovered these 19 instances.</p> <p>This noncompliance started on July 6, 2016, when the Entity was required to log all visitor access information, and ended on August 26, 2016, when the Entity completed its Mitigation Plan.</p> <p>The root cause of this noncompliance was a combination of inadequate training, internal controls, and a visitor control process. The process allowed multiple individuals to complete the access logs, including visitors, which created confusion as to personnel’s responsibilities for ensuring the completion of the visitor logs. Additionally, the process did not require secondary reviews of the logs to ensure they were completed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). The Entity’s incomplete documentation of visitor access to the PSP could have delayed or hindered an investigation of a physical or cyber incident had one occurred. However, the PSP visitors’ identities were known by the Entity and the Entity asserted that it continuously escorted all 18 visitors into the PSP, which was staffed 24/7. None of the visitors had the ability (credentials, user ID, or password) to log onto any of the Cyber Assets inside the PSP. 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) discussed the importance of properly filling out logs to control room staff and authorized escorts; 2) addressed the importance of properly filling out logs at staff meetings; 3) added the topic of visitor logbooks to the annual ██████████ training; and 4) created a new process for the Entity to follow, including: <ol style="list-style-type: none"> a) only allowing escorts to fill out logs; b) a ██████████ reviews the visitor logbook daily; c) management periodically reviews the visitor logbook; d) using a new, more intuitive visitor logbook sheet; and e) a third party periodically audits the visitor logbooks. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017663	CIP-004-6	R4, P4.1	[REDACTED]	[REDACTED]	10/04/2016	10/18/2016	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 violation.)			<p>On May 26, 2017, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-004-6 R4, P4.1. The Entity did not implement its process to authorize electronic access based on need and gave a Physical Access Control System (PACS) Contractor unauthorized access to its PACS server.</p> <p>On April 11, 2017, while preparing for a third-party internal control CIP gap assessment, the Entity identified that, on October 4, 2016, its IT Department had given its PACS contractor unauthorized electronic access to its PACS to perform a change.</p> <p>On September 1, 2016, the Entity's [REDACTED] initiated an internal change request for its PACS Contractor (Contractor) to install and re-install video integration on its system. On three separate occasions, a member of the [REDACTED] used his credentials to log the Contractor into two different PACS Server. The Contractor was physically escorted by approved escorts with the [REDACTED]. These instances occurred on October 4, 2016, October 5, 2016 and October 18, 2016.</p> <p>The scope of affected facilities included [REDACTED] medium impact BES Cyber System (BCS), with [REDACTED] Electronic Security Perimeter (ESP), and [REDACTED] Physical Security Perimeters (PSPs), which consisted of all of the Entity's [REDACTED] BES Cyber Assets (BCAs), Protected Cyber Assets (PCAs), Electronic Access Control and/or Monitoring Systems (EACMSs) and PACS devices.</p> <p>The extent-of-condition assessment consisted of an investigation with the Entity's [REDACTED] subject matter experts (SMEs) for the Distributed Control System and determined that there were no additional instances of unauthorized electronic access.</p> <p>This noncompliance started on October 4, 2016, when the Entity gave the PACS Contractor unauthorized electronic access to the Entity's PACS Server, and ended on October 18, 2016, when the Contractor finished reinstalling the software on the Entity's PACS workstation.</p> <p>The root cause of this noncompliance was a lack of training. The Entity's [REDACTED] erroneously believed that as long as it had a business need for the Contractor to make changes to the PACS Server and was physically escorted, the [REDACTED] could allow the Contractor to access the PACS Server electronically by using an [REDACTED] Employee's credentials.</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 Entity's failure to vet the Contractor through its Personnel Risk Assessment (PRA) process and approve electronic access for the Contractor through its electronic access procedure, could have enabled the Contractor, if they were malicious or incompetent, to install malicious software or deactivate the badge swipe access to the two PSPs and allow the doors to be unlocked, thereby creating potential risk to the bulk power system. However, the Contractor was monitored at all times by a member of the [REDACTED] and was never given credentials to log into the machine. A member of the [REDACTED] logged in each time access was needed for the operation being performed. Also, the Entity subsequently processed the Contractor through its Access Management Program, who underwent and passed a personnel risk assessment and was ultimately, given authorized electronic access rights. Also, the access was limited to the four PACS devices and the badge swipe access continued to function as designed. 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 PACS Contractor take and pass a PRA and obtain CIP training; 2) approved the PACS Contractor for authorized electronic access on the PACS system, by following its procedure; 3) trained its [REDACTED] on physical and electronic access and the Entity's processes, roles and responsibilities; 4) remedied the organizational silos that existed between the [REDACTED] and [REDACTED] with staffing changes and aligned the two departments to work more closely together; and 5) added signage to the PACS server and workstations so anyone working on or authorizing work on the PACS will know that they need the proper authorized 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
SERC2017018496	CIP-006-6	R2, P2.1, P2.2	[REDACTED]	[REDACTED]	04/12/2017	03/21/2018	Self-Report	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>On October 19, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-006-6 R2, P2.1 and P2.2. The Entity had three instances where it did not properly log visitors into Physical Security Perimeters (PSPs) (P2.2), and one instance where it did not provide continuous escort to a visitor within a PSP (P2.1). The Entity submitted an expansion of scope noting an instance with CIP-006-6 P2.1 where it failed to provide continuous escort to a visitor within a PSP. Additionally, on [REDACTED], during a Compliance Audit, SERC identified one instance where a visitor escort failed to log into the logbook as an escort (P2.2).</p> <p>Sometime before May 1, 2017, the Entity began an initiative to implement and bolster internal controls associated with employee security-related responsibilities. As part of this initiative, the Entity conducted a random sampling of access logs encompassing a two month period. On May 1, 2017, during this process, the Entity discovered one instance where a visitor was left unescorted within a PSP (P2.1), and three instances where the Entity failed to properly log the entry and exit of a visitor from a PSP (P2.2).</p> <p>In the first instance, on April 12, 2017, at 8:56 a.m., a visitor entered a substation [REDACTED] PSP housing [REDACTED] medium impact Bulk Electric System (BES) Cyber Systems (BCSs) with access to [REDACTED] BES Cyber Assets (BCAs). The visitor was not logged in as a visitor in the logbook until four minutes later, at 9:00 a.m.</p> <p>In the second instance, on April 18, 2017, at 11:14 a.m., a visitor entered a substation [REDACTED] PSP housing [REDACTED] medium impact BCSs with access to [REDACTED] BCAs. The visitor's entry and exit from the PSP was not logged in the visitor logbook.</p> <p>In the third instance, on May 9, 2017, a visitor was left unescorted within a substation [REDACTED] PSP for 30 seconds. The fourth instance also occurred on May 9, 2017, when the visitor involved in the third instance was not properly logged into or out of the PSP. The PSP at issue in the third and fourth instances housed [REDACTED] medium impact BCSs with access to [REDACTED] BCAs.</p> <p>Regarding the fifth instance, on May 9, 2018, the Entity submitted a Scope Expansion stating that it had an instance with CIP-006-6 R2.1 where it failed to continuously escort a visitor within a PSP. Specifically, on April 10, 2018, while implementing a detective internal control designed to ensure that procedural controls were performed properly, the Entity discovered that on March 21, 2018, an employee did not continuously escort a visitor while inside a substation [REDACTED] PSP, which housed [REDACTED] medium impact BCSs with access to [REDACTED] BCAs. The escort departed the PSP at approximately 3:11 p.m., and reentered the PSP at approximately 3:13 p.m., and resumed escorting the visitor at that time. Both the escort and the visitor were employees performing CIP-related functions from the same business unit.</p> <p>The scope of affected facilities in the five instances described above included [REDACTED] medium impact BCSs and [REDACTED] BCAs.</p> <p>With respect to the sixth instance, on [REDACTED], during a Compliance Audit, SERC identified a control center logbook entry where a visitor escort did not log into the logbook as the escort. This instance occurred on August 9, 2017. This instance was assigned [REDACTED], which was consolidated into the original October 9, 2017 Self-Report.</p> <p>The scope of affected facilities in the sixth instance included [REDACTED] BCS containing [REDACTED] BCAs.</p> <p>This noncompliance started on April 12, 2017, the first known instance where the Entity failed to log a visitor's entry and exit from a PSP, and ended on March 21, 2018, when the last instance of an unescorted visitor occurred.</p> <p>The root cause for all instances of noncompliance was insufficient CIP compliance training.</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 Entity's failure to provide continuous escort to visitors within a PSP and failure to properly log PSP entries and exits could result in unauthorized physical access and misuse of the BCS devices without the Entity's knowledge. However, the Entity employed security cameras that facilitated recognition of employees and visitors. Additionally, the affected BCSs all required access credentials and employed security monitoring. Furthermore, the Entity authorized the visitor (sixth instance) for unescorted PSP access to the primary and backup control centers. 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	To mitigate this noncompliance, the Entity: <ol style="list-style-type: none">1) initiated a CIP compliance stand down by disabling card reader access to the [REDACTED] for all employees;2) required employees that needed to reenter facilities to contact the [REDACTED] to gain access;3) conducted training with the affected management team during the time that [REDACTED] access was disabled;4) reviewed issues and the specific CIP requirements, as well as the means through which the Entity complied with the requirements;5) directed management to take information from the training back to their groups to review it with their staff; and6) reestablished [REDACTED] access to all employees approximately one week after it was disabled.
-------------------	--

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019021507	CIP-002-5.1a	R2; R2.2	[REDACTED] (the "Entity")	[REDACTED]	09/01/2018	11/28/2018	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 violation.)			<p>On May 8, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-002-5.1a R2.2. In particular, the Entity is unable to demonstrate that its CIP Senior Manager (or an approved delegate) approved the identifications required by CIP-002-5.1a R1 at least once every 15 calendar months.</p> <p>The root cause of this noncompliance was a lack of internal controls to ensure that recurring tasks were performed in a timely manner.</p> <p>This noncompliance started on September 1, 2018, which is the first day that is more than 15 calendar months from when the Entity documented CIP Senior Manager (or delegate) approval of the identifications made in CIP-002-5.1a R1 and ended on November 28, 2018, when the Entity's CIP Senior Manager approved the Entity's identifications required by CIP-002-5.1a R1.</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 Entity owns and operates [REDACTED]. The duration of the noncompliance was short, lasting only 88 days. Additionally, no changes in identified assets or impact criteria occurred. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To end this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) documented CIP Senior Manager approval of the identifications required by CIP-002-5.1a R1; and to prevent recurrence of this noncompliance, the Entity will complete the following activities in the future: <ol style="list-style-type: none"> a) implement a monthly compliance call to ensure staff are aware of upcoming compliance dates; b) implement a software solution to create reminders for compliance due dates; and c) create a repository for compliance records and data. <p>Texas RE has verified the completion of all mitigation activities related to ending the noncompliance.</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
TRE2019021295	CIP-007-6	R5.4	██████████ (the "Entity")	██████████	03/21/2018	01/16/2019	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 1, 2019, the Entity submitted a Self-Log stating that, as a ██████████ it was in noncompliance with CIP-007-6 R5, Part 5.4. Specifically, the Entity failed to implement its documented process to change known default passwords, per Cyber Asset capability. This issue impacted ██████ default password on the administrator account o ██████ BES Cyber System.</p> <p>On January 15, 2019, during the review of its annual Cyber Vulnerability Assessment as part of internal compliance verification, the Entity discovered that the default password on the administrator account had not been changed. The default password was changed the following day, ending the noncompliance. The root cause of this noncompliance was insufficient training for personnel responsible for setting passwords on ██████████ BES Cyber Systems. There were ██████ of the specific devices at issue on site, and for ██████████ devices the default administrative password was timely changed.</p> <p>This noncompliance started on March 21, 2018, when device was installed and classified as a ██████████ BES Cyber System and ended on January 16, 2019, when the default password at issue was 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 based on the following factors. First, the device at issue provides communications for relay systems; however, ██████████. The device is located ██████████, the device at issue is secured within the Physical Security Perimeter, and the PSP location is equipped with ██████████. Second, there is no External Routable Connectivity at the ██████████. Third, during the time period at issue, there were no attempts of unauthorized physical access to the Physical Security Perimeter that housed the device at issue. No harm is known to have occurred.</p> <p>Texas RE 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) changed the password for the BES Cyber System at issue; 2) provided training for personnel involved in setting passwords on ██████████ BES Cyber Systems on the applicable procedure; and 3) updated the training materials for the configuration of the specific type of device at 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
TRE2019021333	CIP-003-6	R1; R1.1; R1.2	██████████ (the "Entity")	██████████	12/01/2018	12/21/2018	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 violation.)			<p>On April 5, 2019, the Entity submitted a Self-Report stating that, as a ██████████, it was in noncompliance with CIP-003-6 R1. In particular, the Entity did not review and obtain CIP Senior Manager at least once every 15 calendar months for ██████ cyber security policies that addressed topics identified within CIP-003-6 R1.1 and CIP-003-6 R1.2.</p> <p>This noncompliance started on December 1, 2018, which is the first day of the month that is more than 15 calendar months since the policies were approved, and ended on December 21, 2018, when all of the policies had been reviewed within 15 calendar months.</p> <p>The root cause of this noncompliance was a misconfigured notification system and insufficient time management. The Entity implemented a notification system in 2017. If a notification is not closed by the Entity within the Entity's defined appropriate timeframe a subsequent notification is sent. The notifications for reviewing the Entity's Cyber Security policies were not closed within the defined timeframe, and the system did not send the expected escalations to the CIP Senior Manager.</p> <p>Despite the notification system's failure to send the expected escalations the Entity had already scheduled reviews of the Cyber Security policies. However, the Entity's scheduled timeline did not provide sufficient time to conduct what the Entity considered to be an adequate review of the Cyber Security 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. The risk posed by not reviewing cyber security policies in a timely manner is the policies may become outdated and no longer applicable to the environment they are intended to protect.</p> <p>The risk posed by this noncompliance is reduced due to the following:</p> <ol style="list-style-type: none"> 1) The noncompliance was short, lasting only 21 days; 2) The noncompliance was administrative in nature; and 3) The Entity took additional time to conduct a thorough review instead of signing off on hastily reviewed policies in order to meet compliance. <p>No harm is known to have occurred.</p> <p>Texas RE 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) Reviewed their cyber security policies and obtained CIP Senior Manager approval. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019021578	CIP-006-6	R1; R1.2	[REDACTED] (the "Entity")	[REDACTED]	01/06/2019	01/07/2019	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 May 16, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-006-6 R1. In particular, the Entity failed to continuously utilize at least one physical access control to allow unescorted physical access into a Physical Security Perimeter (PSP) to only those individuals who have authorized unescorted physical access, as required by CIP-006-6 R1.2.</p> <p>This noncompliance started on January 6, 2019, when an individual with authorized unescorted access exited one of the Entity's PSPs and failed to ensure the door closed behind them. This noncompliance ended on January 7, 2019, when the CIP Senior Manager discovered the open door and closed it.</p> <p>The root cause of this noncompliance was insufficient automated controls and a lack of documented procedures. The Entity had [REDACTED] [REDACTED] was subsequently involved in this instance of noncompliance. Entity staff received a notification that the door was held open, determined that an authorized user was responsible, and took no further action.</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 in leaving a physical access point in a non-secure state is unauthorized individuals can gain physical access to BES Cyber Systems and their associated EACMS and PCAs. This can result in the BES Cyber Systems and their associated EACMS and PCAs being rendered unavailable, degraded, or misused. This can subsequently have an impact on the reliable operation of the Bulk Electric System.</p> <p>The risk posed by this noncompliance is reduced due to the following:</p> <ol style="list-style-type: none"> 1) The noncompliance was short, lasting less than 24 hours; and 2) [REDACTED] <p>No harm is known to have occurred.</p> <p>Texas RE 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) Closed the PSP door; and to prevent reoccurrence of this noncompliance the entity: <ol style="list-style-type: none"> a) [REDACTED] that did not already have one installed; and b) updated their Physical Access Monitoring procedure to include more details on alert handling. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019729	CIP-002-5.1a	R2.2	████████████████████ (the "Entity")	████████	10/01/2017	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 violation.)			<p>On May 21, 2018, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-002-5.1a R2.2. Specifically, the Entity failed to have its CIP Senior Manager or delegate to approve the identifications required by Requirement R1 at least once every 15 calendar months.</p> <p>The Entity engaged a third-party contractor to supervise its compliance with NERC Standards. The contractor reviewed the Entity's compliance records and, on May 3, 2018, discovered that the Entity had not required the CIP Senior Manager or a delegate to approve the identifications required by Requirement R1 prior to the expiration of the 15 calendar month period allowed for compliance with the Standard. On May 3, 2018, the Entity's CIP Senior Manager reviewed and approved the Entity's identifications, completed in accordance with CIP-002-5.1a R1, ending the noncompliance.</p> <p>The root cause of this noncompliance was ██████████ failure to track and schedule compliance activities with a routine schedule.</p> <p>This noncompliance started on October 1, 2017, when the 15 calendar month period allowed for compliance expired, and ended on May 3, 2018, when the Entity's CIP Senior Manager approved the identifications required by Requirement R1.</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 average output for this Facility is ██████████ which represents ██████████ of ERCOT's available capacity. Additionally, approximately ██████████ generated are consumed within the ██████████. No harm is known to have occurred.</p> <p>Texas RE 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) completed the required approvals of identifications required by Requirement R1; 2) has continued its engagement of a third-party contractor to supervise NERC compliance activity; and 3) implemented a tracking spreadsheet to remind staff of periodic compliance deadlines. <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
WECC2018020117	CIP-004-6	R4: P4.1.3.	[REDACTED]	[REDACTED]	4/2/2017	5/18/2017	Self-Report	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>On July 27, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in noncompliance with CIP-004-6 R4. Specifically, for two instances, the entity granted unauthorized access to BES Cyber System Information (BCSI) storage locations. The two individuals did not complete CIP training prior to the access being granted which was required per the entity’s documented procedure. In both instances, access permissions from another employee in a similar role were copied instead of implementing the documented process to authorize and then grant access privileges based on need. The first instance started April 2, 2017 when access was inappropriately granted and ended on April 10, 2017 when the individual’s access was authorized, for a total of 9 days. The second instance started on May 15, 2017 and ended on May 18, 2017 when the individual’s access was authorized, for a total of 4 days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to appropriately perform CIP-004-6 R4 Part 4 sub-part 4.1.3. The root cause of the issue was attributed to less than adequate training and controls. Specifically, the entity had a procedure and automated process for authorizing access to BCSI. In these instances, the procedure was not adhered to and the automated process was circumvented.</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 these instances, the entity failed to adequately implement its documented process to authorize access to designated BCSI storage locations as required by CIP-004-6 R4 Part 4 sub-part 4.1.3 when it granted unauthorized access to BCSI storage locations to two individuals.</p> <p>Failure to require authorization of access to designated BCSI storage locations could result in mishandling or exposure of sensitive data due to lack of awareness regarding the proper handling of BCSI. However, the entity had a well-documented process to approve access to BCSI. The two individuals with unauthorized access were supposed to have access because they were eventually authorized and they already had the prerequisite requirement of a personnel risk assessment (PRA). Additionally, as compensation, the entity detected this issue during its quarterly review of access authorization records. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this issue, the entity has:</p> <ul style="list-style-type: none"> a. authorized the access for the two individuals in scope; b. conducted an internal investigation to confirm that the scope of the issue was limited to the two reported instances; c. added electronic labels to access provisioning technology to alert staff that the authorization process is required; d. performed training for staff regarding provisioning access; and e. modified an informal process document to clarify tasks based on feedback provided during the training. <p>WECC has verified the completion of all mitigation activity.</p>					

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC)

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
WECC2018020415	CIP-003-6	R1	[REDACTED]	[REDACTED]	8/1/2018	9/18/2018	Self-Report	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>On September 17, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in potential noncompliance with CIP-003-6 R1. Specifically, the entity employed a consulting firm to monitor compliance with CIP-003-6. At the end of March 2018, the lead project manager assigned to assist the entity was reassigned. Prior to the lead's departure, a checklist of responsibilities was prepared for the staff temporarily assigned to assist the entity, which included obtaining CIP Senior Manger approval for cyber security policies related to its Low Impact Bulk Electric System (BES) Cyber System (LIBCS) by July 31, 2018 (15-calendar months from the initial review and approval performed on April 1, 2017). The temporary staff failed to act on the activity to initiate the review. The root cause of this issue was attributed to an oversight of the task to perform Part 1.2 not being added to a SharePoint task list used by the consulting firm to keep the entity's management informed of upcoming compliance activities.</p> <p>This noncompliance started on August 1, 2018, the day after the 15th calendar month when the entity's cyber security policies should have been reviewed and approved by the CIP Senior Manager and ended on September 18, 2018, when the entity obtained said approval, for a total of 49 days.</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, the entity failed to obtain CIP Senior Manager approval every 15 calendar months for cyber security policies related to its LIBCS, as required by CIP-003-6 R1 Part 1.2.</p> <p>Failing to have the CIP Senior Manager review and approve cyber security policies at least once every 15 calendar months could result in a lack of oversight, and inconsistent or outdated policies that do not address new vulnerabilities. However, the entity [REDACTED] and this issue is purely administrative in nature. No harm is known to have occurred.</p> <p>WECC determined the entity does not have any relevant compliance history for this Standard and Requirement.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reviewed and obtained CIP Senior Manager approval for its cyber security policies related to LIBCS; 2) implemented a new version of the work flow software released by its consulting firm. This update utilized the version history capabilities of SharePoint which generated a task and sent an email notification to the entity's subject matter experts and consultant staff for review and approval of procedures; and 3) implemented an annual review of all applicable Standards at the beginning of each year for heightened awareness and reconciliation as an ongoing control to prevent compliance issues. <p>WECC 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
WECC2017018399	CIP-008-5	R3	[REDACTED]	[REDACTED]	3/7/2017	6/5/2017	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 September 29, 2017, the entity submitted a Self-Report stating, as a [REDACTED], and [REDACTED], it was in noncompliance with CIP-008-5 R3. Specifically, on December 7, 2016, the entity completed an annual test of its Cyber Security Incident response plan and documented lessons learned. However, the entity did not update the plan with the lessons learned until May 31, 2017, and did not notify appropriate personnel until June 5, 2017, exceeding the no later than 90 calendar days requirement by 91 days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to update its Cyber Security Incident response plan with lessons learned as required by Sub-Parts 3.1.2 and failed to notify the applicable personnel of the updates, as required by Sub-Parts 3.1.3. The root cause of the issue was attributed to a less than adequate process. Specifically, the entity's procedure did not include a proper tracking system for the tasks assigned with CIP-008-5 R3. Additionally, the procedures did not provide an accurate timeline for when the tasks should be completed.</p> <p>This noncompliance started on March 7, 2017, 91 days after the test was completed on the entity's Cyber Security Incident response plan and ended on June 5, 2017, when the entity updated its plan with lessons learned and notified and the appropriate personnel for a total of 91 days.</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. In these instances, the entity failed to update its Cyber Security Incident response plan with lessons learned as required by CIP-008-5 R3 Sub-Part 3.1.2 and failed to notify the applicable personnel of the updates, as required by CIP-008-5 R3 Sub-Part 3.1.3. Such failure could potentially result in personnel responsible for recovery to take inappropriate action during an event, which could lead to less effective response or possible exacerbation of the event. However, as compensation, all appropriate personnel were involved in the test and were therefore already aware of the lessons learned. As further compensation, the entity did have a Cyber Security incident response plan and recovery plan in place, which had both previously been documented and distributed. No harm is known to have occurred.</p> <p>WECC determined that the entity did not have any relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the Cyber Security Incident response plan with lessons learned; 2) distributed the updated plan to applicable personnel; 3) updated its procedure to add more clarity on the timeframes for when changes should be documented and distributed; and 4) implemented a new online tool that utilizes automated task reminders for updating and distributing the Cyber Security Incident response plan. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018400	CIP-009-6	3	[REDACTED]	[REDACTED]	3/7/2017	6/5/2017	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 September 29, 2017, the entity submitted a Self-Reports stating, as a [REDACTED], and [REDACTED], it was in noncompliance with CIP-009-6 R3. Specifically, on December 7, 2016, the entity completed an annual test of its recovery plan and documented lessons learned. However, the entity did not update the plan with the lessons learned until May 31, 2017, and did not notify appropriate personnel until June 5, 2017, exceeding the no later than 90 calendar days requirement by 91 days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to update its recovery plan with lessons learned as required by Sub-Parts 3.1.2 and failed to notify the applicable personnel of the updates, as required by Sub-Parts 3.1.3. The root cause of the issue was attributed to a less than adequate process. Specifically, the entity's procedure did not include a proper tracking system for the tasks assigned with CIP-009-6 R3. Additionally, the procedures did not provide an accurate timeline for when the tasks should be completed.</p> <p>This noncompliance started on March 7, 2017, 91 days after the test was completed on the entity's recovery plan and ended on June 5, 2017, when the entity updated its plan with lessons learned and notified and the appropriate personnel for a total of 91 days.</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. In these instances, the entity failed to update its recovery plan with lessons learned as required by CIP-009-6 R3 Sub-Part 3.1.2 and failed to notify the applicable personnel of the updates, as required by CIP-009-6 R3 Sub-Part 3.1.3. Such failure could potentially result in personnel responsible for recovery to take inappropriate action during an event, which could lead to less effective response or possible exacerbation of the event. However, as compensation, all appropriate personnel were involved in the test and were therefore already aware of the lessons learned. As further compensation, the entity did have a recovery plan in place, which had previously been documented and distributed. No harm is known to have occurred.</p> <p>WECC determined that the entity did not have any relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the recovery plan with lessons learned; 2) distributed the updated plan to applicable personnel; 3) updated its procedure to add more clarity on the timeframes for when changes should be documented and distributed; and 4) implemented a new online tool that utilizes automated task reminders for updating and distributing the recovery plan. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019195	CIP-004-6	R2: P2.3	[REDACTED]	[REDACTED]	11/26/2017	11/28/2017	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 February 14, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in noncompliance with CIP-004-6 R2. Specifically, on November 26, 2017, one individual with unescorted physical access to the Physical Security Perimeter controlling access to the entity's High Impact Bulk Electric (BES) Cyber Systems (HIBCS) at the primary Control Center, and to its associated data center areas, did not complete cyber security training within 15 calendar months of their previous training. The issue ended on November 28, 2017 when the employee's unescorted physical access was revoked, as it was no longer needed for their role, for a total of three days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to appropriately perform CIP-004-6 R2 Part 2.3. The root cause of the issue was attributed to insufficient processes and controls. Specifically, the employee did not complete the required training because they knew their role no longer required physical access and believed that their access would be automatically revoked when they failed to complete their training. Further, although the entity sent electronic reminders on three separate instances to the employee to complete the training, the employee's supervisor was not notified of the impending training completion deadline nor was the employee's access reviewed for appropriateness.</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. In this instance, the entity failed to appropriately implement its cyber security training program regarding the required completion of the cyber security training at least once every 15 calendar months as required by CIP-004-6 R2 Part 2.3, for one employee with unescorted physical access to a HIBCS.</p> <p>Failure to require timely completion of cyber security training could have resulted in the individual mishandling information or failing to follow an entity's current documented process when utilizing electronic or physical access. However, as compensation, the individual was a current employee with a personnel risk assessment completed within the past seven years; had previously completed cyber security training; and physical access records show the employee did not enter any secured area for the two days after her training had expired. Additionally, as a detective control, the entity conducted monthly reviews of training completion reports which allowed them to address upcoming training deadlines and identified this issue, reducing the noncompliance period. No harm is known to have occurred.</p> <p>WECC 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 has:</p> <ol style="list-style-type: none"> 1. disabled unescorted physical access for the employee as it was determined the employee no longer required access; 2. hired an additional Information Technology staff member to assess work load and determine if additional staff is required; 3. implemented an internal control to revoke electronic and authorized unescorted physical access if cyber security training was not completed by the deadline; 4. updated process documentation to emphasize the importance of completing cyber security training; 5. updated the training notification email distribution list to include supervisors of employees required to take training; 6. included a question in the training notification email designed to ascertain if access was still necessary; and 7. designed and implemented training for supervisors of employees with authorized electronic or unescorted physical access to Cyber Assets. <p>WECC 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
WECC2018020113	CIP-003-6	R2	[REDACTED]	[REDACTED]	2/5/2018	4/3/2018	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 violation.)			<p>On July 23, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in potential noncompliance with CIP-003-6 R2. Specifically, the entity, as a new owner of a [REDACTED] Facility, discovered through a gap analysis, that the previous owners did not complete a test of the Cyber Security Incident response plan (CSIRP) related to its Low Impact Bulk Electric System (BES) Cyber System (LIBCS) located at the Facility, as required by CIP-003-6 R2 Attachment 1 Section 4.5. The entity found a CSIRP on file at the Facility but no evidence a test or drill was ever performed. The root cause of the issue was attributed to the previous owner's negligence. The issue began on [REDACTED] when the entity took ownership of the Facility, and ended on April 3, 2018, when it completed testing of the plan, for a total of 58 days.</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. In this instance, there was a failure to test the CSIRP related to a LIBCS located [REDACTED], at least once every 36 calendar months, as required by CIP-003-6 R2 Attachment 1 Section 4.5.</p> <p>Failure to test the CSIRP could result in the entity operating under an outdated plan, which could delay the time it takes the entity to recovery in the event of a cyber incident, thus potentially impacting the entity's ability to provide [REDACTED] resources to neighboring entities. However, the affected Facility only operates [REDACTED]. No harm is known to have occurred.</p> <p>WECC determined the entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed a test of its CSIRP related to the one LIBCS; and 2) added a 36 calendar month reminder to ensure compliance going forward. <p>WECC 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
WECC2018019482	CIP-007-6	R2: P2.2	[REDACTED]	[REDACTED]	2/7/2018	3/1/2018	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 violation.)			<p>On April 3, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in noncompliance with CIP-007-6 R2. Specifically, the entity did not evaluate security patches every 35 days for [REDACTED] Physical Access Control Systems (PACS) associated with a High Impact Bulk Electric System (BES) Cyber System. A single employee was responsible for contacting the entity's vendor monthly to inquire about released security patches; the employee terminated their employment and the entity did not immediately identify a replacement for the task. This issue began on February 7, 2018, the day after the evaluation of released security patches since the last evaluation should have occurred and ended on March 1, 2018, when the employee newly assigned to the task conducted the March security patch evaluation and discovered that the February evaluation had not been completed, for a total of 23 days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to adequately perform CIP-007-6 R2 Part 2.1. The root cause of the issue was attributed to less than adequate controls regarding the assignment of compliance related tasks. Specifically, the entity's process did not incorporate preventative controls to prevent the noncompliance from occurring when the sole individual responsible for evaluating the applicability of released security patches left the company and a replacement for the task was not readily identified.</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. In this instance, the entity failed to evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in CIP-007-6 R2 Part 2.1 at least once every 35 calendar days when it failed to review security patches for [REDACTED] PACS for a total of 23 days.</p> <p>The entity did not have controls in place to prevent the noncompliance. However, as compensation, the entity had implemented anti-malware protection for its PACS and employed a third-party vendor to intentionally harden its PACS panels that are technically incapable of supporting anti-virus software. No harm is known to have occurred.</p> <p>WECC 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. evaluated security patches for applicability for the Cyber Assets in scope; 2. provided verbal training regarding security patch requirements and process to relevant personnel; 3. added security patch reviews as an agenda item at the monthly [REDACTED] Compliance Team meetings as a preventative and detective control; and 4. hired a NERC CIP Compliance Specialist to centralize NERC CIP compliance oversight. <p>WECC 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
WECC2018019548	CIP-007-6	R1: P1.1	[REDACTED]	[REDACTED]	07/01/2016	06/09/2017	Compliance 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 violation.)			<p>During a Compliance Audit conducted [REDACTED], WECC determined the entity, as a [REDACTED] had a potential noncompliance with CIP-007-6 R1 Part 1.1. Specifically, the entity had not identified four multi-use workstations as Physical Access Control Systems (PACS) and as such, did not afford the PACS the protections required by CIP-007-6 R1 Part 1.1. [REDACTED] The issue began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable to the entity and ended on June 9, 2017 when the entity replaced the four multi-use workstations with three single-use workstations. [REDACTED] identified the new workstations as PACS, and applied the necessary protections to those PACS including enabling only the logical network accessible ports that were determined to be needed by the entity, for a duration of 344 days.</p> <p>After reviewing all relevant information, WECC Enforcement concurred with the audit findings as described above. The root cause of the issue was attributed to inaccurate device classification. Specifically, the entity did not classify the workstations as PACS because the workstations were multi-use workstations [REDACTED]. The entity was not aware that installing PACS software on the workstations provided administrative access and function which made them PACS Cyber Assets and therefore subject to the protective measures of the CIP Standards.</p>					
Risk Assessment			<p>WECC determined 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, the entity failed to enable only logical network accessible ports that have been determined to be needed as required by CIP-007-6 R1 Part 1.1 on four PACS workstations.</p> <p>Failure to limit open ports to those that are deemed necessary expands the attack surface available to malicious actors. However, as compensation, the entity had afforded some of the protective measures of the CIP Standards to the PACS such as ports and services restrictions, malware protection, and it also required two-factor authentication to access any PACS software on the workstations. Additionally, the PACS were physically located within a PSP and physical and logical access to the PACS was limited to those individuals with a completed personnel risk assessment and training. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) replaced the four multi-purpose workstations with three single-purpose workstations and classified them as PACS; 2) enabled only logical network accessible ports that were determined to be needed for the three replacement PACS; 3) updated its Physical Security Plan to provide additional information regarding which devices should reside within the PSP; 4) provided training to relevant personnel regarding the changes made to the Physical Security Plan; and 5) updated its BES Cyber System Categorization process to include a review of its PSP at least once every 15 calendar months; this review includes ensuring all assets located at the PSP have been identified and appropriately categorized. <p>WECC 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
WECC2018019552	CIP-010-2	R1: P1.1	[REDACTED]	[REDACTED]	07/01/2016	06/09/2017	Compliance 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 violation.)			<p>During a Compliance Audit conducted [REDACTED], WECC determined the entity, as a [REDACTED] had a potential noncompliance with CIP-010-2 R1 Part 1.1. Specifically, the entity had not identified four multi-use workstations as Physical Access Control Systems (PACS) and as such, did not afford the PACS the protections required by CIP-010-2 R1 Part 1.1. [REDACTED] The issue began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable to the entity and ended on June 9, 2017 when the entity replaced the four multi-use workstations with three single-use workstations. [REDACTED], identified the new workstations as PACS, and developed a baseline configuration of the PACS, for a duration of 344 days.</p> <p>After reviewing all relevant information, WECC Enforcement concurred with the audit findings as described above. The root cause of the issue was attributed to inaccurate device classification. Specifically, the entity did not classify the workstations as PACS because the workstations were multi-use workstations [REDACTED]. The entity was not aware that installing PACS software on the workstations provided administrative access and function which made them PACS Cyber Assets and therefore subject to the protective measures of the CIP Standards.</p>					
Risk Assessment			<p>WECC determined 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, the entity failed to develop a baseline configuration as required by CIP-010-2 R1 Part 1.1 on four PACS workstations.</p> <p>Failure to fully develop an accurate baseline configuration makes it less likely an entity will detect unauthorized changes. However, as compensation, the entity had afforded some of the protective measures of the CIP Standards to the PACS such as ports and services restrictions, malware protection, and it also required two-factor authentication to access any PACS software on the workstations. Additionally, the PACS were physically located within a PSP and physical and logical access to the PACS was limited to those individuals with a completed personnel risk assessment and training. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) replaced the four multi-purpose workstations with three single-purpose workstations and classified them as PACS; 2) developed a baseline configuration for the three replacement PACS; 3) updated its Physical Security Plan to provide additional information regarding which devices should reside within the PSP; 4) provided training to relevant personnel regarding the changes made to the Physical Security Plan; and 5) updated its BES Cyber System Categorization process to include a review of its PSP at least once every 15 calendar months; this review includes ensuring all assets located at the PSP have been identified and appropriately categorized. <p>WECC 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
WECC2017018614	CIP-010-2	R1: P1.2	[REDACTED]	NCR [REDACTED]	10/25/2016	1/3/2018	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 violation.)			<p>On November 8, 2017, the entity submitted a Self-Report stating, as a [REDACTED] and [REDACTED], it was in potential noncompliance with CIP-010-2 R1. Specifically, on September 15, 2017, after completing an internal spot check, the entity discovered nine change records in which it did not provide authorization for the change applied to the baseline configurations of 10 Bulk Electric System (BES) Cyber Assets (BCAs), six Electronic Access Control or Monitoring Systems (EACMS), and eight Protected Cyber Assets (PCAs) associated with two Medium Impact BES Cyber System (MIBCS) [REDACTED]. In each instance, the baseline configurations were properly vetted and given in-process approval, however were not properly documented and authorized. The root cause of this issue was attributed to a less than adequate process. Specifically, the entity's change control procedure was complicated and lacked clear steps to be taken to ensure any changes to baselines configurations were authorized and documented as required by the Standard and Requirement.</p> <p>After reviewing all relevant information, WECC determined the entity failed CIP-010-2 R1 Part 1.2 as described above. The first of the nine changes began on October 25, 2016, when a change to an existing baseline configuration was not authorized and documented, and ended on January 3, 2018, when the last of the nine changes to an existing baseline configuration were authorized and documented, for a duration of 436 days.</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. In these instances, the entity failed to authorize and document changes that deviate from the existing baseline configuration for nine changes to CIP applicable Cyber Assets, as required by CIP-010-2 R1 Part 1.2.</p> <p>Such failure could result in the entity not knowing what programs and systems patch levels are in use. Without this knowledge the affected Cyber Assets could interact with approved programs/systems negatively, and result in degrading or disabling Cyber Assets that monitor and control BES elements. However, as compensation, each of the changes to the baseline configuration had been vetted and approved. It was the documentation of the changes and corresponding authorization that did not occur. The affected Cyber Assets [REDACTED]. As further compensation both MIBCS were [REDACTED]. No harm is known to have occurred.</p> <p>WECC considered the entity's compliance history in its designation of this remediated issue as a CE. The entity's prior compliance history with CIP-010-2 R1 includes NERC Violation ID [REDACTED]. WECC determined the entity's compliance history should not serve as a basis for pursuing an enforcement action and/or applying a penalty because the root cause and fact pattern was distinct and separate from the issue of this CE.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) authorized and documented the nine changes that occurred to the baseline configurations; 2) updated its process to remove extraneous information and define clearly the required test steps to verify security controls for CIP-005 and CIP-007 are not impacted by the change; 3) updated and simplified the change control request form; and 4) trained personnel responsible for the change control process on the updated procedures and forms. <p>WECC 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
WECC2018019294	CIP-006-6	R1	[REDACTED]	[REDACTED]	07/01/2016	08/06/2018	Self-Certification	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>On February 27, 2018, the entity submitted a Self-Certification stating, as a [REDACTED], it was in noncompliance with CIP-006-6 R1. Specifically, on November 16, 2017 while reviewing network diagrams and CIP-006 documentation, the entity discovered that a cabinet in its data center contained an Electronic Access Control or Monitoring System (EACMS) associated with a Medium Impact Bulk Electric System (BES) Cyber System (MIBCS) that was not afforded the protective measures of CIP-006-6 R1.</p> <p>After reviewing all relevant information, WECC determined the entity failed to adequately implement its documented physical security plan for one EACMS used for access to a MIBCS, as required by CIP-006-6 R1. Specifically, the entity did not include in its physical security plan one CIP cabinet that contains an EACMS, and only had one physical lock installed that was not controlled. As a result, the entity failed to define operational and procedural controls to restrict physical access as required by Part 1.1; utilize at least one physical access control to allow unescorted physical access into a Physical Security Perimeter as required by P1.2; monitor for unauthorized access through a physical access point into a Physical Security Perimeter as required by Part 1.4; issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter within 15 minutes of detection as required by Part 1.5; log entry of each individual with authorized unescorted physical access into each Physical Security Perimeter as required by Part 1.8; and retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days as required by Part 1.9.</p> <p>WECC determined this issue started on July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on August 6, 2018 when the entity completed mitigating activities, for a total of 100 days.</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, the entity failed to adequately implement its documented physical security plan for one EACMS as required by CIP-006-6 R1 as described above. However, as compensation, the EACMS was inside a locked cabinet, which was inside a secured data center where unescorted physical access was limited to authorized personnel via a [REDACTED]. Additionally, forced access through the data center door would have generated e-mail alerts and sent them to [REDACTED], alerting them of the unauthorized access attempt.</p> <p>No harm is known to have occurred.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, VEA has:</p> <ol style="list-style-type: none"> 1) updated its physical security plan to include the cabinet containing the EACMS; 2) updated its PSP diagrams 3) added access card readers to the cabinet doors; 4) configured the access card readers to monitor access; 5) generated alerts by adding forced door alarms to the cabinet doors; 6) configured the access card readers to generate access logs; 7) generated access logs for 90-day retention; 8) created an asset inventory list that shows all Cyber Assets and where they are located to keep track of, and ensure they are within a PSP and are afforded CIP protections; and 9) created an automated workflow for configuring new Cyber Assets to ensure compliance prior to placing a new device into service. <p>WECC has verified the completion of all mitigation activity.</p>					

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	MRO2019021531			Yes	Yes									Category 2 – 12: 2 years
2	MRO2018019124			Yes	Yes									Category 2 – 12: 2 years
3	MRO2018020852			Yes	Yes									Category 2 – 12: 2 years
4	MRO2019021514			Yes	Yes									Category 2 – 12: 2 years
5	MRO2018020156	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
6	MRO2018020272			Yes	Yes					Yes				Category 2 – 12: 2 years
7	SPP2018019377			Yes	Yes									Category 2 – 12: 2 years
8	MRO2018020160	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
9	MRO2018019144			Yes	Yes					Yes				Category 2 – 12: 2 years
10	MRO2019021544			Yes	Yes									Category 2 – 12: 2 years
11	SPP2018019378			Yes	Yes									Category 2 – 12: 2 years
12	SPP2018019379			Yes	Yes									Category 2 – 12: 2 years
13	NPCC2019021340			Yes	Yes		Yes		Yes	Yes	Yes			Categories 3 – 4: 2 years Categories 6, 8-10: 3 years
14	NPCC2019021341			Yes	Yes		Yes		Yes	Yes	Yes			Categories 3 – 4: 2 years Categories 6, 8-10: 3 years
15	NPCC2019012197			Yes	Yes		Yes		Yes					Categories 3 – 4: 2 years Categories 6, 8: 3 years
16	NPCC2019021396	Yes		Yes	Yes					Yes				Categories 3 – 4: 2 years Categories 1, 9: 3 years
17	NPCC2019021287			Yes	Yes				Yes					Categories 3 – 4: 2 years Category 8: 3 years
18	NPCC2019021298	Yes		Yes	Yes									Categories 3 – 4: 2 years Category 1: 3 years
19	RFC2018020559	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
20	RFC2018020560	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
21	RFC2018020370	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
22	RFC2018020373	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
23	RFC2018020375	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
24	RFC2018020376	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
25	RFC2018020377	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
26	RFC2018020380	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
27	RFC2018020381	Yes		Yes	Yes					Yes				Category 1: 3 years; 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)
28	RFC2018020675	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
29	RFC2018020676	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
30	RFC2018020677	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
31	RFC2018020679	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
32	RFC2018020638	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
33	RFC2018020789	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
34	RFC2018020790	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
35	RFC2018019815	Yes		Yes	Yes	Yes	Yes							Category 1: 3 years; Category 2-12: 2 years
36	RFC2018019818	Yes		Yes	Yes	Yes	Yes							Category 1: 3 years; Category 2-12: 2 years
37	RFC2018020757	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
38	RFC2018020758	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
39	RFC2018020678	Yes		Yes	Yes	Yes			Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
40	RFC2018019464	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
41	RFC2018020465	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
42	RFC2018020739	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
43	RFC2018020740	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
44	SERC2016016573			Yes	Yes								Yes	Category 2 – 12: 2 year
45	SERC2017017036			Yes	Yes					Yes				Category 2 – 12: 2 year
46	SERC2017017662			Yes	Yes									Category 2 – 12: 2 year
47	SERC2016016519			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
48	TRE2018020853	Yes		Yes	Yes	Yes	Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 year
49	TRE2018020854	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
50	WECC2018019299			Yes	Yes					Yes				Category 2 – 12: 2 year
51	WECC2018019644			Yes	Yes								Yes	Category 2 – 12: 2 year
52	WECC2018019369			Yes	Yes						Yes			Category 2 – 12: 2 year
53	WECC2018019945			Yes	Yes					Yes				Category 2 – 12: 2 year
54	WECC2018019947			Yes	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
MRO2019021531	CIP-003-6	R2	████████████████████ (The Entity)	████████	04/01/2017	01/15/2019	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 January 8, 2019, the Entity submitted a Self-Log stating that, as a ██████████, it was in noncompliance with CIP-003-6 R2.</p> <p>Per the Entity, when the Cyber Security Incident Response was first tested on March 21, 2017, the test exercise did not include test of external response for the test incident. The test incident was not a Reportable Cyber Security Incident, and the interaction with outside agencies was not tested.</p> <p>The cause of the noncompliance was the testing preparation was inadequate.</p> <p>The issue started on April 1, 2017, when the Cyber Security Incident response plan was not fully tested by the date in the implementation plan, and ended on January 15, 2019, when a comprehensive tabletop plan for testing a Reportable Cyber Security Incident was tested.</p>					
Risk Assessment			This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per the Entity, the majority of the Cyber Security Incident Response plan was tested on or before April 1, 2017. No harm is known to have occurred.					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed a comprehensive table top exercise for a hypothetical Reportable Cyber Security Incident; and 2) updated the exercise preparation form to reinforce that all future scenarios will be designed to test a Reportable Cyber Security Incident. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019124	CIP-006-6	R1	<div style="background-color: black; width: 100px; height: 15px; margin-bottom: 5px;"></div> (The Entity)	<div style="background-color: black; width: 40px; height: 15px;"></div>	02/02/2017	11/30/2017	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 January 8, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R1. During the 2017 fourth quarter review of authorized accesses, the Entity discovered that two employees retained unescorted physical access to their Backup Control Center (BUCC) without need. The employees' access to the BUCC was supposed to be revoked on January 31, 2017 following a determination that there no longer existed a need for the access, but it was discovered that the employees' access was not actually revoked.</p> <p>The cause of the noncompliance was that access revocation process lacked checks and balances needed to ensure the process was effective. The ineffective process was influenced by deficiencies in both the process itself, and in the clarity of the data utilized by the process.</p> <p>The issue began on February 2, 2017, which was after the end of the next calendar day following the responsible entity determination that the individuals no longer required access, and ended on November 30, 2017, when access to the BUCC was revoked for both employees.</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. Neither employee used their access card to enter the BUCC during the noncompliance. Both employees had Personnel Risk Assessments (PRAs) and had up-to-date training. Additionally, access revocation was a result of a voluntary refinement of need, and not due to termination, reassignment, or transfer. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked physical access for the two employees; 2) conducted an extent of condition analysis in fourth quarter of 2017 and repeated in the first quarter of 2018 and implemented a new physical security system, which supported improved reporting; 3) added a peer review step within the access revocation procedure; and 4) updated an internal guideline to be more explicit and includes a list of reports, with each report being specific to a unique PSP. The PSP specific reporting was an improvement over the single legacy report generated by the legacy system. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021514	CIP-006-6	R2	[REDACTED] (the Entity)	[REDACTED]	11/30/2018	03/20/2019	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 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R2. The self-log identified two instances of noncompliance.</p> <p>The first instance of noncompliance was discovered during an internal review of logs. The Entity states that an individual (P1) with authorized unescorted physical access privileges to the Primary Control Center (PCC) Physical Security Perimeter (PSP) entered the PCC with a visitor (V1). On November 30, 2018, the Entity states P1 and V1 exited the PCC, and neither the visitor’s nor the escort’s name were sufficiently logged. The cause of this noncompliance was that the Entity did not have a sufficiently rigorous procedure in place for issuance of temporary or visitor PSP badges. This noncompliance began on November 30, 2018 and ended on March 20, 2019, when [REDACTED] identified the visitor’s identity.</p> <p>For the second instance of noncompliance, the Entity states that a custodial employee with authorized unescorted physical access privilege to the PCC PSP escorted a contract plumber into the PCC PSP without first obtaining the proper visitor credentials (badge). The custodial employee was instructed to bring the plumber to security personnel, but the custodial employee brought the plumber to the Information Desk, who issued a corporate security badge. When the plumber swiped the badge at the PSP entrance, an invalid badge alert was issued, security personnel intercepted the plumber, and escorted the plumber out of the PSP so that the plumber could properly enter and be escorted. The cause of this noncompliance was that the Entity’s custodial employee failed to follow the Entity’s visitor control program. This noncompliance occurred on January 23, 2019, and ended a few minutes later when the plumber was escorted out of the PSP.</p> <p>The noncompliance began on November 30, 2018, when the visitor in instance one entered the PSP, and ended on March 20, 2019, when the Entity identified the visitor’s identity.</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 instance was minimal because per the Entity, for both P1 and V1, the time in the PSP was limited to a few minutes; the visitor was continuously escorted by someone with authorized unescorted PSP privileges. The second instance was minimal per the Entity because controls in place identified the noncompliance and supported quick resolution within a few minutes and the risk associated with the incident was reduced due to the fact that the plumbing contractor is regularly used (and trusted) by the entity. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) determined the identity of the visitor; 2) implemented a process to provide a printed checklist detailing proper issuance of a temporary badge; and 3) sent a memo to all individuals with authorized unescorted PSP access privileges to reinforce access management procedures which includes the visitor badge procedure. <p>To mitigate this second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) instructed the visitor and escort to leave the PSP and to obtain the correct visitor badge; 2) updated training materials with improved wording and format changes to reinforce the visitor control program and distributed to all personnel holding authorized unescorted access privileges to a PSP; and 3) sent memo to all individuals with authorized unescorted PSP access privileges to reinforce access management procedures, which includes the visitor badge 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
MRO2018020156	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	10/03/2017	02/09/2018	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 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2. The Self-Log identified four instances of noncompliance; MRO concluded that one of the instances did not represent noncompliance.</p> <p>The first instance of noncompliance involved a Protected Cyber Asset (PCA) (relay) for which the Entity failed to install or add to a dated mitigation plan for an applicable security patch within 35 days of evaluation. The individual creating the mitigation plan associated with the patch did not include the relay on the mitigation plan. The Entity discovered the issue through an internal review of previous patch mitigation plans. The cause of the noncompliance was that the Entity failed to follow its process for applying and/or creating a mitigation plan for applicable security patches. The noncompliance began on October 12, 2017, 35 days after the security patch was evaluated for the relay, and on February 9, 2018, when the applicable patch was added to a mitigation plan.</p> <p>In the second instance of noncompliance, for Electronic Access Control or Monitoring Systems (EACMS) (firewalls) associated with BES Cyber Systems at Control Centers, the Entity failed to evaluate applicable security patches within 35 days. It failed to follow its identified patch source when evaluating security patches, resulting in six security patches not being evaluated for the firewalls. The issue was discovered when another alternate patch source for the firewalls notified the Entity of a security release associated to the firewalls. The cause of the noncompliance was that the Entity failed to follow its process for evaluating security patches for applicability for firewalls, resulting in applicable security patches for firewalls not being evaluated. The noncompliance began on October 3, 2017 when an applicable security patch was not evaluated within 35 days of the last evaluation cycle and ended on January 31, 2018 when the Entity evaluated the applicable security patches.</p> <p>In the third instance of noncompliance, for a patch mitigation plan that included multiple BES Cyber Assets, EACMS, PCAs and Physical Access Control Systems (PACS) devices, the Entity failed to complete the mitigation plan or revise the mitigation plan within the timeframe of the mitigation plan. The Entity discovered that a patch mitigation plan dated for completion by January 1, 2018 was not implemented nor was an extension approved by the CIP Senior Manager. The cause of the noncompliance was that the Entity failed to follow its process for implementing patch mitigations plans, resulting in a mitigation plan not being implemented nor extended per the plans timeframe. The noncompliance began on January 1, 2018 when the patch mitigation plan was not updated to reflect a change in the anticipated date, and ended on January 17, 2018, when the patch mitigation plan was updated and approved with a new anticipated completion date.</p> <p>The noncompliance began on October 3, 2017 when applicable security patches were not evaluated in the second instance, and ended on February 9, 2018, when the applicable patch for the relay was added to a mitigation plan in the first 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. Per the Entity, the first instance was minimal because it was related to one PCA at one Transmission Facility and the vulnerability addressed by the patch was related to the functionality of the relay and did not include a potential vulnerability that could be used to compromise other devices on the network. The second instance was minimal, because per the Entity, the firewalls [REDACTED]. The third instance was minimal because per the Entity, the devices associated to the patch sources are [REDACTED] and the noncompliance was limited to not documenting the extension of the mitigation plan. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) added a security patch associated to the relay and mitigation plan; 2) performed an extent of condition review, which confirmed no additional relays were impacted on other mitigation plans created by the involved employee; and 3) the relay Administrator and Supervisor approved an additional step to add to the device management document under the commissioning section. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) utilized the correctly identified patch source for the firewalls of issue and performed an evaluation for applicable security patches; 2) reinforced the importance of utilizing the specified patch source listed and to update the patch source if needed, the reinforcement training was conducted at a patch review meeting; and 3) updated the firewall device management document to include clear instructions for reviewing full and interim patch releases for security patch applicability. <p>To mitigate the third instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the mitigation plan implementation date with approval from the Senior CIP Manager; and 2) included the next upcoming mitigation plan due dates in the minutes of its monthly patch meeting to ensure mitigation plan dates are visible to the patching team. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020272	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	01/31/2018	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 violation.)			<p>On June 5, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2. [REDACTED]</p> <p>The cause of the noncompliance was the Entity's patch management process lacked sufficient detail and did not include a source that the Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source existed.</p> <p>The issue began on July 1, 2016, when CIP-007-6-2 became enforceable and the Entity failed to include one of its sources to track for the release of cyber security patches in its patch management process documentation, and ended on January 31, 2018 when the missing source was added to the patch management process documentation.</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 the Entity, the noncompliance impacted a single PACS system. Additionally, the Entity states that no patches were released during the period of noncompliance, Finally, the Entity reports that it utilizes a third party to track its PACS updates and that third party was tracking the source despite the Entity missing it in its documentation. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) created new enterprise-wide CIP-007-6 R2 patch management processes that include documenting the source used to track for Cyber Security updates; 2) developed and documented patch management controls to ensure repeatable and sustainable processes, and templates to capture evidence for CIP-007-6 R2 completion; and 3) developed training materials for the revised patch management processes and completed training with all responsible 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
SPP2018019377	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	09/05/2016	02/19/2018	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 violation.)			<p>On March 12, 2018, the Entity submitted a Self-Certification stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2. The Self-Certification included two issues.</p> <p>For the first issue, during a review of the CIP-007-6 R2 documentation the Entity discovered that there were 10 instances of patches failing to be evaluated within the required 35 days. These patches were all evaluated within one to 11 days late. This issue began on September 5, 2016, when the first patch evaluation was not completed on time and ended on February 19, 2018 when the last patch was evaluated.</p> <p>For the second issue, a Subject Matter Expert (SME) failed to check the “Applicable” check box after a patch evaluation in the Entity’s patch management workflow and a patch was not applied as required by CIP-007-6 R2.3. The Entity discovered the noncompliance during an active network vulnerability scan. This issue started on May 5, 2017, when an applicable patch failed to be applied, and ended on July 11, 2017 when the patch was applied.</p> <p>The cause of the noncompliance was the Entity’s process for CIP-007 patch management was inadequate in that it did not have a verification step to complete the process.</p> <p>The noncompliance was noncontiguous; the noncompliance began on September 5, 2016, when the first patch evaluation was not completed on time in the first issue and ended on February 19, 2018 when the last patch was evaluated in the first issue.</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>Per the Entity, the first issue was minimal because all patches were evaluated within 46 days of the patch release date, limiting the exposure of any individual instance. Additionally, the Entity found that nine of the 10 patches were not applicable to the system. Finally, the one patch found to be applicable was evaluated one day late, and was applied 44 days from the release of the patch, which is within the 70 days allowed under R2 (35 days in P2.2 and 35 days in P2.3). Per the Entity, the second issue was minimal because only a single server (PCA) was impacted by this issue and that server was associated with the quality assurance testing environment. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate the first issue, the Entity:</p> <ol style="list-style-type: none"> 1) evaluated all impacted patches; 2) revised automated alerts associated with the patch management remediation workflow to include additional notifications; and 3) had applicable SMEs review and revise CIP-007 process documents. <p>To mitigate the second issue, the Entity:</p> <ol style="list-style-type: none"> 1) applied the impacted patch; 2) updated its patch management form to change the “Applicable” check box to a required selection of either “Yes” or “No”; and 3) applicable SMEs reviewed and revised the CIP-007 process documents and also created a patch management process map. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020160	CIP-007-6	R3	[REDACTED] (the Entity)	[REDACTED]	02/05/2018	02/15/2018	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 10, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R3. Specifically, the Entity did not implement its documented process to mitigate against the threat of detected malicious code as required by P3.2. The Entity states that on February 5, 2018 malicious code was detected in a back-up directory. The Entity reports that it promptly determined that the detection was a false positive, but it failed to implement its process by not documenting the response. The noncompliance was caused by the Entity failing to follow its process for responding to detected malicious code.</p> <p>This noncompliance started on February 5, 2018, when the malicious code was detected, and ended on February 15, 2018, when the Entity documented the response.</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 the Entity, the malicious code detection was a false positive, the Entity promptly determined that it was a false positive, and the noncompliance can be accurately characterized as failing to document the false positive determination. Additionally, the Entity [REDACTED], the Entity [REDACTED]. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) documented the false positive determination; 2) reconfigured the impacted device to provide for enhanced alerting; 3) updated the configuration instructions in the impacted device's applicable device management document; and 4) updated the device management document to include steps to notify the security and compliance department when a new Cyber Asset, that uses the same anti-virus detection application, is added to the BES Cyber System to ensure that proper alerting is enabled. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019144	CIP-007-6	R5	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	02/05/2019	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 December 1, 2017, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5. The Self-Log included six issues.</p> <p>For the first issue, the Entity determined that it had an issue with P5.2 because it failed to satisfactorily identify and inventory generic user accounts for [REDACTED] BES Cyber Assets (BCAs) and [REDACTED] Protected Cyber Assets (PCAs) associated with medium impact BES Cyber Systems (BCS) across seven substations. All the Cyber Assets are substation relays. The PCAs were dual-categorized as low impact BCAs and PCAs. The cause of the noncompliance was that the Entity’s device management documentation lacked detail sufficient to ensure that generic accounts would be documented prior to commissioning the Cyber Assets. The issue started on July 1, 2016, when the requirement became enforceable, and ended on October 27, 2017, when missing accounts were documented and errantly documented accounts were corrected.</p> <p>For the second issue, the Entity determined that it failed to identify a default account that had a vendor-provided hardcoded password on [REDACTED] BCAs (Remote Terminal Unit Input/Output modules). The account is associated with an RTU maintenance utility, accessible exclusively via a serial maintenance port. The cause of the noncompliance was that the Entity’s device management documentation lacked detail sufficient to ensure that generic accounts would be documented prior to commissioning the Cyber Assets. The issue started on July 1, 2016, when the requirement became enforceable, and ended on November 2, 2017, when the account was documented.</p> <p>For the third issue, the Entity determined that [REDACTED] medium impact BCAs (relays) with External Routable Connectivity were found with one default password in noncompliance with P5.4. The same default password is available to other customers through manufacturer documentation. The cause of the noncompliance was the Entity’s device onboarding process documentation lacked detail sufficient to ensure that, prior to commissioning Cyber Assets, passwords would be changed from default and that complex passwords are used. The issue started on July 1, 2016, when the requirement became enforceable, and ended on July 18, 2017, when the default password was changed.</p> <p>For the fourth issue, the Entity determined that multiple computer systems still had default Basic Input/Output System (BIOS) passwords in place in noncompliance with P5.4. The cause of the noncompliance was the Entity’s device onboarding process documentation lacked detail sufficient to ensure that, prior to commissioning Cyber Assets, passwords would be changed from default and that complex passwords are used. The issue started on July 1, 2016, when the requirement became enforceable, and ended on August 30, 2018, when the passwords were changed.</p> <p>For the fifth issue, the Entity determined that multiple computer systems did not have sufficiently complex BIOS passwords in place. The cause of the noncompliance was the Entity’s device onboarding process documentation lacked detail sufficient to ensure that, prior to commissioning Cyber Assets, passwords would be changed from default and that complex passwords are used. The issue started on July 1, 2016, when the requirement became enforceable, and ended on August 30, 2018, when the passwords were changed.</p> <p>For the sixth issue, the Entity determined that multiple computer systems failed to change their BIOS passwords within 15 months in noncompliance with P5.6. The cause of the noncompliance was the Entity’s procedural documentation lacked detail sufficient to ensure that passwords for password-only authentication for interactive user access would be changed at least once every 15 calendar months. The issue started on October 1, 2017, which is 15 months after the date when the requirement became enforceable, and ended on February 5, 2019, when a Technical Feasibility Exception (TFE) was submitted and approved.</p> <p>The issue started on July 1, 2016, when the requirement became enforceable, and ended on February 5, 2019, when a TFE was submitted and approved for the sixth issue.</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>Per the Entity, the first issue was minimal because with the exception of three relays, all vendor-supplied default passwords for the reported relays were changed from their default prior to July 1, 2016. The three excepted relays were included in the third issue. Per the Entity, the second issue was minimal because the account cannot be disabled and its password is hardcoded; additionally, the account cannot be accessed via routable protocol as it is accessed exclusively via a serial maintenance port. Per the Entity, the third issue was minimal because the affected relays were network accessible but that level of access cannot be achieved without elevating through two other levels of authentication and the issue was limited to three protective relays. Per the Entity, the fourth, fifth, and sixth issue are minimal because the noncompliance affected only BIOS accounts. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the first issue, the Entity:</p> <p>1) documented generic accounts; and</p>					

2) revised the commissioning section of its relay device management document and added the reference information necessary to ensure that the relay account information is included for all relay accounts.

To mitigate the second issue, the Entity:

- 1) documented the default account for the affected BCAs;
- 2) determined the extent of condition by a review of all in-scope Cyber Assets to identify if this situation existed elsewhere; and
- 3) revised the pertinent section of its device management documentation and informed the responsible personnel about it.

To mitigate the third issue, the Entity:

- 1) changed the passwords;
- 2) updated the onboarding process to include additional details to ensure all passwords are changed from default; and
- 3) trained applicable personnel on the updated onboarding procedure and reiterated the requirement regarding default passwords.

To mitigate the fourth issue, the Entity:

- 1) changed the passwords from the default setting;
- 2) updated onboarding procedures to include additional details to ensure all passwords are changed from default; and
- 3) trained applicable personnel on the updated onboarding procedure and reiterated the requirement regarding default passwords.

To mitigate the fifth noncompliance, the Entity:

- 1) changed the passwords to be complex;
- 2) updated onboarding process to include additional details to ensure all passwords are set to complex; and
- 3) trained applicable personnel on the updated onboarding procedure and reiterated the requirement regarding complex passwords.

To mitigate the sixth noncompliance, the Entity:

- 1) filed a TFE;
- 2) changed the BIOS passwords in all affected devices where changing of passwords was feasible;
- 3) updated process documentation to include additional details to ensure all passwords which can be changed are changed periodically; and
- 4) responsible team reviewed changes to all procedural level documentation.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021544	CIP-009-6	R2	[REDACTED] (the Entity)	[REDACTED]	10/01/2018	02/07/2019	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 10 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-009-6 R2. The Entity states that following the performance of a vulnerability assessment, it determined that three recovery plans for systems that support the SCADA system were not tested within 15 calendar months of the previous test.</p> <p>The cause of the noncompliance was that the Entity's task notification system did not specifically identify the recovery plans that required testing, resulting in some plans being overlooked.</p> <p>The issue started on October 1, 2018, 16 calendar months after the previous test completion, and ended on February 7, 2019 when a tabletop exercise was conducted to test the three recovery plans.</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 issue was minimal risk because seven of ten recovery plans were tested within 15 calendar months. Further, the three recovery plans were related to Cyber Assets that were not part of a BES Cyber System. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) tested the three overdue recovery plans; and 2) reconfigured the task notification system so that each recovery plan has its own reminder. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2018019379	CIP-010-2	R3	[REDACTED] (the Entity)	[REDACTED]	11/28/2017	12/01/2017	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 violation.)			<p>On March 12, 2018, the Entity submitted a Self-Certification stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R3. Specifically, the Entity deployed a BES Cyber Asset (workstation) without first conducting an active vulnerability assessment of the device as required by P3.3.</p> <p>The cause of the noncompliance was a result from a failure of the Entity to follow its process for adding a new Cyber Asset to the production environment; an employee was not aware that a previously decommissioned SCADA/EMS asset was considered a new asset and not a like-kind replacement.</p> <p>The noncompliance began on November 28, 2017, when a vulnerability assessment was not completed prior to adding a Cyber Asset to the production environment, and ended on December 1, 2017, when the Cyber Asset was removed from the production 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. Per the Entity, this issue was limited to a single BES Cyber Asset and limited to four days. The Entity also stated that the impacted Cyber Asset had previously been deployed as a BES Cyber Asset and since its decommissioning had been stored in a controlled environment within the SCADA/EMS PSP and had not been connected to the SCADA/EMS network while it was in storage. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) removed the Cyber Asset from the SCADA/EMS production environment; 2) reviewed the interpretation of “like-kind replacement” with applicable personnel; and 3) completed an in-depth review of Change Management processes that included updating process documentation and a walk through for “like-kind replacement” versus “new asset” determinations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021340	CIP-003-6	R1; R1.2	[REDACTED]	[REDACTED]	2/23/2019	4/3/2019	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] (the entity) submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-003-6 R1 (1.2.). The entity failed to review and approve documented cyber security policies within the 15-calendar month interval.</p> <p>As part of the preparation for a [REDACTED] compliance audit, the entity hired a third-party consultant to perform an independent review of the NERC Compliance Program. As part of the review, the consultant discovered that the compliance program was implemented on [REDACTED] prior to the NERC Registration Date for the entity. Since the compliance program began in [REDACTED] the consultant reviewed the compliance calendar to ensure all required tasks were identified and had been accomplished within the defined intervals.</p> <p>The plant engineer at the entity was working with the contracted operating company on the development and oversight of the NERC Compliance Program. As part of the implementation of the compliance program, the plant engineer developed a compliance calendar with the required tasks, intervals, and due dates outlined by the applicable reliability standards.</p> <p>Shortly after commissioning, the plant engineer quit, leaving the position vacant until a new plant engineer could be hired [REDACTED]. The compliance calendar was completed but had not been uploaded into the [REDACTED] and as a result, the CIP Senior Manager did not receive notification to complete the review of the cyber security policies required in R1.2.1 and R1.2.4 within the 15-calendar month interval. Several meetings were held between the departure of the original plant engineer and the discovery of the violation but the early completion of the initial verification relative to asset registration, meant that the upcoming due date of the second verification/signature was earlier than expected.</p> <p>This noncompliance started on February 23, 2019, when the entity failed to review the documented cyber security policies within 15 months of its compliance program implementation. The noncompliance ended on April 3, 2019, when the entity completed the review and approval.</p> <p>The root cause of this noncompliance was an insufficient process to ensure the continuity of responsibilities during personnel turnover.</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>Specifically, failing to review cyber security policies of Bulk Electric System (BES) Cyber Systems could lead to inadequate or non-existent protective measures of applicable CIP Standards. This could potentially result in a compromise or misuse of BES Cyber Systems affecting real-time operation of the BPS.</p> <p>With the departure of the plant engineer tasked with the development and implementation of the compliance program at the entity, oversight was provided by the [REDACTED] and the [REDACTED]. The incoming plant engineer did not have prior experience with NERC, thus some oversight overlap occurred between the interim oversight and the new plant engineer until the compliance calendar could be incorporated into [REDACTED].</p> <p>At the time of the noncompliance, the entity had already implemented an annual review of the NERC Compliance Program to ensure that required tasks, intervals, and dates correspond with the compliance calendar and standard requirements had been accomplished throughout the year. Additionally, the duration of the noncompliance was short and the discrepancy between the NERC registration date and the implementation of the compliance program led to mistaken assumptions about when the review and approval was due.</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 prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the review and approval of cyber security policies; 2) incorporated the compliance calendar into the [REDACTED]; 3) scheduled notification reminders for the CIP senior manager and additional oversight personnel; and 4) instituted a monthly NERC deadline matrix to be included in reports for plant managers and owners. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021341	CIP-002-5.1a	R2	[REDACTED]	[REDACTED]	2/23/2019	4/3/2019	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 April 9, 2019, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-002-5.1a R2. The entity failed to perform the review and approval of the BES Cyber System Categorization identification within the 15-calendar month interval.</p> <p>As part of the preparation for a [REDACTED] compliance audit, the entity hired a third-party consultant to perform an independent review of the NERC Compliance Program. As part of the review, the consultant discovered that the compliance program was implemented on [REDACTED] prior to the NERC Registration Date for the entity. Since the compliance program began in [REDACTED] the consultant reviewed the compliance calendar to ensure all required tasks were identified and had been accomplished within the defined intervals.</p> <p>The plant engineer at the entity was working with the contracted operating company on the development and oversight of the NERC Compliance Program. As part of the implementation of the compliance program, the plant engineer developed a compliance calendar with the required tasks, intervals, and due dates outlined by the applicable reliability standards.</p> <p>Shortly after commissioning, the plant engineer quit, leaving the position vacant until a new plant engineer could be hired [REDACTED]. The compliance calendar was completed but had not been uploaded into the [REDACTED] and as a result, the CIP Senior Manager did not received notification to complete the review of the identifications in Requirement R1 within the 15-calendar month interval. Several meetings were held between the departure of the original plant engineer and the discovery of the violation but the early completion of the initial verification relative to asset registration, meant that the upcoming due date of the second verification/signature was earlier than expected.</p> <p>This noncompliance started on February 23, 2019, when the entity failed to perform the review and approval of BES Cyber System Categorization identification within 15 months of its compliance program implementation. The noncompliance ended on April 3, 2019, when the entity completed the review and approval of the identifications.</p> <p>The root cause of this noncompliance was an insufficient process to ensure responsibilities continuity during personnel turnover.</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>Specifically, failing to review and approve BES System Categorization identifications could result in an incorrect categorization of Bulk Electric System (BES) Cyber Systems, which could lead to inadequate or non-existent protective measures of applicable CIP Standards. This could potentially result in a compromise or misuse of BES Cyber Systems affecting real-time operation of the BPS.</p> <p>With the departure of the plant engineer tasked with the development and implementation of the compliance program at the entity, oversight was provided by the [REDACTED] and the [REDACTED]. The incoming plant engineer did not have prior experience with NERC, thus some oversight overlap occurred between the interim oversight and the new plant engineer until the compliance calendar could be incorporated into [REDACTED].</p> <p>At the time of the noncompliance, the entity had already implemented an annual review of the NERC Compliance Program to confirm that required tasks, intervals, and dates correspond with the compliance calendar and standard requirements had been accomplished throughout the year. Additionally, the duration of the noncompliance was short and largely resulted from confusion caused by the difference between the NERC registration date and the implementation of the compliance program that led to mistaken assumptions about when the review and approval was due.</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 prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the review and approval of the BES Cyber System Categorization identification; 2) incorporated the compliance calendar into the [REDACTED]; 3) scheduled notification reminders for the CIP senior manager and additional oversight personnel; and 4) instituted a monthly NERC deadline matrix to be included in reports for plant managers and owners. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021297	CIP-004-6	R3; R3.5	[REDACTED]	[REDACTED]	2/24/2019	2/25/2019	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 April 3, 2019, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-004-6 R3; R3.5. Specifically, the entity failed to ensure that individuals with electronic or authorized unescorted physical access had a Personnel Risk Assessment (PRA) completed within the last seven years.</p> <p>On February 23, 2019, the PRA for a contract employee expired. The expiration occurred on a Saturday. The following Monday, February 25, 2019, [REDACTED] requested confirmation from [REDACTED] that the PRA was updated or if the contractor's access was revoked. [REDACTED] responded that there was a failure to update the PRA by the expiration date or revoke access.</p> <p>A list of all individuals with authorized unescorted physical access and their respective PRA dates are maintained in a the [REDACTED] database. The dates are used to produce upcoming PRA expiration dates and PRA revocation alerts. Those in need of a PRA update are notified by email along with other individuals responsible for the requirement.</p> <p>When a PRA is not completed, the database prompts the administrators to revoke access and notify the responsible managers. When the expiration falls on a holiday or weekend, the prompt occurs on the last work day before. The system administrator did not receive a notification on Friday, February 22, 2019. After a review of the [REDACTED] database, the entity determined that the pop-up feature that alerts administrators of pending actions had been mistakenly deleted as a result of upgrade work performed by the system developer several weeks prior.</p> <p>The noncompliance began on February 24, 2019, the day after the PRA expired. The noncompliance ended on February 25, 2019, when the entity revoked access for the contract employee. A new PRA for the contract employee was completed on March 6, 2019. No issues were discovered and the contract employee's access was restored.</p> <p>The root cause of this noncompliance was an ineffective change management process that did not identify potentially adverse consequences of work conducted on the [REDACTED] access database.</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. Failing to complete a PRA could result in an individual with access having unidentified criminal or other negative history.</p> <p>However, the issue identified and subsequently corrected was on the Physical Access Control System (PACS), which is separate from the Energy Management System. The PACS does not control or operate the Bulk Electric System. The individual did not access the PACS (physically or electronically) during the duration of the noncompliance.</p> <p>The contract employee was current on NERC CIP training and was otherwise in good standing with the entity. Once the PRA was completed, no derogatory information was discovered. The risk was minimal due to the short duration (two days) of the noncompliance and the risk was reduced further by the internal compliance program that quickly identified and corrected the noncompliance.</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 are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) revoked physical and cyber access for the contract employee; 2) re-installed and tested the database alert feature for functionality; 3) reviewed the database to ensure no other PRA dates were missed; 4) confirmed the contractor did not physically access any NERC areas or log in to any PACS; 5) reviewed and reinforced NERC CIP responsibilities with the contractor; and 6) developed a Change Management Process to identify and correct changes that could result in adverse effects on the [REDACTED] before being put into production. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021396	CIP-007-6	R4; R4.3; R4.4	[REDACTED]	[REDACTED]	7/13/2018	3/5/2019	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 April 18, 2019, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-007-6 R4. The entity failed to retain logs for at least 90 days and failed to review a summarization or sampling of logged events no greater than 15 days to identify Cyber Security Incidents.</p> <p>During a system upgrade, new network attached storage was connected to the [REDACTED] BES Cyber Systems residing at the Primary and Alternate Control Centers. During the installation process, the entity verified that the newly installed assets were communicating successfully with the asset tracking system. However, event logging to that system was not verified during the commissioning performed with the entity's main Energy Management System (EMS) vendor and syslog forwarding was not configured. As a result, the follow-up testing and evidence collection verified only the connection to the asset tracking system itself.</p> <p>The noncompliance was discovered during the [REDACTED] Analysis of the meeting's discussions and action plans led to the discovery of the issue. The two clustered pairs of assets in question had local logging enabled, but were not sending event logs to a designated syslog server. Therefore, the logs were not retained in accordance with the 90-day retention requirements or included in the summarization/sampling process.</p> <p>This noncompliance started on July 13, 2018, when the newly installed assets were installed without event logging or syslog forwarding. The noncompliance ended on March 5, 2019, when the system logging was configured for export to the asset tracking system.</p> <p>The root cause of this noncompliance was management provided insufficient controls within the verification procedure of Security Event Monitoring.</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 retain event logs for 90 days and failing to review a sample of the events could potentially cause Cyber Security incidents to go undetected or impede the entity's ability to investigate incidents.</p> <p>However, the assets were located within an Electronic Security Perimeter (ESP) and were secured by the documented Electronic Access Points (EAPs) into the ESP and [REDACTED]. The assets are located within a Physical Security Perimeter (PSP) with [REDACTED] and monitored physical access. The entity has limited cyber and physical access to BES Cyber Assets and those with access have prerequisites (PRAs and training). Additionally, local logging was occurring, though it was not stored for 90 days.</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 prior instances with relevant underlying causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) configured system logging on both clustered pairs; 2) verified that event logs are being correctly forwarded to asset tracking system; 3) reviewed the issue with analysts performing implementation of new assets; and 4) modified internal procedure to include more detailed checklists specifying how each verification should be conducted. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021287	CIP-006-6	R2	[REDACTED]	[REDACTED]	1/9/2019	1/9/2019	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 1, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it was in noncompliance with CIP-006-6 R2 (2.1.) An internal compliance investigation determined that the entity failed to provide continuous escorted access of a visitor within a Physical Security Perimeter (PSP).</p> <p>On January 9, 2019, a company employee visited the PSP for training purposes. While there, the employee needed to leave the PSP and was escorted out. When the employee returned, the employee was given access without a continuous escort. The employee gained access when other employees leaving held the door for the visitor without realizing that the employee was an unescorted visitor. The visitor was given access to a hallway within the PSP. The visitor had no additional access except to exit back out through the PSP Entry/Exit point.</p> <p>A security guard quickly noticed the event and resolved the issue. As a result, the entity completed an internal investigation reviewing visitor logs and video footage and determined that a noncompliance had occurred. The duration of the unescorted access lasted approximately one minute. The visitor had no access to any devices during the noncompliance.</p> <p>This noncompliance began on January 9, 2019 and ended the same day. The duration of the noncompliance was approximately one minute.</p> <p>The entity reviewed its escort policies and procedures and determined they were consistent with other utilities. The entity determined that the cause of this noncompliance was a momentary lapse in situational awareness by the employee who held the door. The employee failed to enforce the escort policy and security procedure.</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 provide continuous escort within a PSP, the individual entering 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>However, the entity control centers containing BES Cyber Systems can only be accessed with additional or separate key card controls. The employee did not have access to areas that house BES Cyber Systems for the brief period of time the employee was unescorted. Additionally, other detective and corrective controls reduced the risk by quickly identifying the unescorted visitor and correcting the issue immediately.</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) benchmarked the entity program with other similar utilities regarding their interpretation of “continuous escorted access” and their visitor escorting programs; 2) reviewed the escort policy and security procedure and determined that no revisions were necessary; and 3) distributed the escort policy and security procedure for review by all [REDACTED] employees to ensure policy awareness. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021298	CIP-005-5	R1.	[REDACTED]	[REDACTED]	2/7/2019	2/8/2019	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 April 5, 2019, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-005-5 R1 (1.2). The entity failed to ensure all External Routable Connectivity (ERC) was through an identified Electronic Access Point (EAP).</p> <p>This noncompliance started on February 7, 2019, when the entity failed to ensure all ERC was through an identified EAP. The noncompliance ended on February 8, 2019, when the entity discovered the issue and disconnected the appliance from their network.</p> <p>Specifically, while working on a project to upgrade software, an appliance was directly connected to a network within the ESP. The connection bypassed the firewall (the EAP) and remained in place for 19.5 hours. The connection was removed after being identified in a post-job briefing.</p> <p>The root cause of this noncompliance was a narrow and informal pre-job briefing that did not provide sufficient focus on unplanned tasks.</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, had a malicious actor gained access to the application, the threat actor would have the ability to identify vulnerabilities in the BES Cyber System, map the networks and potentially exploit them.</p> <p>However, connection to the network where the appliance resides requires [REDACTED]. The appliance [REDACTED] and a review of network flows captured by the Intrusion Detection System during the time of the noncompliance showed that there were no unexpected connections to or from the configured interfaces related to this on-going work.</p> <p>All of the affected Cyber Assets are located within a PSP, and the noncompliance was detected and resolved in less than 24 hours.</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 prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disconnected the appliance from the BES ESP networks; 2) implemented a more effective pre-job briefing with a wider scope and emphasis on written work plans; and 3) addressed unplanned tasks with a checklist covering each of the major IT disciplines. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020559	CIP-010-2	R1	[REDACTED]	[REDACTED]	6/9/2018	6/21/2018	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 12, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-010-2 R1.</p> <p>On June 21, 2018, as a result of a bi-weekly review, the entity discovered deviations due to software installed on a Protected Cyber Asset (PCA) on May 10, 2018, and May 21, 2018 that was not added to the PCA's existing baseline.</p> <p>As background, on May 7, 2018, the entity made a change that altered [REDACTED] the PCA. This change resulted in a failure in the process that sent the PCA's software inventory to the baseline management tool. This process failure resulted in baseline data not being properly updated in the baseline management tool for the PCA for the software changes implemented on May 10, 2018, and May 21, 2018. Therefore, the entity failed to update the baseline configuration on a PCA that supports [REDACTED] within 30 days of completing a change.</p> <p>The root cause of this noncompliance was an ineffective verification process when the entity made a change [REDACTED] for the affected PCA resulting in a process communication issue which failed to update the baseline management tool.</p> <p>This noncompliance involves the management practices of asset and configuration management and implementation. Asset and configuration management is involved because the entity's failure centered on an inability to update its baseline configurations for a PCA. Implementation is involved [REDACTED]</p> <p>This noncompliance started on June 9, 2018, thirty days after the entity first made a change that resulted in a baseline change that was not updated, and ended on June 21, 2018, when the entity documented the missed baseline changes.</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 instance of noncompliance is that an entity may be operating off of stale data due to a failure to update a baseline which could result in harm to the Bulk Power System (BPS). The risk is minimized because the noncompliance was limited to a single PCA. The change at issue that was not timely updated in the baseline was appropriately authorized and had been tested for changes to security controls. Further lessening the risk, the noncompliance was discovered and remedied promptly via the entity's internal controls. The duration was just 12 days. The entity's review of the noncompliance on June 21, 2018 found no unauthorized deviations. 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. ReliabilityFirst did not consider the prior noncompliances repeat infractions warranting alternate disposition because of the different root causes between the prior noncompliances and the instant noncompliance. Additionally, all of these are high frequency conduct noncompliances for which the entity has demonstrated the ability to quickly identify and correct noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) corrected the process that sends PCA's software inventory to the baseline management tool. The entity also updated the baseline for the affected device with the baseline deviations that had occurred between May 7, 2018 and June 21, 2018; 2) performed an extent of condition to examine the two other servers of the same device type using the same process. These servers were unaffected; 3) developed a new preventative control for [REDACTED] devices to alert if data is not received by the baseline tool in a timely manner; 4) developed a representative system for testing changes on the Cyber Asset and Cyber Assets of the same device type to ensure baseline processes are not adversely impacted before applying changes to applicable production devices; 5) developed training for the enhancement to the control and the new representative system for testing; and 6) implemented enhancements to the preventative control, established the representative system, and trained affected personnel. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020560	CIP-010-2	R2	[REDACTED]	[REDACTED]	6/11/2018	6/21/2018	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 12, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-010-2 R2.</p> <p>The entity failed to monitor at least once every 35 calendar days for changes to the baseline configuration on a Protected Cyber Asset (PCA) that supports High Impact Bulk Electric System Cyber Systems. On June 21, 2018, while performing a bi-weekly review of baseline deviations, the entity discovered that baseline data was not being refreshed in the baseline management tool for one PCA.</p> <p>As background, on May 7, 2018, the entity made an alteration which changed the [REDACTED] the PCA. This change resulted in a failure in the process that sent the PCA's software inventory to the baseline management tool. This process failure resulted in baseline data not being properly updated in the baseline management tool for changes made to the PCA. As a result, the entity failed to monitor a PCA for changes to the baseline configuration for a 45 day period (ten days too long) ending June 21, 2018.</p> <p>The root cause of this noncompliance was an ineffective verification process when the entity made a change from one automated patching source to another for the affected PCA resulting in a process communication issue that prevented monitoring in the baseline management tool.</p> <p>This noncompliance involves the management practices of asset and configuration management and implementation. Asset and configuration management is involved because the entity's failure centered on an inability to monitor its baseline configurations for a PCA. Implementation management is involved because the failure resulted from the change of one automated patching source to another without confirming that the change was integrated effectively.</p> <p>This noncompliance started on June 11, 2018, 35 days after the entity changed the baseline configuration on a PCA without monitoring and ended on June 21, 2018, when the entity reviewed the baseline configuration of the impacted PCA.</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 instance of noncompliance is lack of awareness of deviations that indicate a potential compromise of the asset. The risk is lessened because the noncompliance involved only one PCA which limits the breadth of the attack vector. Further limiting the risk, the duration of the noncompliance was limited to just 10 days. Finally, a review of the baseline configuration was performed on June 21, 2018 and the entity discovered no unauthorized deviations. 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. ReliabilityFirst did not consider the prior noncompliances repeat infractions warranting alternate disposition because of the different root causes between the prior noncompliances and the instant noncompliance. Additionally, all of these are high frequency conduct noncompliances for which the entity has demonstrated the ability to quickly identify and correct noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) corrected the process that sends PCA's software inventory to the baseline management tool. The entity also updated the baseline for the affected device with the baseline deviations that had occurred between May 7, 2018 and June 21, 2018; 2) performed an extent of condition to examine the two other servers of the same device type using the same process. These servers were unaffected; 3) developed a new preventative control for [REDACTED] devices to alert if data is not received by the baseline tool in a timely manner; 4) developed a representative system for testing changes on the Cyber Asset and Cyber Assets of the same device type to ensure baseline processes are not adversely impacted before applying changes to applicable production devices; 5) developed training for the enhancement to the control and the new representative system for testing; and 6) implemented enhancements to the preventative control, established the representative system, and trained affected personnel. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020370	CIP-004-6	R5	[REDACTED]	[REDACTED]	4/26/2018	7/10/2018	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 August 31, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. The entity identified two cases where an individual's access was not revoked within 24 hours of termination. These cases involve two contractors who were assigned to a project that contained information related to [REDACTED]. Each case is described separately below.</p> <p>First, on April 30, 2018, an entity supervisor learned that a contractor had resigned on April 25, 2018. Although a project team member collected the contractor's badge and laptop on April 25, 2018, the contractor still retained electronic remote access to the entity network, which provided access to the project's [REDACTED] containing Bulk Electric System Cyber Security Information (BCSI). Immediately after discovering that the contractor's account had not been disabled, the supervisor requested removal of the contractor from the relevant system, which was completed on April 30, 2018.</p> <p>Second, on July 6, 2018, another contractor working on the same project resigned and the entity supervisor was not notified until July 10, 2018. Although the vendor company collected the contractor's badge and laptop on July 6, 2018, he still retained electronic remote access to the project's [REDACTED] containing BCSI. Immediately after the vendor company notified the entity's supervisor of the resignation on July 10, 2018, he contacted the appropriate personnel to disable the contractor's electronic access.</p> <p>The root cause of each instance is as follows. For the first instance, the root cause was that the vendor company provided only verbal notice to the entity project team of the personnel change, which violated the relevant protocol, and the entity supervisor failed to take action on the verbal notice. For the second instance, the root cause was that the vendor company failed to notify the entity project team of the change in personnel. These root causes involve the management practice of external interdependencies, in that the noncompliance arose out of issues with the entities' ability to manage the performance of an external company.</p> <p>This noncompliance has two durations, one for each instance. The first instance started on April 26, 2018, when the entity was required to have removed the contractor's electronic access, and ended on April 30, 2018, when the entity actually removed his access. The second instance started on July 7, 2018, when the entity was required to have removed the contractor's access, and ended on July 10, 2018, when the entity actually removed his 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 (BPS) based on the following factors. The risk posed by failing to remove an individual's electronic access after termination is that the individual could use that access to cause harm to the entity's network and the BPS. This risk was mitigated in this case by the following factors. First, both contractors were trusted individuals with current CIP training and valid Personnel Risk Assessments, who left their employer on good terms. Second, the contractors retained electronic access for 3 or 4 days, which limited the amount of time that they could have utilized the access inappropriately. Third, the contractors were unaware that they still retained electronic access, reducing the likelihood that they would have attempted to utilize it. ReliabilityFirst also notes that the entity confirmed that neither contractor attempted to access their accounts during the time of 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 noncompliances arose from different causes or involve conduct that ReliabilityFirst has determined constitutes high-frequency conduct that the entity has demonstrated the ability to quickly identify and correct.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disabled user 1's contractor account access rights that remained in the access system; 2) disabled user 2's contractor account access rights that remained in the access system; 3) distributed reminder emails to all project team members containing the contractor termination process; 4) met with user 1 and user 2's supervisor to review the contractor termination process; 5) reviewed the contractor termination process with supervisors with contractors reporting to them and contractor leads within the project; and 6) reviewed all contractors both active and terminated from inception of the project on [REDACTED] that were given access to the [REDACTED] to verify that the end date within the access management tool accurately reflects the proper off-boarding date for the resource and to confirm timely revocation if an end date for a terminated contractor is incorrect. <p>ReliabilityFirst 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
RFC2018020373	CIP-004-6	R5	[REDACTED]	[REDACTED]	4/26/2018	7/10/2018	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 August 31, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. The entity identified two cases where an individual's access was not revoked within 24 hours of termination. These cases involve two contractors who were assigned to a project that contained information related to [REDACTED]. Each case is described separately below.</p> <p>First, on April 30, 2018, an entity supervisor learned that a contractor had resigned on April 25, 2018. Although a project team member collected the contractor's badge and laptop on April 25, 2018, the contractor still retained electronic remote access to the entity network, which provided access to the project's [REDACTED] containing Bulk Electric System Cyber Security Information (BCSI). Immediately after discovering that the contractor's account had not been disabled, the supervisor requested removal of the contractor from the relevant system, which was completed on April 30, 2018.</p> <p>Second, on July 6, 2018, another contractor working on the same project resigned and the entity supervisor was not notified until July 10, 2018. Although the vendor company collected the contractor's badge and laptop on July 6, 2018, he still retained electronic remote access to the project's [REDACTED] containing BCSI. Immediately after the vendor company notified the entity supervisor of the resignation on July 10, 2018, he contacted the appropriate personnel to disable the contractor's electronic access.</p> <p>The root cause of each instance is as follows. For the first instance, the root cause was that the vendor company provided only verbal notice to the entity project team of the personnel change, which violated the relevant protocol, and the entity supervisor failed to take action on the verbal notice. For the second instance, the root cause was that the vendor company failed to notify the entity project team of the change in personnel. These root causes involve the management practice of external interdependencies, in that the noncompliance arose out of issues with the entities' ability to manage the performance of an external company.</p> <p>This noncompliance has two durations, one for each instance. The first instance started on April 26, 2018, when the entity was required to have removed the contractor's electronic access, and ended on April 30, 2018, when the entity actually removed his access. The second instance started on July 7, 2018, when the entity was required to have removed the contractor's access, and ended on July 10, 2018, when the entity actually removed his 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 (BPS) based on the following factors. The risk posed by failing to remove an individual's electronic access after termination is that the individual could use that access to cause harm to the entity's network and the BPS as a whole. This risk was mitigated in this case by the following factors. First, both contractors were trusted individuals with current CIP training and valid Personnel Risk Assessments, who left their employer on good terms. Second, the contractors retained electronic access for 3 or 4 days, which limited the amount of time that they could have utilized the access inappropriately. Third, the contractors were unaware that they still retained electronic access, reducing the likelihood that they would have attempted to utilize it. ReliabilityFirst also notes that the entity confirmed that neither contractor attempted to access their accounts during the time of 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 noncompliances arose from different causes or involve conduct that ReliabilityFirst has determined constitutes high-frequency conduct that the entity has demonstrated the ability to quickly identify and correct.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disabled user 1's contractor account access rights that remained in the access system; 2) disabled user 2's contractor account access rights that remained in the access system; 3) distributed reminder emails to all project team members containing the contractor termination process; 4) met with user 1 and user 2's supervisor to review the contractor termination process; 5) reviewed the contractor termination process with supervisors with contractors reporting to them and contractor leads within the project; and 6) reviewed all contractors both active and terminated from inception of the project on [REDACTED] that were given access to the [REDACTED] to verify that the end date within the access management tool accurately reflects the proper off-boarding date for the resource and confirm timely revocation if an end date for a terminated contractor is incorrect. <p>ReliabilityFirst 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
RFC2018020375	CIP-004-6	R5	[REDACTED]	[REDACTED]	4/26/2018	7/10/2018	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 August 31, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. The entity identified two cases where an individual's access was not revoked within 24 hours of termination. These cases involve two contractors who were assigned to a project that contained information related to [REDACTED]. Each case is described separately below.</p> <p>First, on April 30, 2018, an entity supervisor learned that a contractor had resigned on April 25, 2018. Although a project team member collected the contractor's badge and laptop on April 25, 2018, the contractor still retained electronic remote access to the entity network, which provided access to the project's [REDACTED] containing Bulk Electric System Cyber Security Information (BCSI). Immediately after discovering that the contractor's account had not been disabled, the supervisor requested removal of the contractor from the relevant system, which was completed on April 30, 2018.</p> <p>Second, on July 6, 2018, another contractor working on the same project resigned and the entity supervisor was not notified until July 10, 2018. Although the vendor company collected the contractor's badge and laptop on July 6, 2018, he still retained electronic remote access to the project's [REDACTED] containing BCSI. Immediately after the vendor company notified the entity supervisor of the resignation on July 10, 2018, he contacted the appropriate personnel to disable the contractor's electronic access.</p> <p>The root cause of each instance is as follows. For the first instance, the root cause was that the vendor company provided only verbal notice to the entity project team of the personnel change, which violated the relevant protocol, and the entity supervisor failed to take action on the verbal notice. For the second instance, the root cause was that the vendor company failed to notify the entity project team of the change in personnel. These root causes involve the management practice of external interdependencies, in that the noncompliance arose out of issues with the entities' ability to manage the performance of an external company.</p> <p>This noncompliance has two durations, one for each instance. The first instance started on April 26, 2018, when the entity was required to have removed the contractor's electronic access, and ended on April 30, 2018, when the entity actually removed his access. The second instance started on July 7, 2018, when the entity was required to have removed the contractor's access, and ended on July 10, 2018, when the entity actually removed his 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 (BPS) based on the following factors. The risk posed by failing to remove an individual's electronic access after termination is that the individual could use that access to cause harm to the entity's network and the BPS as a whole. This risk was mitigated in this case by the following factors. First, both contractors were trusted individuals with current CIP training and valid Personnel Risk Assessments, who left their employer on good terms. Second, the contractors retained electronic access for 3 or 4 days, which limited the amount of time that they could have utilized the access inappropriately. Third, the contractors were unaware that they still retained electronic access, reducing the likelihood that they would have attempted to utilize it. ReliabilityFirst also notes that the entity confirmed that neither contractor attempted to access their accounts during the time of 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 noncompliances arose from different causes or involve conduct that ReliabilityFirst has determined constitutes high-frequency conduct that the entity has demonstrated the ability to quickly identify and correct.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disabled user 1's contractor account access rights that remained in the access system; 2) disabled user 2's contractor account access rights that remained in the access system; 3) distributed reminder emails to all project team members containing the contractor termination process; 4) met with user 1 and user 2's supervisor to review the contractor termination process; 5) reviewed the contractor termination process with supervisors with contractors reporting to them and contractor leads within the project; and 6) reviewed all contractors both active and terminated from inception of the project on [REDACTED] that were given access to the [REDACTED] to verify that the end date within the access management tool accurately reflects the proper off-boarding date for the resource and confirm timely revocation if an end date for a terminated contractor is incorrect. <p>ReliabilityFirst 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
RFC2018020376	CIP-004-6	R5			4/26/2018	7/10/2018	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 August 31, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. The entity identified two cases where an individual's access was not revoked within 24 hours of termination. These cases involve two contractors who were assigned to a project that contained information related to [REDACTED]. Each case is described separately below.</p> <p>First, on April 30, 2018, an entity supervisor learned that a contractor had resigned on April 25, 2018. Although a project team member collected the contractor's badge and laptop on April 25, 2018, the contractor still retained electronic remote access to the entity network, which provided access to the project's [REDACTED] containing Bulk Electric System Cyber Security Information (BCSI). Immediately after discovering that the contractor's account had not been disabled, the supervisor requested removal of the contractor from the relevant system, which was completed on April 30, 2018.</p> <p>Second, on July 6, 2018, another contractor working on the same project resigned and the entity supervisor was not notified until July 10, 2018. Although the vendor company collected the contractor's badge and laptop on July 6, 2018, he still retained electronic remote access to the project's [REDACTED] containing BCSI. Immediately after the vendor company notified the entity supervisor of the resignation on July 10, 2018, he contacted the appropriate personnel to disable the contractor's electronic access.</p> <p>The root cause of each instance is as follows. For the first instance, the root cause was that the vendor company provided only verbal notice to the entity project team of the personnel change, which violated the relevant protocol, and the entity supervisor failed to take action on the verbal notice. For the second instance, the root cause was that the vendor company failed to notify the entity project team of the change in personnel. These root causes involve the management practice of external interdependencies, in that the noncompliance arose out of issues with the entities' ability to manage the performance of an external company.</p> <p>This noncompliance has two durations, one for each instance. The first instance started on April 26, 2018, when the entity was required to have removed the contractor's electronic access, and ended on April 30, 2018, when the entity actually removed his access. The second instance started on July 7, 2018, when the entity was required to have removed the contractor's access, and ended on July 10, 2018, when the entity actually removed his 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 (BPS) based on the following factors. The risk posed by failing to remove an individual's electronic access after termination is that the individual could use that access to cause harm to the entity's network and the BPS as a whole. This risk was mitigated in this case by the following factors. First, both contractors were trusted individuals with current CIP training and valid Personnel Risk Assessments, who left their employer on good terms. Second, the contractors retained electronic access for 3 or 4 days, which limited the amount of time that they could have utilized the access inappropriately. Third, the contractors were unaware that they still retained electronic access, reducing the likelihood that they would have attempted to utilize it. ReliabilityFirst also notes that the entity confirmed that neither contractor attempted to access their accounts during the time of 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 noncompliances arose from different causes or involve conduct that ReliabilityFirst has determined constitutes high-frequency conduct that the entity has demonstrated the ability to quickly identify and correct.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disabled user 1's contractor account access rights that remained in the access system; 2) disabled user 2's contractor account access rights that remained in the access system; 3) distributed reminder emails to all project team members containing the contractor termination process; 4) met with user 1 and user 2's supervisor to review the contractor termination process; 5) reviewed the contractor termination process with supervisors with contractors reporting to them and contractor leads within the project; and 6) reviewed all contractors both active and terminated from inception of the project on [REDACTED] that were given access to the [REDACTED] to verify that the end date within the access management tool accurately reflects the proper off-boarding date for the resource and confirm timely revocation if an end date for a terminated contractor is incorrect. <p>ReliabilityFirst 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
RFC2018020377	CIP-004-6	R5	[REDACTED]	[REDACTED]	4/26/2018	7/10/2018	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 August 31, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. The entity identified two cases where an individual's access was not revoked within 24 hours of termination. These cases involve two contractors who were assigned to a project that contained information related to [REDACTED]. Each case is described separately below.</p> <p>First, on April 30, 2018, an entity supervisor learned that a contractor had resigned on April 25, 2018. Although a project team member collected the contractor's badge and laptop on April 25, 2018, the contractor still retained electronic remote access to the entity network, which provided access to the project's [REDACTED] containing Bulk Electric System Cyber Security Information (BCSI). Immediately after discovering that the contractor's account had not been disabled, the supervisor requested removal of the contractor from the relevant system, which was completed on April 30, 2018.</p> <p>Second, on July 6, 2018, another contractor working on the same project resigned and the entity supervisor was not notified until July 10, 2018. Although the vendor company collected the contractor's badge and laptop on July 6, 2018, he still retained electronic remote access to the project's [REDACTED] containing BCSI. Immediately after the vendor company notified the entity supervisor of the resignation on July 10, 2018, he contacted the appropriate personnel to disable the contractor's electronic access.</p> <p>The root cause of each instance is as follows. For the first instance, the root cause was that the vendor company provided only verbal notice to the entity project team of the personnel change, which violated the relevant protocol, and the entity supervisor failed to take action on the verbal notice. For the second instance, the root cause was that the vendor company failed to notify the entity project team of the change in personnel. These root causes involve the management practice of external interdependencies, in that the noncompliance arose out of issues with the entities' ability to manage the performance of an external company.</p> <p>This noncompliance has two durations, one for each instance. The first instance started on April 26, 2018, when the entity was required to have removed the contractor's electronic access, and ended on April 30, 2018, when the entity actually removed his access. The second instance started on July 7, 2018, when the entity was required to have removed the contractor's access, and ended on July 10, 2018, when the entity actually removed his 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 (BPS) based on the following factors. The risk posed by failing to remove an individual's electronic access after termination is that the individual could use that access to cause harm to the entity's network and the BPS as a whole. This risk was mitigated in this case by the following factors. First, both contractors were trusted individuals with current CIP training and valid Personnel Risk Assessments, who left their employer on good terms. Second, the contractors retained electronic access for 3 or 4 days, which limited the amount of time that they could have utilized the access inappropriately. Third, the contractors were unaware that they still retained electronic access, reducing the likelihood that they would have attempted to utilize it. ReliabilityFirst also notes that the entity confirmed that neither contractor attempted to access their accounts during the time of 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 noncompliances arose from different causes or involve conduct that ReliabilityFirst has determined constitutes high-frequency conduct that the entity has demonstrated the ability to quickly identify and correct.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disabled user 1's contractor account access rights that remained in the access system; 2) disabled user 2's contractor account access rights that remained in the access system; 3) distributed reminder emails to all project team members containing the contractor termination process; 4) met with user 1 and user 2's supervisor to review the contractor termination process; 5) reviewed the contractor termination process with supervisors with contractors reporting to them and contractor leads within the project; and 6) reviewed all contractors both active and terminated from inception of the project on [REDACTED] that were given access to the [REDACTED] to verify that the end date within the access management tool accurately reflects the proper off-boarding date for the resource and confirm timely revocation if an end date for a terminated contractor is incorrect. <p>ReliabilityFirst 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
RFC2018020380	CIP-004-6	R5			4/26/2018	7/10/2018	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 August 31, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. The entity identified two cases where an individual's access was not revoked within 24 hours of termination. These cases involve two contractors who were assigned to a project that contained information related to [REDACTED]. Each case is described separately below.</p> <p>First, on April 30, 2018, an entity supervisor learned that a contractor had resigned on April 25, 2018. Although a project team member collected the contractor's badge and laptop on April 25, 2018, the contractor still retained electronic remote access to the entity network, which provided access to the project's [REDACTED] containing Bulk Electric System Cyber Security Information (BCSI). Immediately after discovering that the contractor's account had not been disabled, the supervisor requested removal of the contractor from the relevant system, which was completed on April 30, 2018.</p> <p>Second, on July 6, 2018, another contractor working on the same project resigned and the entity supervisor was not notified until July 10, 2018. Although the vendor company collected the contractor's badge and laptop on July 6, 2018, he still retained electronic remote access to the project's [REDACTED] containing BCSI. Immediately after the vendor company notified the entity supervisor of the resignation on July 10, 2018, he contacted the appropriate personnel to disable the contractor's electronic access.</p> <p>The root cause of each instance is as follows. For the first instance, the root cause was that the vendor company provided only verbal notice to the entity project team of the personnel change, which violated the relevant protocol, and the entity supervisor failed to take action on the verbal notice. For the second instance, the root cause was that the vendor company failed to notify the entity project team of the change in personnel. These root causes involve the management practice of external interdependencies, in that the noncompliance arose out of issues with the entities' ability to manage the performance of an external company.</p> <p>This noncompliance has two durations, one for each instance. The first instance started on April 26, 2018, when the entity was required to have removed the contractor's electronic access, and ended on April 30, 2018, when the entity actually removed his access. The second instance started on July 7, 2018, when the entity was required to have removed the contractor's access, and ended on July 10, 2018, when the entity actually removed his 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 (BPS) based on the following factors. The risk posed by failing to remove an individual's electronic access after termination is that the individual could use that access to cause harm to the entity's network and the BPS as a whole. This risk was mitigated in this case by the following factors. First, both contractors were trusted individuals with current CIP training and valid Personnel Risk Assessments, who left their employer on good terms. Second, the contractors retained electronic access for 3 or 4 days, which limited the amount of time that they could have utilized the access inappropriately. Third, the contractors were unaware that they still retained electronic access, reducing the likelihood that they would have attempted to utilize it. ReliabilityFirst also notes that the entity confirmed that neither contractor attempted to access their accounts during the time of 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 noncompliances arose from different causes or involve conduct that ReliabilityFirst has determined constitutes high-frequency conduct that the entity has demonstrated the ability to quickly identify and correct.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disabled user 1's contractor account access rights that remained in the access system; 2) disabled user 2's contractor account access rights that remained in the access system; 3) distributed reminder emails to all project team members containing the contractor termination process; 4) met with user 1 and user 2's supervisor to review the contractor termination process; 5) reviewed the contractor termination process with supervisors with contractors reporting to them and contractor leads within the project; and 6) reviewed all contractors both active and terminated from inception of the project on [REDACTED] that were given access to the [REDACTED] to verify that the end date within the access management tool accurately reflects the proper off-boarding date for the resource and confirm timely revocation if an end date for a terminated contractor is incorrect. <p>ReliabilityFirst 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
RFC2018020381	CIP-004-6	R5			4/26/2018	7/10/2018	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 August 31, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. The entity identified two cases where an individual's access was not revoked within 24 hours of termination. These cases involve two contractors who were assigned to a project that contained information related to [REDACTED]. Each case is described separately below.</p> <p>First, on April 30, 2018, an entity supervisor learned that a contractor had resigned on April 25, 2018. Although a project team member collected the contractor's badge and laptop on April 25, 2018, the contractor still retained electronic remote access to the entity network, which provided access to the project's [REDACTED] containing Bulk Electric System Cyber Security Information (BCSI). Immediately after discovering that the contractor's account had not been disabled, the supervisor requested removal of the contractor from the relevant system, which was completed on April 30, 2018.</p> <p>Second, on July 6, 2018, another contractor working on the same project resigned and the entity supervisor was not notified until July 10, 2018. Although the vendor company collected the contractor's badge and laptop on July 6, 2018, he still retained electronic remote access to the project's [REDACTED] containing BCSI. Immediately after the vendor company notified the entity supervisor of the resignation on July 10, 2018, he contacted the appropriate personnel to disable the contractor's electronic access.</p> <p>The root cause of each instance is as follows. For the first instance, the root cause was that the vendor company provided only verbal notice to the entity project team of the personnel change, which violated the relevant protocol, and the entity supervisor failed to take action on the verbal notice. For the second instance, the root cause was that the vendor company failed to notify the entity project team of the change in personnel. These root causes involve the management practice of external interdependencies, in that the noncompliance arose out of issues with the entities' ability to manage the performance of an external company.</p> <p>This noncompliance has two durations, one for each instance. The first instance started on April 26, 2018, when the entity was required to have removed the contractor's electronic access, and ended on April 30, 2018, when the entity actually removed his access. The second instance started on July 7, 2018, when the entity was required to have removed the contractor's access, and ended on July 10, 2018, when the entity actually removed his 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 (BPS) based on the following factors. The risk posed by failing to remove an individual's electronic access after termination is that the individual could use that access to cause harm to the entity's network and the BPS as a whole. This risk was mitigated in this case by the following factors. First, both contractors were trusted individuals with current CIP training and valid Personnel Risk Assessments, who left their employer on good terms. Second, the contractors retained electronic access for 3 or 4 days, which limited the amount of time that they could have utilized the access inappropriately. Third, the contractors were unaware that they still retained electronic access, reducing the likelihood that they would have attempted to utilize it. ReliabilityFirst also notes that the entity confirmed that neither contractor attempted to access their accounts during the time of 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 noncompliances arose from different causes or involve conduct that ReliabilityFirst has determined constitutes high-frequency conduct that the entity has demonstrated the ability to quickly identify and correct.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disabled user 1's contractor account access rights that remained in the access system; 2) disabled user 2's contractor account access rights that remained in the access system; 3) distributed reminder emails to all project team members containing the contractor termination process; 4) met with user 1 and user 2's supervisor to review the contractor termination process; 5) reviewed the contractor termination process with supervisors with contractors reporting to them and contractor leads within the project; and 6) reviewed all contractors both active and terminated from inception of the project on [REDACTED] that were given access to the [REDACTED] to verify that the end date within the access management tool accurately reflects the proper off-boarding date for the resource and confirm timely revocation if an end date for a terminated contractor is incorrect. <p>ReliabilityFirst 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
RFC2018020675	CIP-011-2	R1	[REDACTED]	[REDACTED]	8/1/2018	8/3/2018	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 9, 2018, the entity, [REDACTED], submitted a Self-Report stating that, it was in noncompliance with CIP-011-2 R1. On August 1, 2018, an entity associate emailed to an outside vendor an asset inventory list spreadsheet, which contained Bulk Electric System Cyber System Information (BCSI). However, the spreadsheet was not labeled as "CIP Protected" and the associate sent the spreadsheet without using proper secure external electronic transmission methods as required by entity policy. The BCSI at issue was [REDACTED] in scope for the CIP Standards. Two days later, the associate received an email from a team member reminding him that the spreadsheet contained BCSI. The associate then immediately contacted the vendor to ask that the email and spreadsheet be deleted. The vendor confirmed that it deleted the information upon request.</p> <p>The root cause of this noncompliance was that the associate who created the spreadsheet failed to recognize that the spreadsheet contained BCSI and failed to label it as such. Because it was not labeled, another associate sent the spreadsheet via email to the external vendor without proper protections. This root cause involves the management practice of information management, which includes identifying and assessing information item risk, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on August 1, 2018, when the associate improperly sent the spreadsheet to an outside vendor and ended on August 3, 2018, when the vendor confirmed it deleted the information.</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 label and transmit BCSI is that the information could be obtained by unauthorized individuals. This risk was mitigated in this case by the following factors. First, the associate emailed the BCSI to a trusted vendor that had a legitimate business need for the information. Second, the BCSI at issue was of limited value because an unauthorized person would still need further credentials to access the systems listed in the file. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) requested confirmation from the vendor that copies of the emails have been removed; 2) conducted an awareness meeting with the team of the associate that created the spreadsheet to reinforce the need to follow the entity's policy with regard to encryption and the security of externally transmitted BCSI; 3) conducted an awareness meeting with the team of the associate that sent the email to reinforce the need to follow the entity's policy with regard to encryption and the security of externally transmitted BCSI; 4) sent a message to the teams mentioned in Milestone 2 and 3 to reinforce the importance of following correct procedures regarding protected information; and 5) presented the impacted groups with a procedure to reinforce the need to apply proper labeling to BCSI. <p>ReliabilityFirst 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
RFC2018020676	CIP-011-2	R1	[REDACTED]	[REDACTED]	8/1/2018	8/3/2018	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 9, 2018, the entity, [REDACTED], submitted a Self-Report stating that, it was in noncompliance with CIP-011-2 R1. On August 1, 2018, an entity associate emailed to an outside vendor an asset inventory list spreadsheet, which contained Bulk Electric System Cyber System Information (BCSI). However, the spreadsheet was not labeled as "CIP Protected" and the associate sent the spreadsheet without using proper secure external electronic transmission methods as required by entity policy. The BCSI at issue was [REDACTED] in scope for the CIP Standards. Two days later, the associate received an email from a team member reminding him that the spreadsheet contained BCSI. The associate then immediately contacted the vendor to ask that the email and spreadsheet be deleted. The vendor confirmed that it deleted the information upon request.</p> <p>The root cause of this noncompliance was that the associate who created the spreadsheet failed to recognize that the spreadsheet contained BCSI and failed to label it as such. Because it was not labeled, another associate sent the spreadsheet via email to the external vendor without proper protections. This root cause involves the management practice of information management, which includes identifying and assessing information item risk, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on August 1, 2018, when the associate improperly sent the spreadsheet to an outside vendor and ended on August 3, 2018, when the vendor confirmed it deleted the information.</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 label and transmit BCSI is that the information could be obtained by unauthorized individuals. This risk was mitigated in this case by the following factors. First, the associate emailed the BCSI to a trusted vendor that had a legitimate business need for the information. Second, the BCSI at issue was of limited value because an unauthorized person would still need further credentials to access the systems listed in the file. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) requested confirmation from the vendor that copies of the emails have been removed; 2) conducted an awareness meeting with the team of the associate that created the spreadsheet to reinforce the need to follow the entity's policy with regard to encryption and the security of externally transmitted BCSI; 3) conducted an awareness meeting with the team of the associate that sent the email to reinforce the need to follow the entity's policy with regard to encryption and the security of externally transmitted BCSI; 4) sent a message to the teams mentioned in Milestone 2 and 3 to reinforce the importance of following correct procedures regarding protected information; and 5) presented the impacted groups with a procedure to reinforce the need to apply proper labeling to BCSI. <p>ReliabilityFirst 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
RFC2018020677	CIP-011-2	R1	[REDACTED]	[REDACTED]	8/1/2018	8/3/2018	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 9, 2018, the entity, [REDACTED], submitted a Self-Report stating that, it was in noncompliance with CIP-011-2 R1. On August 1, 2018, an entity associate emailed to an outside vendor an asset inventory list spreadsheet, which contained Bulk Electric System Cyber System Information (BCSI). However, the spreadsheet was not labeled as "CIP Protected" and the associate sent the spreadsheet without using proper secure external electronic transmission methods as required by entity policy. The BCSI at issue was [REDACTED] in scope for the CIP Standards. Two days later, the associate received an email from a team member reminding him that the spreadsheet contained BCSI. The associate then immediately contacted the vendor to ask that the email and spreadsheet be deleted. The vendor confirmed that it deleted the information upon request.</p> <p>The root cause of this noncompliance was that the associate who created the spreadsheet failed to recognize that the spreadsheet contained BCSI and failed to label it as such. Because it was not labeled, another associate sent the spreadsheet via email to the external vendor without proper protections. This root cause involves the management practice of information management, which includes identifying and assessing information item risk, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on August 1, 2018, when the associate improperly sent the spreadsheet to an outside vendor and ended on August 3, 2018, when the vendor confirmed it deleted the information.</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 label and transmit BCSI is that the information could be obtained by unauthorized individuals. This risk was mitigated in this case by the following factors. First, the associate emailed the BCSI to a trusted vendor that had a legitimate business need for the information. Second, the BCSI at issue was of limited value because an unauthorized person would still need further credentials to access the systems listed in the file. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) requested confirmation from the vendor that copies of the emails have been removed; 2) conducted an awareness meeting with the team of the associate that created the spreadsheet to reinforce the need to follow the entity's policy with regard to encryption and the security of externally transmitted BCSI; 3) conducted an awareness meeting with the team of the associate that sent the email to reinforce the need to follow the entity's policy with regard to encryption and the security of externally transmitted BCSI; 4) sent a message to the teams mentioned in Milestone 2 and 3 to reinforce the importance of following correct procedures regarding protected information; and 5) presented the impacted groups with a procedure to reinforce the need to apply proper labeling to BCSI. <p>ReliabilityFirst 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
RFC2018020679	CIP-011-2	R1	[REDACTED]	[REDACTED]	8/1/2018	8/3/2018	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 9, 2018, the entity, [REDACTED], submitted a Self-Report stating that, it was in noncompliance with CIP-011-2 R1. On August 1, 2018, an entity associate emailed to an outside vendor an asset inventory list spreadsheet, which contained Bulk Electric System Cyber System Information (BCSI). However, the spreadsheet was not labeled as "CIP Protected" and the associate sent the spreadsheet without using proper secure external electronic transmission methods as required by entity policy. The BCSI at issue was [REDACTED] in scope for the CIP Standards. Two days later, the associate received an email from a team member reminding him that the spreadsheet contained BCSI. The associate then immediately contacted the vendor to ask that the email and spreadsheet be deleted. The vendor confirmed that it deleted the information upon request.</p> <p>The root cause of this noncompliance was that the associate who created the spreadsheet failed to recognize that the spreadsheet contained BCSI and failed to label it as such. Because it was not labeled, another associate sent the spreadsheet via email to the external vendor without proper protections. This root cause involves the management practice of information management, which includes identifying and assessing information item risk, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on August 1, 2018, when the associate improperly sent the spreadsheet to an outside vendor and ended on August 3, 2018, when the vendor confirmed it deleted the information.</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 label and transmit BCSI is that the information could be obtained by unauthorized individuals. This risk was mitigated in this case by the following factors. First, the associate emailed the BCSI to a trusted vendor that had a legitimate business need for the information. Second, the BCSI at issue was of limited value because an unauthorized person would still need further credentials to access the systems listed in the file. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) requested confirmation from the vendor that copies of the emails have been removed; 2) conducted an awareness meeting with the team of the associate that created the spreadsheet to reinforce the need to follow the entity's policy with regard to encryption and the security of externally transmitted BCSI; 3) conducted an awareness meeting with the team of the associate that sent the email to reinforce the need to the entity's policy with regard to encryption and the security of externally transmitted BCSI; 4) sent a message to the teams mentioned in Milestone 2 and 3 to reinforce the importance of following correct procedures regarding protected information; and 5) presented the impacted groups with a procedure to reinforce the need to apply proper labeling to BCSI. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020638	CIP-007-6	R2	[REDACTED]	[REDACTED]	8/25/2018	8/27/2018	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 25, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-007-6 R2. The entity did not evaluate [REDACTED] patches for applicability within the timeframe set forth in CIP-007-6 R2.2. The patch evaluation process was completed three days late.</p> <p>The root causes of this noncompliance were insufficient training and deficient instructions regarding new procedural steps. Subject matter experts (SMEs) began performing the patch evaluations that are the subject of this noncompliance on August 21, 2018, and they were relatively new to this task. The entity had also recently implemented new controls and steps in its patch evaluation process ([REDACTED]). The SMEs lack of experience and training, coupled with confusion regarding the new controls and steps, led to the failure to complete the evaluations on or before August 24, 2018, which was the due date for completion. The SMEs submitted the patch evaluations for final review on Thursday, August 23, 2018, and Friday, August 24, 2018; however, the SMEs omitted [REDACTED] and submitted the evaluations in a non-conforming format. This caused the aggregate review process to expand from its typical period (i.e., one or two hours) to a period of multiple days.</p> <p>This noncompliance implicates the management practice of workforce management. Workforce management includes the need to strive for operational proficiency through well-defined and executable processes and procedures. Combining appropriately skilled and trained staff with adequate processes, procedures, and work tools can assist in minimizing this type of violation.</p> <p>This noncompliance started on August 25, 2018, when the entity failed to evaluate patches for applicability and ended on August 27, 2018, when the evaluations were 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) based on the following factors. The failure to evaluate security patches could result in missing the installation of critical patches (or failing to implement adequate mitigation plans), thereby providing bad actors additional time to exploit known vulnerabilities and adversely affect the BPS. Here, the risk was minimized based upon the following facts. First, the evaluations were only completed three days late. Second, notwithstanding the delay, all systems were patched (or had an approved mitigation plan) as required within 35 days of August 24, 2018 (i.e., the due date for the missed evaluations), thus further reducing the risk to 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 noncompliance involves high frequency conduct and the entity promptly identified and corrected the issue.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the evaluation of patches that were not completed within the timeframe set forth in the standard; 2) held a patching team conference and discussed lessons learned and current methodology of completing the patch cycle; and 3) improved documentation of patching discovery steps, including the integration of a flow chart into training documentation. <p>ReliabilityFirst 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
RFC2018020789	CIP-010-2	R1	[REDACTED]	[REDACTED]	11/29/2018	11/30/2018	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 30, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-010-2 R1. Entity staff connected a new Cyber Asset type to the entity's [REDACTED] Electronic Security Perimeter (ESP) on November 29, 2018. The new device type was verbally authorized, but not authorized in accordance with the entity's procedures prior to introduction into the ESP. [REDACTED], the device did not have an active vulnerability assessment performed prior to it being added to the ESP. [REDACTED]</p> <p>[REDACTED] While the device was plugged in, and configuration started, the configuration was not yet completed, and was unable to successfully pull the status of the [REDACTED]. The configuration was never completed and the light was not hooked up, therefore the device was not usable. In sum, although the device was connected to the ESP, the device was not yet configured/usable.</p> <p>As background, the supervisor originally responsible for installing the device was placed on medical leave. That supervisor's responsibilities were then transitioned to an employee within that supervisor's chain-of-command. A full knowledge transfer was not possible due to the supervisor being on leave. The entity's Supervisory Control and Data Acquisition vendor arrived onsite on November 29, 2018 for a support visit to install the new device. The entity technician moved forward with the installation without following all of the entity's procedures, incorrectly assuming that the supervisor had already completed all of the required steps (authorized change ticket and vulnerability assessment) before he went on leave.</p> <p>Another entity employee witnessed this installation and questioned whether all necessary steps had been taken, which led to the discovery of this noncompliance.</p> <p>The root cause of this noncompliance was the entity technician's failure to follow established procedures when connecting the new device.</p> <p>This noncompliance involves the management practices of work management and workforce management. Work management is involved because the entity did not have an effective knowledge transfer policy in place to ensure that the technician now responsible for installing this device understood what entity procedures needed to be followed. Workforce management through ineffective training is involved because the technician was not effectively trained on what procedures needed to be followed when connecting this new device.</p> <p>This noncompliance started on November 29, 2018, when the entity connected the new device to the ESP in violation of the entity's internal procedures by not having an authorized change ticket and ended on November 30, 2018, when the entity disconnected the device from the ESP.</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 an unauthorized change that could adversely affect system security. The risk is minimized because while the device was plugged in, and configuration started, the configuration was not yet completed, and was unable to successfully pull the status of the [REDACTED]. The configuration was never completed and the light was not hooked up, therefore the device was not usable for the duration of the noncompliance. Additionally, the entity quickly identified, assessed, and corrected this noncompliance as the duration was only one day. No harm is known to have occurred. (The entity is confident that no vulnerabilities were introduced to the ESP when this device was connected to the ESP because (1) at the time of installation, the device was on the latest firmware and (2) [REDACTED] protections were in place for the entire time the device was plugged into the ESP and those did not detect any malicious activities.)</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history does not warrant an alternative disposition method and should not serve as a basis for applying a penalty because some of the prior noncompliances are distinguishable as they involved different root causes. For the two issues that are arguably similar, ReliabilityFirst determined that the current noncompliance continues to qualify for compliance exception treatment as it posed only minimal risk and is not indicative of a systemic or programmatic issue. Further, the entity quickly identified the noncompliance and corrected the issues through its internal controls.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disconnected the device and suspended the deployment of the device until all parties involved were clear on what steps had been completed and what steps needed to be completed prior to deployment; 2) updated the change ticketing system to include searchable and reportable fields for vulnerability assessments associated with change tickets; 3) updated the change management process as follows: (i) Required that new devices are introduced to the database earlier in the process to make the change ticketing system easier to utilize for new devices; (ii) Required that [REDACTED] networking employees validate change tickets, authorization, and vulnerability assessments before opening ports for a new device; and (iii) Required that all documentation be reviewed in the event that responsibilities for device deployment change; and 4) trained all applicable personnel on the process and procedure changes. <p>ReliabilityFirst 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
RFC2018020790	CIP-010-2	R3	[REDACTED]	[REDACTED]	11/29/2018	11/30/2018	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 30, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-010-2 R3. Entity staff connected a new Cyber Asset type to the entity's [REDACTED] Electronic Security Perimeter (ESP) on November 29, 2018.</p> <p>The new device type was verbally authorized, but not authorized in accordance with the entity's procedures prior to introduction into the ESP. [REDACTED] The device did not have an active vulnerability assessment performed prior to it being added to the ESP. [REDACTED]</p> <p>[REDACTED] While the device was plugged in, and configuration started, the configuration was not yet completed, and was unable to successfully pull the status of the [REDACTED]. The configuration was never completed and the light was not hooked up, therefore the device was not usable. In sum, although the device was connected to the ESP, the device was not yet configured/usable.</p> <p>The supervisor originally responsible for installing the device was placed on medical leave. That supervisor's responsibilities were then transitioned to an employee within that supervisor's chain-of-command. A full knowledge transfer was not possible due to the supervisor being on leave. The entity's Supervisory Control and Data Acquisition vendor arrived onsite on November 29, 2018 for a support visit to install the new device. The entity technician moved forward with the installation without following all of the entity's procedures assuming that the supervisor had already completed all of the required steps (authorized change ticket and vulnerability assessment).</p> <p>Another entity employee witnessed this installation and questioned whether all necessary steps had been taken which led to the discovery of this noncompliance.</p> <p>The root cause of this noncompliance was the entity technician's failure to follow established procedures when connecting the new device.</p> <p>This noncompliance involves the management practices of work management and workforce management. Work management is involved because the entity did not have an effective knowledge transfer policy in place to ensure that the technician now responsible for installing this device understood what entity procedures needed to be followed. Workforce management through ineffective training is involved because the technician was not effectively trained on what procedures needed to be followed when connecting this new device.</p> <p>This noncompliance started on November 29, 2018, when the entity connected the new device to the ESP in violation of the entity's internal procedures by not performing a vulnerability assessment and ended on November 30, 2018, when the entity disconnected the device from the ESP.</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 permitting a baseline change (connecting a new device to the ESP) before performing a vulnerability assessment on that change could adversely affect system security. The risk is minimized because while the device was plugged in, and configuration started, the configuration was not yet completed, and was unable to successfully pull the status of the [REDACTED]. The configuration was never completed and the light was not hooked up, therefore the device was not usable for the duration of the noncompliance. Additionally, the entity quickly identified, assessed, and corrected this noncompliance as the duration was only one day. No harm is known to have occurred. (The entity is confident that no vulnerabilities were introduced to the ESP when this device was connected to the ESP because (1) at the time of installation, the device was on the latest firmware and (2) [REDACTED] protections were in place for the entire time the device was plugged into the ESP and those did not detect any malicious activities.)</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history does not warrant an alternative disposition method and should not serve as a basis for applying a penalty because some of the prior noncompliances are distinguishable as they involved different root causes. For the two issues that are arguably similar, ReliabilityFirst determined that the current noncompliance continues to qualify for compliance exception treatment as it posed only minimal risk and is not indicative of a systemic or programmatic issue. Further, the entity quickly identified the noncompliance and corrected the issues through its internal controls.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) disconnected the device and suspended the deployment of the device until all parties involved were clear on what steps had been completed and what steps needed to be completed prior to deployment; 2) updated the change ticketing system to include searchable and reportable fields for vulnerability assessments associated with change tickets; 3) updated the change management process as follows: (i) Required that new devices are introduced to the database earlier in the process to make the change ticketing system easier to utilize for new devices; (ii) Required that [REDACTED] networking employees validate change tickets, authorization, and vulnerability assessments before opening ports for a new device; and (iii) Required that all documentation be reviewed in the event that responsibilities for device deployment change; and 					

ReliabilityFirst Corporation (ReliabilityFirst)

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
RFC2018020790	CIP-010-2	R3			11/29/2018	11/30/2018	Self-Report	Completed
			4) trained all applicable personnel on the process and procedure changes. ReliabilityFirst has verified the completion of all mitigation activity.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019815	CIP-007-6	R5	[REDACTED]	[REDACTED]	7/1/2016	7/9/2018	Self-Report	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 May 24, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-007-6 R5.</p> <p>An administrator for the entity discovered on February 19, 2018, that the default lockout policy did not apply to two types of [REDACTED] accounts. Specifically, [REDACTED] and a [REDACTED] were impacted. There was no existing Technical Feasibility Exception (TFE) in place to comply with CIP-007 R5.7. One [REDACTED] account was deleted when the noncompliance was discovered; the other [REDACTED] account is used to login to the console and the [REDACTED] account is used to login to the [REDACTED]. The default lockout policy did not apply to the remaining [REDACTED] and [REDACTED] accounts because the system manages other accounts in a separate internal database. Therefore, the [REDACTED] and [REDACTED] accounts should be covered by a TFE, but were not at the time of the noncompliance.</p> <p>The root cause of this noncompliance was the entity's insufficient controls around a process change from Version 3 to Version 5 standards resulting in a failure to identify and request a TFE on these accounts.</p> <p>This noncompliance involves the management practices of workforce management and verification. Workforce management is implicated because the new account administrator was not aware of relevant requirements as a result of an insufficient transition of responsibilities caused by a change in standards. Verification management is involved because the Entities failed to inventory and request a TFE for two types of administrative accounts.</p> <p>The noncompliance began on July 1, 2016, the date the entity was required to comply with CIP-007-6 R5. The noncompliance ended on July 9, 2018, the date the entity completed its Mitigating Activities.</p> <p>ReliabilityFirst notes that the risk was mitigated upon [REDACTED].</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 the ability for a bad actor to gain access to Cyber Assets. The risk is minimized in this instance because of the following three compensating measures which were in place prior to July 1, 2016: 1) the entity performed log reviews each week for anomalies including review of [REDACTED] activity; 2) the entity [REDACTED] requirements which exceed the NERC password complexity requirements; and 3) a number of the tasks that could be performed with the [REDACTED]. Thus, the risk posed to the bulk-power system was minimal. 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) added a control so that the [REDACTED] can only be accessed through the jump host; 2) filed a TFE with SERC Region for the affected devices. (The devices in scope for this Self Report were part of a Bulk Electric System Cyber System associated the [REDACTED] for both [REDACTED] e and [REDACTED]. None of the devices were located at the two generation facilities. The [REDACTED] for [REDACTED] is now registered in [REDACTED] and the TFEs are filed under that registration.); 3) updated commissioning checklist to include a review of "all types of accounts" and tested any vendor statement impacting compliance requirements; and 4) trained individuals on the modification made to the commissioning checklist. <p>ReliabilityFirst 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
RFC2018019818	CIP-007-6	R5	[REDACTED]	[REDACTED]	10/8/2016	7/9/2018	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 May 24, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED], it was in noncompliance with CIP-007-6 R5.</p> <p>An administrator for the entity discovered on February 19, 2018, that the default lockout policy did not apply to two types of [REDACTED] accounts. Specifically, two [REDACTED] accounts and a [REDACTED] account were impacted. There was no existing Technical Feasibility Exception (TFE) in place to comply with CIP-007 R5.7. One [REDACTED] account was deleted when the noncompliance was discovered; the other [REDACTED] account is used to login to the console and the [REDACTED] account is used to login to the [REDACTED]. The default lockout policy did not apply to the remaining [REDACTED] and [REDACTED] accounts because the system manages other accounts in a separate internal database. Therefore, the [REDACTED] and [REDACTED] accounts should be covered by a TFE, but were not at the time of the noncompliance.</p> <p>The root cause of this noncompliance was the entity's insufficient controls around a process change from Version 3 to Version 5 standards resulting in a failure to identify and request a TFE on these accounts.</p> <p>This noncompliance involves the management practices of workforce management and verification. Workforce management is implicated because the new account administrator was not aware of relevant requirements as a result of an insufficient transition of responsibilities caused by a change in standards. Verification management is involved because the Entities failed to inventory and request a TFE for two types of administrative accounts.</p> <p>The noncompliance began on October 8, 2016, the date the entity was required to comply with CIP-007-6 R5. The noncompliance ended on July 9, 2018, the date the entity completed its Mitigating Activities.</p> <p>ReliabilityFirst notes that the risk was mitigated upon [REDACTED].</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 the ability for a bad actor to gain access to Cyber Assets. The risk is minimized in this instance because of the following three compensating measures which were in place prior to July 1, 2016: 1) the entity performed log reviews each week for anomalies including review of [REDACTED] activity; 2) the entity utilized [REDACTED] requirements which exceed the NERC password complexity requirements; and 3) a number of the tasks that could be performed with the [REDACTED]. Thus, the risk posed to the bulk-power system was minimal. 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) added a control so that the [REDACTED] can only be accessed through the jump host; 2) filed a TFE with SERC Region for the affected devices. (The devices in scope for this Self Report were part of a Bulk Electric System Cyber System associated the [REDACTED] for both [REDACTED] and [REDACTED]. None of the devices were located at the two generation facilities. The [REDACTED] for [REDACTED] is now registered in [REDACTED] and the TFEs are filed under that registration.); 3) updated commissioning checklist to include a review of "all types of accounts" and tested any vendor statement impacting compliance requirements; and 4) trained individuals on the modification made to the commissioning checklist. <p>ReliabilityFirst 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
RFC2018020757	CIP-003-6	R1	[REDACTED]	[REDACTED]	6/17/2018	7/26/2018	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 21, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-003-6 R1.</p> <p>On July 26, 2018, an employee reviewing the entity's cyber security policy discovered that the internal policy that enumerates the entity's CIP policies and programs (CIP Policy) had not been reviewed within 15 months as required per CIP-003-6 R1. The previous CIP Policy review was performed on March 16, 2017, and the next review was required to be performed by June 16, 2018. After discovering this issue, the entity CIP Senior Manager approved the CIP Policy following a review on July 26, 2018.</p> <p>The root cause of this noncompliance was an input error that occurred when the entity transitioned work management systems that it uses to track deadlines for policy renewals. During the noncompliance, the entity replaced the existing work management system with a new work management system. The work management task associated with obtaining the 15 month approval on the policy had an incorrect date assigned during the conversion process from the old system to the new system.</p> <p>This noncompliance involves the management practices of risk management and work management. Risk management is involved because the CIP Policy [REDACTED]. Work management is involved because the CIP Policy is implemented and reviewed for the purpose of managing work related to grid reliability and the entity did not have an effective control in place to make sure the task was transitioned correctly to the new system.</p> <p>The noncompliance started on June 17, 2018, when the entity was required to complete their 15 month review of the CIP Policy, and ended on July 26, 2018, when the entity completed the CIP Policy review.</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 instance of noncompliance is potential application of inadequate, nonexistent, or outdated controls, resulting in compromise or misuse of Bulk Electric System Cyber Systems. The risk here is minimized because of the short duration of the noncompliance of just 40 days. Further minimizing the risk, the nature of this noncompliance was administrative and not substantive as no changes were made to the policy upon its July 26, 2018 review. 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 immediately reviewed and approved the policy. No changes were required to the content of the policy. The entity also corrected the "date of approval" in the work management system to prevent this issue from recurring going forward.</p> <p>ReliabilityFirst 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
RFC2018020758	CIP-003-6	R1	[REDACTED]	[REDACTED]	6/17/2018	7/26/2018	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 21, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-003-6 R1.</p> <p>On July 26, 2018, an employee reviewing the entity's cyber security policy discovered that the internal policy that enumerates the entity's CIP policies and programs (CIP Policy) had not been reviewed within 15 months as required per CIP-003-6 R1. The previous CIP Policy review was performed on March 16, 2017, and the next review was required to be performed by June 16, 2018. After discovering this issue, the entity CIP Senior Manager approved the CIP Policy following a review on July 26, 2018.</p> <p>The root cause of this noncompliance was an input error that occurred when the entity transitioned work management systems that it uses to track deadlines for policy renewals. During the noncompliance, the entity replaced the existing work management system with a new work management system. The work management task associated with obtaining the 15 month approval on the policy had an incorrect date assigned during the conversion process from the old system to the new system.</p> <p>This noncompliance involves the management practices of risk management and work management. Risk management is involved because the CIP Policy [REDACTED]. Work management is involved because the CIP Policy is implemented and reviewed for the purpose of managing work related to grid reliability and the entity did not have an effective control in place to make sure the task was transitioned correctly to the new system.</p> <p>The noncompliance started on June 17, 2018, when the entity was required to complete their 15 month review of the CIP Policy, and ended on July 26, 2018, when the entity completed the CIP Policy review.</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 instance of noncompliance is potential application of inadequate, nonexistent, or outdated controls, resulting in compromise or misuse of Bulk Electric System Cyber Systems. The risk here is minimized because of the short duration of the noncompliance of just 40 days. Further minimizing the risk, the nature of this noncompliance was administrative and not substantive as no changes were made to the policy upon its July 26, 2018 review. 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 immediately reviewed and approved the policy. No changes were required to the content of the policy. The entity also corrected the "date of approval" in the work management system to prevent this issue from recurring going forward.</p> <p>ReliabilityFirst 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
RFC2018020678	CIP-010-2	R1	[REDACTED]	[REDACTED]	8/17/2018	9/30/2018	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 9, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-010-2 R1.</p> <p>On August 17, 2018, an IT analyst installed protective anti-malware software on a [REDACTED] workstation, which is classified as a [REDACTED]. The IT analyst received verbal authorization to make this change, but a change ticket was not created to document the verbal authorization. [REDACTED] during routine baseline monitoring activities, the entity identified this change and learned there was no corresponding change ticket.</p> <p>The root cause of this noncompliance was the IT analyst's mistaken belief that this change was covered by a prior change ticket (and therefore that the verbal authorization was sufficient to move forward with the change). The IT analyst should have confirmed, prior to making the change, that this assumption was correct. Additionally, the other employee failed to adhere to the procedures when he gave verbal authorization as opposed to going through the proper procedures, which require approving a change ticket in the system. This root cause involves the management practice of verification because the IT analyst failed to verify that the change was formally approved prior to making it. It also involves workforce management as the other employee was not properly trained regarding verbal authorizations.</p> <p>This noncompliance started on August 17, 2018, when the IT analyst made the change, and ended on September 30, 2018, when the entity formally approved the change with a change ticket.</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 making baseline impacting changes without prior authorization and documentation is that the change could have adverse effects on the system. This risk was mitigated in this case based on the following factors. First, the entity identified the issue through normally occurring internal controls. Second, the software at issue is part of the standard suite of applications installed on devices of this type, and had already been installed on every other like device with no negative impact. No harm is known to have occurred.</p> <p>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 noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) created, completed and closed a change ticket for change at issue on the PCA device; 2) conducted refresher change management training that includes the change management ticketing process; and 3) conducted training for entity [REDACTED] team on [REDACTED] process. <p>ReliabilityFirst 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
RFC2018019464	CIP-004-6	R4	[REDACTED]	[REDACTED]	7/25/2017	11/15/2017	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 March 26, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-004-6 R4. The entity had implemented a process to authorize electronic access to Bulk Electric System (BES) Cyber Systems and their associated Electronic Access Control or Monitoring Systems and Physical Access Control Systems and BES Cyber System Information, but in this case, an employee bypassed that process and obtained unauthorized access to certain CIP-scoped assets. Specifically, as of July 25, 2017, a system administrator did not have authorized access to CIP-scoped [REDACTED] systems. Yet, on that date and without having been granted proper access, the administrator obtained the passwords for the [REDACTED] on those systems.</p> <p>As background, the administrator had been tasked with changing the passwords [REDACTED] on all of the [REDACTED] systems (i.e., CIP-scoped and non-CIP-scoped). Based upon his job responsibilities, the administrator assumed that he had authorized access to the CIP-scoped [REDACTED] systems, but he discovered that he did not [REDACTED]. Thereafter, the administrator retrieved the password for the non-CIP-scoped [REDACTED] systems and ran a script intending to change the passwords for the non-CIP-scoped [REDACTED] systems. But, the script also changed the passwords for the CIP-scoped [REDACTED] systems because, in this case, the passwords for the non-CIP-scoped and CIP-scoped systems were the same. After executing the script, the administrator had the passwords for (and corresponding unauthorized access to) all of the [REDACTED] systems (i.e., CIP-scoped and non-CIP-scoped). The issue was discovered in November, 2017, when departments were discussing [REDACTED].</p> <p>The root cause of this noncompliance was that passwords for the [REDACTED] on the CIP-scoped and non-CIP-scoped [REDACTED] systems were the same. ReliabilityFirst considers the intentional use of duplicate passwords between systems or accounts to be poor security practice, which should only be used when there is a business justification to do so. This noncompliance implicates the management practice of asset and configuration management, which includes the need to maintain the integrity of assets and systems in the context of reliability and resilience. It also implicates the management practice of workforce management since the administrator should have known to follow the entity's process for requesting access after he discovered that he did not have requisite access.</p> <p>This noncompliance started on July 25, 2017, when the system administrator obtained the passwords for (and corresponding unauthorized access to) the CIP-scoped [REDACTED] systems and ended on November 15, 2017, when the entity changed the passwords, thereby removing the administrator's ability to access the systems.</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. Unauthorized access to systems can be detrimental to an entity and the reliability of the BPS as harm could be caused intentionally or as a result of misuse. In this case, the risk was mitigated by the following facts. The system administrator had all necessary qualifications and had completed requisite training to obtain access. Further, the entity had intended to provision the administrator access to the [REDACTED] for the CIP-scoped [REDACTED] systems based upon his job responsibilities but overlooked its failure to do so. And, the entity had, in fact, provisioned the employee access to many other CIP-scoped systems. Soon after the discovery of this noncompliance, the entity provisioned the system administrator appropriate access to the affected systems. 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 instant noncompliance involves different facts and circumstances and a different root cause.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) changed the passwords on the [REDACTED] systems so that CIP-scoped and non-CIP-scoped passwords are different, thereby addressing the root cause; 2) granted the employee appropriate access for his job role and responsibilities; 3) performed detailed root cause analysis; 4) added training to its quarterly training that it includes information on recognizing a lack of access and that access must be requested; and 5) updated its password security standard to reflect that passwords for accounts on both CIP and non-CIP assets must be different, effective when passwords are changed. <p>ReliabilityFirst 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
RFC2018020465	CIP-007-6	R2	[REDACTED]	[REDACTED]	4/25/2018	6/22/2018	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 September 20, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-007-6 R2. The entity failed to evaluate two IBM service packs for applicability within the time period set forth in CIP-007-6 R 2.2. The first service pack was released on March 20, 2018, but was not evaluated until June 12, 2018 (i.e., 84 days after it was released). The first service pack affected [REDACTED]. The second service pack was released on May 4, 2018, but was not evaluated until June 22, 2018 (i.e., 49 days after it was released). The second service pack affected [REDACTED].</p> <p>The issue was discovered when the entity's patch scheduling team noticed that the service packs were missing when preparing to install other IBM patches. Upon investigation, it was determined that the individual responsible for evaluating patches failed to identify the above-referenced service packs when they were released because IBM changed the way patches were listed on its website. Specifically, the most recent patches were no longer listed at the top of the page by default, and the individual responsible for evaluating patches was not aware of the need to filter and sort the list of patches.</p> <p>The root cause of this noncompliance was a procedural gap or training gap. The entity's patch tracking procedure or training did not describe the steps one must take to filter the IBM site correctly. The individual responsible for evaluating patches did not know to filter and sort the list of patches.</p> <p>The noncompliance implicates the management practices of workforce management and external interdependencies. Important components of workforce management are (a) the implementation of clear, thorough, and executable procedures and (b) training staff in order to promote awareness and impart skills and knowledge to enable staff to perform specific reliability and resilience functions. External interdependencies was involved because the entity assumed that IBM would continue releasing and posting patches in a consistent manner. The entity failed to account for a potential change by IBM, and this noncompliance could have been prevented through more effective management of the entity's reliance on IBM to reduce risks.</p> <p>The noncompliance relating to the first service pack started on April 25, 2018, after the entity failed to complete an evaluation within the time period set forth in CIP-007-6 R 2.2 and ended on June 12, 2018, after the entity finished its evaluation. The noncompliance relating to the second service pack started on June 9, 2018, after the entity failed to complete an evaluation within the time period set forth in CIP-007-6 R 2.2 and ended on June 22, 2018, after the entity finished its 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 based on the following factors. The failure to evaluate patches in a timely manner could leave BES Cyber Systems vulnerable to malicious activity. The risk was mitigated in this case based upon the following facts. The duration of the noncompliance was relatively short, and the entity self-identified and corrected the issue. Further, after evaluating the service packs and while creating dated mitigation plans in accordance with CIP-007-6 R 2.3, the entity determined that existing controls in the entity's environment sufficiently mitigated the risk until the patches could be applied at later dates. 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 instant noncompliance involves different facts, circumstances, and/or causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) created a mitigation plan and documented the target installation date for the first service pack; 2) evaluated for applicability the first service pack; 3) created a mitigation plan and documented the target installation date for the second service pack; 4) evaluated for applicability the second service pack; 5) updated the internal patch tracking procedure with specific instructions on how to filter the IBM patch tracking site. This mitigation step will close the gap in the entity's evaluation process to correct the identified root cause; 6) conducted reconciliation to verify that no other patches were missed due to the gap in the entity's patch evaluation process for the IBM site going back to January 1, 2018; and 7) conducted additional training to ensure that pertinent personnel are aware of the changes made to the entity's internal patch tracking 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
RFC2018020739	CIP-006-6	R2	[REDACTED]	[REDACTED]	9/20/2018	9/20/2018	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 16, 2018, the entity [REDACTED] submitted a Self-Report stating that, [REDACTED] in noncompliance with CIP-006-6 R2. [REDACTED]</p> <p>On September 20, 2018 at 16:40 hours, at a data center, a clerk escorted a visitor into a Physical Security Perimeter (PSP). The visitor was a contractor responsible for completing maintenance on a water fountain system. While the visitor conducted his routine work activities, the escort walked away for approximately 8 minutes and the escort could no longer view the visiting contractor, resulting in a noncompliance of CIP-006-6 R2.1.</p> <p>Within a few minutes of the noncompliance the escort self-reported the incident to a security officer. The security officer then located the unescorted visitor within the PSP and remained with the visitor until the maintenance was complete and then escorted the visitor out of the PSP at 16:53 hours. The entity reviewed the archived visitor log and determined that the visitor's name, company, and entry and exit times were logged, reflecting the security officer who escorted the visitor out of the PSP as the assigned escort.</p> <p>The root cause of the noncompliance was improper training and knowledge transfer to entity employees. The employee serving as an escort failed to execute the process for escorting visitors within the PSP as documented in the entity's policy and training.</p> <p>This noncompliance involves the management practices of external interdependencies and workforce management. External interdependencies management is involved because the entity relies on contractors to perform certain roles within the PSP but was not sufficiently prepared to manage the additional requirements which are introduced when a contractor is given access to a PSP. Workforce management is involved because the entity employee serving as an escort was inadequately trained on his responsibilities when escorting visitors inside a PSP.</p> <p>This noncompliance started on September 20, 2018, when the escort left his visitor unescorted inside the PSP and ended approximately eight minutes later on September 20, 2018, when the entity security officer began escorting the visitor inside the PSP again.</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 risk posed by permitting unauthorized individuals to access Bulk Electric System Cyber Systems without supervision is the potential for a bad actor to adversely affect the reliable operation of the BPS by operating or compromising assets within the PSP. This risk was minimized by the following factors. First, the visitor had an entity contractor identification badge and had been granted authorized access to entity facilities due to his role in maintaining the water fountains. Second, the visitor was in a break-room for the entire time he was left unescorted, did not have access to the server room, and did not have electronic access to any Cyber Assets. Lastly, staff and security officers are within the building containing the PSP at issue 24 hours a day, seven days a week. 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 Standard and Requirement governs high frequency conduct (escorting) for which the entity has demonstrated an ability to quickly identify and correct noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) provided security awareness coaching to the employee serving as an escort with respect to the importance of following escorted-visitor processes and procedures as trained. [REDACTED] 2) required the employee serving as an escort to re-take the [REDACTED]; and 3) designed and implemented mandatory training which includes key concepts, roles and responsibilities for security officers. The new NERC CIP Security Training security officers' initial training is required [REDACTED], with annual refresher and/or post-incident training to follow. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020740	CIP-006-6	R2	[REDACTED]	[REDACTED]	9/20/2018	9/20/2018	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 16, 2018, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-006-6 R2.</p> <p>On September 20, 2018 at 16:40 hours, at a data center, a clerk escorted a visitor into a Physical Security Perimeter (PSP). The visitor was a contractor responsible for completing maintenance on a water fountain system. While the visitor conducted his routine work activities, the escort walked away for approximately 8 minutes and the escort could no longer view the visiting contractor, resulting in a noncompliance of CIP-006-6 R2.1.</p> <p>Within a few minutes of the noncompliance the escort self-reported the incident to a security officer. The security officer then located the unescorted visitor within the PSP and remained with the visitor until the maintenance was complete and then escorted the visitor out of the PSP at 16:53 hours. The entity reviewed the archived visitor log and determined that the visitor's name, company, and entry and exit times were logged, reflecting the security officer who escorted the visitor out of the PSP as the assigned escort.</p> <p>The root cause of the noncompliance was improper training and knowledge transfer to entity employees. The employee serving as an escort failed to execute the process for escorting visitors within the PSP as documented in the entity's policy and training.</p> <p>This noncompliance involves the management practices of external interdependencies and workforce management. External interdependencies management is involved because the entity relies on contractors to perform certain roles within the PSP but was not sufficiently prepared to manage the additional requirements which are introduced when a contractor is given access to a PSP. Workforce management is involved because the entity employee serving as an escort was inadequately trained on his responsibilities when escorting visitors inside a PSP.</p> <p>This noncompliance started on September 20, 2018, when the escort left his visitor unescorted inside the PSP and ended approximately eight minutes later on September 20, 2018, when the entity security officer began escorting the visitor inside the PSP again.</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 risk posed by permitting unauthorized individuals to access Bulk Electric System Cyber Systems without supervision is the potential for a bad actor to adversely affect the reliable operation of the BPS by operating or compromising assets within the PSP. This risk was minimized by the following factors. First, the visitor had an entity contractor identification badge and had been granted authorized access to entity facilities due to his role in maintaining the water fountains. Second, the visitor was in a break-room for the entire time he was left unescorted, did not have access to the server room, and did not have electronic access to any Cyber Assets. Lastly, staff and security officers are within the building containing the PSP at issue 24 hours a day, seven days a week. 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 Standard and Requirement governs high frequency conduct (escorting) for which the entity has demonstrated an ability to quickly identify and correct noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) provided security awareness coaching to the employee serving as an escort with respect to the importance of following escorted-visitor processes and procedures as trained. [REDACTED] 2) required the employee serving as an escort to re-take the [REDACTED]; and 3) designed and implemented mandatory training which includes key concepts, roles and responsibilities for security officers. The new NERC CIP Security Training security officers' initial training is required by all current and new [REDACTED], with annual refresher and/or post-incident training to follow. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016573	CIP-004-3a	R4.1	[REDACTED]	[REDACTED]	03/22/2016	07/21/2016	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 violation.)			<p>On November 28, 2016, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-004-3a R4.1. The Entity did not maintain an accurate list of personnel with authorized unescorted physical access to Critical Cyber Assets (CCAs).</p> <p>On July 11, 2016, while conducting the second quarter 2016 quarterly access review, the Entity discovered that during the transition from its CIP Version 3 access management process to the Version 5 process, physical access rights were improperly granted to two employees.</p> <p>The Entity's first quarter 2016 access review conducted in April 2016 used the existing CIP Version 3 review process, which used data pulled during the last two weeks of the quarter (March 21-31, 2016). On March 22, 2016, the Entity executed the new CIP Version 5 process as an early transition exercise. The Entity's analyst conducted the CIP Version 5 review against the production database in real-time and determined that two employees should have had physical access to certain CCAs but did not. Because the database did not indicate that the Entity had previously revoked access for these two employees, the analyst reinstated access. In April 2016, during the required CIP Version 3 review using the existing V3 process, the Entity's analyst assessed access permissions using the data pulled prior to the Version 5 review, which properly showed that the access permissions for the two employees had been revoked in 2014 when they transferred to different departments and no longer needed the access. However, because the CIP Version 5 review pulled data in real-time, as opposed to previously pulled data, the analyst conducting the CIP Version 5 review was unaware of the access revocations.</p> <p>The extent-of-condition assessment consisted of the Entity conducting the quarterly access permissions review. The Entity reviewed all individuals with CIP access, using both CIP Version 3 and 5 methods, and confirmed it had identified all failures from the initial use of the CIP Version 5 process.</p> <p>This noncompliance started on March 22, 2016, when the Entity improperly reinstated the two employee's previously revoked physical access permissions, and ended on July 21, 2016, when the Entity revoked the last of the two employees' physical access permissions.</p> <p>The root-cause of this issue was a lack of training. The migration from one tool to another, coupled with the scope of assets and people involved under the transition from CIP Version 3 to Version 5 required more training on the need for self/peer checking of 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. The Entity improperly granting physical access permissions to employees could have permitted an employee unauthorized access to an Entity Physical Security Perimeter (PSP) who could degrade or destroy CCAs. However, the unauthorized access was granted to two current Entity employees who transferred to different departments and no longer needed such access. Neither of the two employees were aware that their access privileges were reinstated. The employees did not attempt to access an entity PSPs. No harm is known to have occurred.</p> <p>SERC considered the Entity's CIP-004 R4 compliance history, which includes NERC Violation ID [REDACTED], [REDACTED], and [REDACTED]. SERC determined that the Entity's compliance history should not serve as a basis for applying a penalty. The instant issue occurred during the transition from CIP Version 3 to Version 5; the mitigation for the prior instances would not have prevented the instant issue.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked inappropriate access for both employees; 2) coached the responsible employee who improperly granted access to reinforce proper use of human performance tools of peer checking and self-checking; and 3) re-trained IT Staff on the Access Management Guide. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017036	CIP-007-3a	R5.2	██████████	██████████	05/13/2016	05/17/2016	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 violation.)			<p>On February 16, 2017, the Entity submitted a Self-Report stating that, as a ██████████ and ██████████, it was in noncompliance with CIP-007-3a R5.2. The Entity deployed ██████ devices without changing the factory default passwords.</p> <p>On May 13, 2016, a contractor installed the ██████ new relays as part of a protection scheme for a substation autotransformer. The Entity identified the substation ██████████ as a Critical Asset under CIP Version 3. The contractor failed to follow the Entity's Account Management procedure, and did not change the default passwords prior to putting the relays into service. The Entity classified the ██████ relays as Critical Cyber Assets (CCAs).</p> <p>On May 17, 2016, while conducting a Supervisory Control And Data Acquisition (SCADA) checkout on new equipment, which has a component to assess passwords used, to check on the work performed for all new installations and modifications to existing architecture, the Entity discovered that the ██████ relays installed in the Critical Asset retained their factory default passwords. The Entity immediately changed the factory default passwords on the ██████ relays.</p> <p>An extent-of-condition assessment was conducted on all substations that contained medium impact Bulk Electric Cyber Systems (BCSs) using the failed status report notes to verify password changes had occurred. The Entity discovered no additional instances had occurred.</p> <p>This noncompliance started on May 13, 2016, when the Entity installed and placed ██████ CCAs into service without changing the default passwords, and ended on May 17, 2016, when the Entity discovered and changed the default passwords.</p> <p>The root cause of this noncompliance was an inadequate internal control to ensure adherence to the change management process. To mitigate this noncompliance, ██████████ now conducts weekly reviews for any upcoming Remote Terminal Unit SCADA checkout work, and when checkout work is identified, a checkout team member is assigned to be responsible for reviewing the upcoming modeling change and checkout. The team member is required to complete a SCADA Checkout Checklist, which aids in the identification of items that will require attention from the checkout team and verification that default passwords are changed prior to placing the device into service.</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 Entity's failure to change default passwords of newly installed CCAs could have permitted hackers to utilize default passwords to modify settings and create a potential opportunity for a cascading outage to occur. However, the relays were in service less than four days with the default password in place, and all ██████ relays resided at ██████ Critical Asset. The ██████ CCAs were within a secured Physical Security Perimeter that restricted physical access, and protected within a secure Electronic Security Perimeter that restricted remote access. 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) configured the devices in its automated change management system; 2) changed the passwords; 3) created an oversight process to alert technicians when password changes must occur; and 4) communicated new change management oversight process to appropriate personnel. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017662	CIP-007-6	R2.1	██████████	██████████	12/05/2016	12/06/2016	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 violation.)			<p>On May 24, 2017, the Entity submitted a Self-Report stating that, as a ██████████ and ██████████, it was in noncompliance with CIP-007-6 R2.1. The Entity did not track and evaluate security patches prior to installing them on ██████████ Bulk Electric System Cyber Assets (BCAs).</p> <p>On December 5, 2016, the Entity deployed security patches on three servers classified as BCAs within a high impact Bulk Electric System Cyber System (BCS). The affected [SCADA] servers were in the production environment, but were running in a back-up capacity, and were not serving as the primary and real-time operational servers. The patch deployment occurred without the Entity assessing the security patches for applicability. The Entity deployed the patches in error, and the patches were within the production environment for approximately 20 hours until they were being backed-out and removed pending successful assessment.</p> <p>The Entity discovered this issue through an internal control, an automated change and configuration management application. The tool runs at least daily looking for any unauthorized changes to the Cyber Asset baselines. On December 5, 2016, during the nightly application run, the tool discovered the untested security patches within the secured environment and alerted Entity personnel. On December 6, 2016, the Entity investigated and removed the patches.</p> <p>The extent-of-condition assessment involved using the same tool and reviewing the results for any other similar issues. The Entity discovered no additional instances.</p> <p>This noncompliance started on December 5, 2016, when the Entity deployed security patches to three servers prior to assessment, and ended on December 6, 2016, when the Entity rolled the servers back and removed the involved security patches.</p> <p>The root-cause of this issue was lack of training on how the Entity executes its patch management program.</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 Entity's deployment of unassessed security patches could have resulted in unnecessary or inappropriate security patches, potentially creating an unstable or unresponsive energy management system. However, the vendors had assessed and approved the patches. The Entity permitted the unassessed patches to exist in the CIP environment for approximately 20 hours. The patches only affected three servers, all of which were running in production in a back-up state. The affected servers were not primary operational servers. 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) removed the security patches off the servers; and 2) retrained the involved individuals on using the patch management processes. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016519	CIP-007-6	R5, P5.2	[REDACTED]	[REDACTED]	07/01/2016	11/04/2016	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 violation.)			<p>On November 16, 2016, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5, P5.2. The Entity had one instance where it did not identify and inventory one enabled default account type.</p> <p>On October 13, 2016, during preparations for an internal audit of CIP requirements, the Entity discovered one remote terminal units (RTUs) type, consisting of [REDACTED] RTUs, with a default account that it had not previously identified or inventoried. The default account was a “supervisor” account, which the RTU configuration application could access through a serial port. This type of RTU was identified at all of the Entity’s [REDACTED] substations ([REDACTED] has [REDACTED] RTU and [REDACTED] has [REDACTED] RTUs). During the internal audit, the Entity’s Cyber Security team had a conversation with a Senior Engineer in the [REDACTED]. The conversation revealed the RTUs with the default account was discovered during the test plan process and was applied when making configuration changes during the transition to CIP Version 5 of the standard. Specifically, prior to July 1, 2016, in preparation for CIP Version 5, the Entity hardened the RTUs by removing each RTU’s default account and changing the local user account password, which was stored in a local configuration file. Thereafter, the Entity generated a configuration file that listed each RTU account. However, the supervisor account did not appear in the RTU configuration file, along with the default account, nor did it appear in the RTU Software Manual, and the Entity did not confirm that the enabled default account type had been identified.</p> <p>On October 18, 2016, once the Entity discovered the issue, the Entity followed-up with the vendor and confirmed a listing of all default accounts on the model of RTU at issue. The vendor responded with a list of default accounts, which also did not include the supervisor account. Pressing further, the Entity received another response from the vendor, which confirmed that the supervisor account did exist but that no other default account existed. On November 4, 2016, the Entity identified and inventoried the default supervisor accounts.</p> <p>The noncompliance affected 12 facilities associated with [REDACTED] medium impact Bulk Electric System (BES) Cyber Systems, which are also classified as [REDACTED] BES Cyber Assets.</p> <p>The extent-of-condition assessment consisted of documentation review, vendor attestation, and additional research into each devices capability. The Entity reviewed Cyber Asset inventory to identify similar Cyber Assets, which may have possessed default accounts unknown or not documented by the vendor. The Entity discovered no additional instances.</p> <p>This noncompliance started on July 1, 2016, when the standard became mandatory and enforceable, and ended on November 4, 2016, when the Entity identified and inventoried the missing RTU default account.</p> <p>The root cause of the noncompliance was a lack of management oversight during the transition to CIP Version 5. Although the vendor was unaware of the specifications and capabilities of the RTU type, the Entity discovered the issue prior to the effective date of CIP Version 5, and should have conducted more testing to confirm the issues was resolved.</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 identifying and inventorying all known account types, there was a potential avenue for hackers to gain access to overlooked accounts and make configuration changes to RTUs or compromise monitoring situational awareness and adversely affect grid security. However, this specific account was unknown to the industry through literature and manuals, and was obscure even to the vendor. None of the RTUs had External Routable Connectivity. The Entity protected the RTUs within access-controlled Physical Security Perimeters, and firmware updates would not be possible without physical access. The Entity otherwise controlled electronic access by way of Electronic Security Perimeters with two-factor authentication required for remote access via an Intermediate System. Finally, remote access monitoring and logging was in place, and control center operators monitored real-time RTU status. 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) amended the CIP-007 Account tracking document to show the new default and shared account for the RTU type and the user roles that have authorized access to this shared account; and 2) provided lessons learned to multiple Entity departments to reinforce the need for Entity staff to research and establish complete documentation of security controls and features for existing and new 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
TRE2018020853	CIP-002-5.1	R1; R1.3	[REDACTED] (the "Entity")	[REDACTED]	07/01/2016	04/01/2017	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 violation.)			<p>During a Self-Certification conducted from August 24, 2018, through December 20, 2018, Texas RE determined that the Entity, as a [REDACTED] was in noncompliance with CIP-002-5.1 R1. The Entity did not identify each asset that contains a [REDACTED] BES Cyber System according to Attachment 1, Section 3.</p> <p>This noncompliance started on July 1, 2016, when CIP-002-5.1 R1 became enforceable and ended on April 1, 2017, when the Entity identified each asset containing a [REDACTED] BES Cyber System.</p> <p>The root cause of this issue was a lack of formal structure around the Entity's internal compliance program. During the transition to CIP-002-5.1 R1 becoming enforceable the Entity had multiple transition projects managed on a per project basis and as such did not have a single person responsible for assuring NERC compliance prior to transitioning to CIP-002-5.1.</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>A failure to implement a process to identify assets that contain [REDACTED] BES Cyber Systems can result in an entity being unaware of locations where BES Cyber Assets are present. This can then result in BES Cyber Assets not being afforded the protections prescribed by the CIP standards. A failure to implement appropriate [REDACTED]</p> <p>The risk posed by the non-compliance was mitigated by the following factors:</p> <ul style="list-style-type: none"> • The Entity's [REDACTED], which has a maximum generation capability [REDACTED]. A loss of this asset would not pose a serious risk on the BES. • After implementing its BES Cyber System categorization process, the Entity identified [REDACTED] BES Cyber Systems. The BES Cyber Systems at this asset were subsequently categorized [REDACTED] to meet its other compliance obligations for the CIP Version 6 family of NERC Reliability Standards. This demonstrates that at no time during the period of noncompliance was the Entity at risk of violating compliance requirements related to the implementation of physical or cyber security controls. • [REDACTED] • [REDACTED] <p>No harm is known to have occurred.</p> <p>Texas RE 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) implemented their documented CIP-002-5.1 process; and 2) assigned a single individual the responsibility of overseeing NERC compliance. <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
TRE2018020854	CIP-003-6	R2	[REDACTED] (the "Entity")	[REDACTED]	04/01/2017	01/22/2019	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 violation.)			<p>During a Self-Certification conducted from August 24, 2018, through December 20, 2018, Texas RE determined that the Entity, as a [REDACTED] had a potential noncompliance with CIP-003-6 R2. The Entity's cyber security plan did not document Attachment 1, Section 1 Cyber Security Awareness and Section 4 Cyber Security Incident Response Sub-Sections 4.2, 4.5, and 4.6. Additionally, the Entity did not test its Cyber Security Incident response plan for a Reportable Cyber Security Incident.</p> <p>This noncompliance started on April 1, 2017, when CIP-003-6 R2 became enforceable. The noncompliance was partially mitigated when the Entity updated its [REDACTED] to include Sections 4.2, 4.5, and 4.6 of CIP-003-6 Attachment 1. The noncompliance ended on January 22, 2019, when the Entity tested its [REDACTED] using a Reportable Cyber Security Incident.</p> <p>The root cause of this issue was a lack of formal structure around the Entity's internal compliance program. During the transition to CIP-003-6 becoming enforceable, the Entity had multiple transition projects managed on a per project basis and as such did not have a single person responsible for assuring NERC compliance prior to transitioning to CIP-003-6.</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>Failure to include section 4.2 in a [REDACTED] can lead to an entity failing to identify a Cyber Security Incident as a Reportable Cyber Security Incident. This may result in the incident not being reported to E-ISAC.</p> <p>Failure to include section 4.5 in a [REDACTED] can lead to an entity failing to test their Cyber Security Incident Response Plan on a regular basis. This may result in the Cyber Security Incident Response Plan being out of date and not in a usable state when it is needed.</p> <p>Failure to include section 4.6 in a [REDACTED] may result in the Cyber Security Incident Response Plan not being updated in a timely manner. This may result in the Cyber Security Incident Response Plan being out of date and not in a usable state when it is needed.</p> <p>An entity that fails to test their [REDACTED] is at risk of not detecting oversights in the plan or of failing to identify potential improvements in the plan. This can lead to an entity being unprepared should a Cyber Security Incident occur.</p> <p>These risks were mitigated by the following factors. First, the Entity had tested its [REDACTED] using a Cyber Security Incident, however due to an administrative oversight the test was not conducted using a Reportable Cyber Security Incident. Despite the test not using a Reportable Cyber Security Incident, lessons learned for improvements were uncovered and documented. No harm is known to have occurred.</p> <p>Texas RE 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) updated the [REDACTED] to include Sections 4.2, 4.5, and 4.6 of CIP-003-6 Attachment 1; 2) performed a test of the [REDACTED] using a Reportable Cyber Security Incident; and 3) has assigned a single individual responsibility for assuring NERC compliance. <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
WECC2018019299	CIP-002-5.1a	R2: P2.1, P2.2	[REDACTED]	[REDACTED]	10/02/2017	2/13/2018	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 violation.)			<p>On February 28, 2018, the entity submitted a Self-Certification stating, as a [REDACTED] it was in noncompliance with CIP-002-5.1a R2. Specifically, on October 2, 2017, the entity, who previously identified a Low Impact Bulk Electric System (BES) Cyber System (BCS), did not review its identifications in R1 and its parts within 15 months of its prior review of its assets and BCS. Therefore, the entity's CIP Senior Manager or delegate also did not approve the identifications within 15 months of its last approval. The issue ended on February 13, 2018 when the entity and its CIP Senior Manager finalized its review, for a total of 135 days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to adequately perform CIP-002-5.1a R2 Part 2.1 and 2.2. The root cause of the issue was attributed to inadequate process and controls. Specifically, although the entity had a documented process that required a review of its R1 identifications every 12 months, the process did not have controls embedded to ensure the reviews were 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. In this instance, the entity failed to adhere to its documented process to review the identifications in R1 and its parts at least once every 15 calendar months as required by CIP-002-5.1a R2 Part 2.1 and failed to have its CIP Senior Manager or delegate approve its identifications at least once every 15 calendar months as required by CIP-002-5.1a R2 Part 2.2, for a total of 135 days.</p> <p>Failure to review and approve the impact evaluations of BES Cyber Systems from R1 could potentially result in mis-categorizing BES Cyber Systems which can lead to inadequate or non-existent cyber security controls. However, as compensation, the entity had implemented all monitoring systems, and physical and electronic access controls required for LIBCS to the affected Facility. In addition, the affected Facility was a [REDACTED]. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ul style="list-style-type: none"> a. completed the identification review of R1 and its parts and obtained CIP Senior Manager approval; b. updated its procedure to include additional subject matter experts to assist with completion of the required identification reviews in R1 and its parts; and c. implemented automated controls such as task reminders and members of management are notified electronically if the identification review has not been completed and prepared for CIP Senior Manager approval within 30 days prior to its due date. <p>WECC 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
WECC2018019644	CIP-007-6	R4	[REDACTED]	[REDACTED]	1/20/2018	4/26/2018	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 violation.)			<p>On May 7, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in noncompliance with CIP-007-6 R4. Specifically, during the installation of [REDACTED] Bulk Electric System (BES) Cyber Asset (BCA) without External Routable Connectivity (ERC) associated with a Medium Impact BES Cyber System (MIBCS) on the field crew did not verify that security event monitoring was enabled on one BCA. As a result, the BCA was not detecting successful login attempts, failed access attempts, and failed login attempts as required by Part 4.1. The configuration for the BCA was built by the entity’s compliance team and during installation the field crew utilized a checklist to ensure a correct install; however, the checklist did not include verification that security event logging is enabled. The entity discovered this issue on April 26, 2018 while reviewing evidence associated with installation work as part of its internal change management process. This issue began on January 20, 2018, when events should have been logged on the Cyber Asset and ended on April 26, 2018, when event logging was enabled, for a total of 97 days.</p> <p>After reviewing all relevant information, WECC Enforcement determined the entity failed to log events on one BCA, as required by CIP-007-6 R4 Part 4.1 sub-parts 4.1.1 and 4.1.2. The root cause of the issue was attributed to the entity not verifying or validating the accuracy of its tasks. Specifically, the entity enabled the logging configuration on the BCAs prior to the Cyber Asset installation activities however, it did not verify those configurations after installation.</p>					
Risk Assessment			<p>WECC determined 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, the entity failed to log events on one BCA for identification of, and after-the-fact investigations of, Cyber Security Incidents that included detected successful login attempts; detected failed access attempts; and failed login attempts as required by CIP-007-6 R4 Part 4.1 sub-parts 4.1.1 and 4.1.2.</p> <p>However, as compensation, the entity changed the default password on the BCA prior to installation and the BCA does not have ERC. No suspicious or malicious activities or incidents were identified during the issue. The entity implemented good detective controls in the form of an internal change management process that included reviewing evidence associated with installation work which was how this issue was discovered. No harm is known to have occurred.</p> <p>The entity’s prior compliance history with CIP-007-6 R4 includes NERC Violation ID [REDACTED]. WECC determined the entity’s compliance history should not serve as a basis for pursuing an enforcement action and/or applying a penalty because it is only one instance of previous noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) enabled password event logging on the one BCA in scope; and 2) updated the checklist used when installing BCAs to include a step to enable password event logging if it has been disabled. This checklist is a required checklist which is currently being used but now includes an additional verification control for ensuring that password event logging is enabled. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019369	CIP-007-6	R2: P2: 2.2; 2.4	[REDACTED]	[REDACTED]	Instance 1: 7/1/2016 Instance 2: 4/14/2017	Instance 1: 2/12/2018 Instance 2: 4/27/2017	Compliance 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 violation.)			<p>During a Compliance Audit conducted [REDACTED], WECC determined the entity, as a [REDACTED], had a potential noncompliance with CIP-007-6 R2 Parts 2.2 and 2.4. In the first instance, the entity failed to document a process for CIP Senior Manager approval of revisions or extensions to security patch mitigation plans as required by CIP-007-6 R2 Part 2.4. The first instance began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity and ended on February 12, 2018, when the entity updated its procedure to include obtaining CIP Senior Manager approval, for a total of 591 days.</p> <p>In the second instance, the entity failed to conduct an evaluation of security patches every 35 days as required by CIP-007-6 R2 Part 2.2. The second instance began on April 14, 2017, the day after the evaluation of applicability of any released security patches should have occurred and ended on April 27, 2017, when a security patch evaluation was conducted, for a total of 14 days.</p> <p>After reviewing all relevant information, WECC Enforcement concurred with the audit findings as stated above. The root cause of these instances was less than adequate processes or procedures. Specifically, the entity did not document a process for CIP Senior Manager approval of revisions or extensions to mitigation plans. Second, the entity did not implement detective controls in its security patch management process, therefore, staff were not alerted of the missed evaluation cycle.</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. In the first instance, the entity failed to document a process for CIP Senior Manager approval of revisions or extensions to security patch mitigation plans as required by CIP-007-6 R2 Part 2.4. In the second instance, the entity failed to conduct an evaluation of security patches every 35 days as required by CIP-007-6 R2 Part 2.2.</p> <p>In the first instance, the entity did not implement controls to ensure its procedures contained all the requirements of the Standards however, the issue was administrative and not technical, which lessens the risk. As further compensation, in the second instance, the Cyber Assets were protected by firewalls, malware prevention, intrusion detection systems, and intrusion prevention systems. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate these instances, the entity has:</p> <ol style="list-style-type: none"> a. developed a security patch management mitigation approval process; b. provided training to staff on the process for obtaining CIP Senior Manager approval to revise or extend a mitigation plan; c. conducted a security patch evaluation; and d. provided training to employees that emphasized the importance of completing and documenting the 35-day security patch evaluation. <p>WECC 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
WECC2018019945	CIP-010-2	R1; P1.3 P1.4	[REDACTED]	[REDACTED]	8/25/2016	3/27/2019	Compliance 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 violation.)			<p>During a Compliance Audit conducted [REDACTED], WECC determined the entity, as a [REDACTED], had a potential noncompliance with CIP-010-2 R1. Specifically, the entity was not able to provide evidence to demonstrate it had updated baseline configurations as necessary within 30 calendar days of completing one change as required by Part 1.3. Additionally, the entity was not able to provide evidence to demonstrate that prior to the one change, it determined whether the required cyber security controls in CIP-005 and CIP-007 that could be impacted were not adversely affected and document the results of the verification as required by Part 1.4. The Cyber Assets in scope of the one change requiring Part 1.3 included [REDACTED] Bulk Electric System (BES) Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS) in the primary Control Center, and the one change requiring Part 1.4 included [REDACTED] BCAs, [REDACTED] Electronic Access Control or Monitoring Systems (EACMS), [REDACTED] Protected Cyber Asset (PCA), and [REDACTED] Physical Access Control System associated with a MIBCS. The MIBCS were in both the primary and backup Control Centers. The Part 1.3 issue began on September 2, 2016, the 31st day after baseline configuration changes should have been updated and ended on July 5, 2017, when baseline configuration changes were updated, for a total of 307 days. The Part 1.4 issue began on August 25, 2016, when baseline configuration changes should have considered the impact of cyber security controls in CIP-005 and CIP-007 prior to the change and ended on March 27, 2019 when the entity updated its configuration change management procedures, for a total of 945 days.</p> <p>After reviewing all relevant information, WECC Enforcement concurred with the audit findings as stated above. The root cause of the issue was attributed to less than adequate procedures. Specifically, the entity utilized a change request form that did not allow the reviewer of the change to add notes and the entity did not have an implementation procedure to ensure cyber security controls as required in Part 1.3 and Part 1.4.</p>					
Risk Assessment			<p>WECC determined 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, the entity failed to update the baseline configuration as necessary within 30 calendar days of completing the change for a change that deviated from the existing baseline configuration, and prior to the change, failed to determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; following the change, verify that identified required cyber security controls were not adversely affected; and document the results of the verification as required by CIP-010-2 R1 Part 1.3 and Part 1.4.</p> <p>However, as compensation, the entity monitored network and external service provider activity to detect potential Cyber Security Incidents; had an intrusion prevention system running for the Cyber Assets at both the primary and backup Control Centers; and log files were sent to a SIEM with notifications via email, which were verified at audit. No harm is known to have occurred.</p> <p>The entity does not have any relevant previous violations of this or similar Standards and Requirements</p>					
Mitigation			<p>To mitigate this noncompliance, the entity: conducted vulnerability assessments on the seven Cyber Assets in scope;</p> <ol style="list-style-type: none"> 1) documented the results and any action plans to remediate or mitigate issues identified from the assessments; 2) revised its vulnerability assessment procedure to clearly define the steps to perform a paper or active vulnerability assessment and the documentation required to demonstrate the activities were performed; 3) updated all personnel on the revised procedure during a status meeting; and 4) distributed the procedure to appropriate personnel through its document management program which includes an acknowledgement of receipt and review. <p>WECC 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
WECC2018019947	CIP-010-2	R3; P3.1 P3.4	[REDACTED]	[REDACTED]	7/1/2017	12/18/2018	Compliance 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 violation.)			<p>During a Compliance Audit conducted [REDACTED], WECC determined the entity, as a [REDACTED], had a potential noncompliance with CIP-010-2 R3. Specifically, the entity was not able to provide supporting evidence to demonstrate it had performed a paper or active vulnerability assessment by July 1, 2017 for [REDACTED] Cyber Assets of which [REDACTED] were EACMS, and [REDACTED] was a PCA, associated with its MIBCS as required by CIP-010-2 R3 Part 3.1, and document the results of the vulnerability assessment as required by CIP-010-2 R3 Part 3.4. This issue began on July 1, 2017, when the Standard and Requirements became mandatory and enforceable to the entity and ended on December 18, 2018, when vulnerability assessments were completed and documented, for a total of 536 days</p> <p>After reviewing all relevant information, WECC Enforcement concurred with the audit findings as stated above. The root cause of this issue was attributed to a misunderstanding of what evidence was required to demonstrate compliance. Specifically, the entity maintained a spreadsheet with dates, but no supporting evidence that vulnerability assessments were conducted.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to conduct a paper or active vulnerability assessment by July 1, 2017 and failed to document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified including the planned date of completing the action plan and the execution status of any remediation or mitigation action items as required by CIP-010-2 R3 Part 3.1 and Part 3.4, respectively.</p> <p>As compensation, the entity monitored network and external service provider activity to detect potential Cyber Security Incidents; had an intrusion prevention system running for the Cyber Assets at both the primary and backup Control Centers; and log files were sent to a SIEM with notifications via email, which were verified at audit. No harm is known to have occurred.</p> <p>The entity does not have any relevant previous violations of this or similar Standards and Requirements</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) conducted vulnerability assessments on the [REDACTED] Cyber Assets in scope; 2) documented the results and any action plans to remediate or mitigate issues identified from the assessments; 3) revised its vulnerability assessment procedure to clearly define the steps to perform a paper or active vulnerability assessment and the documentation required to demonstrate the activities were performed; 4) updated all personnel on the revised procedure during a status meeting; and 5) distributed the procedure to appropriate personnel through its document management program which includes an acknowledgement of receipt and review. <p>WECC has verified the completion of all mitigation activity.</p>					

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 Exception 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	FRCC2019021353		Yes	Yes	Yes									Category 2 – 12: 2 years
2	MRO2018019026			Yes	Yes									Category 2 – 12: 2 years
3	MRO2018020514			Yes	Yes									Category 2 – 12: 2 years
4	MRO2018020515			Yes	Yes									Category 2 – 12: 2 years
5	MRO2018020766			Yes	Yes								Yes	Category 2 – 12: 2 years
6	MRO2018020827			Yes	Yes									Category 2 – 12: 2 years
7	MRO2018020828			Yes	Yes									Category 2 – 12: 2 years
8	MRO2018020830			Yes	Yes									Category 2 – 12: 2 years
9	MRO2019020981			Yes	Yes									Category 2 – 12: 2 years
10	MRO2019020982			Yes	Yes									Category 2 – 12: 2 years
11	MRO2019020983	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
12	MRO2019021189			Yes	Yes									Category 2 – 12: 2 years
13	SPP2018019594			Yes	Yes								Yes	Category 2 – 12: 2 years
14	SPP2018019595			Yes	Yes									Category 2 – 12: 2 years
15	NPCC2018020451	Yes		Yes	Yes									Categories 2 – 12: 2 year Category 1: 3 years
16	NPCC2018019967	Yes		Yes	Yes						Yes			Categories 2 – 12: 2 year Category 1: 3 years
17	RFC2018019906	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
18	RFC2018020672	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
19	RFC2018020851	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
20	RFC2018020066	Yes	Yes	Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
21	RFC2018020067	Yes	Yes	Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
22	RFC2018020068	Yes	Yes	Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
23	RFC2018020070	Yes	Yes	Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
24	RFC2018020379	Yes		Yes	Yes	Yes								Category 1: 3 years; Category 2-12: 2 years
25	RFC2018020510	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
26	RFC2018020615	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
27	RFC2018020511	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
28	RFC2017018768	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; 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)
29	RFC2017018769	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
30	RFC2017018771	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
31	RFC2017018773	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
32	RFC2018020642	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
33	SERC2017016826		Yes	Yes					Yes					Category 2 – 12: 2 year
34	SERC2018018918			Yes	Yes					Yes				Category 2 – 12: 2 year
35	SERC2016016518			Yes	Yes					Yes				Category 2 – 12: 2 year
36	SERC2017016992			Yes	Yes					Yes				Category 2 – 12: 2 year
37	SERC2018019715			Yes	Yes									Category 2 – 12: 2 year
38	TRE2017018450	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
39	TRE2018019854	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
40	TRE2017018193	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
41	TRE2017018194	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
42	TRE2018020236			Yes	Yes									Category 2 – 12: 2 year
43	TRE2019021079	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
44	TRE2017017563	Yes		Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 year
45	TRE2017018359	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
46	TRE2017018372	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
47	TRE2017018188	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
48	TRE2019021059	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
49	TRE2019021060	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
50	TRE2018020691	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
51	TRE2018020692	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
52	TRE2019021290	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
53	TRE2019021291	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
54	WECC2017018873			Yes	Yes					Yes	Yes			Category 2 – 12: 2 year
55	WECC2018020256			Yes	Yes									Category 2 – 12: 2 year
56	WECC2017018363			Yes	Yes									Category 2 – 12: 2 year
57	WECC2019021066			Yes	Yes									Category 2 – 12: 2 year

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)
58	WECC2019021268	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
59	WECC2016016694			Yes	Yes					Yes				Category 2 – 12: 2 year
60	WECC2017018244			Yes	Yes					Yes	Yes			Category 2 – 12: 2 year
61	WECC2018020468			Yes	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
FRCC2019021353	CIP-010-2	R4.	[REDACTED] ("the Entity")	[REDACTED]	5/1/2018	6/1/2018	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 April 17, 2019, the Entity submitted a Self-Report stating that [REDACTED] it was in noncompliance with CIP-010-2 R4.</p> <p>This noncompliance started on May 1, 2018, when the Entity failed to install Transient Cyber Asset (TCA) security patches and connected the TCA to a BES Cyber Asset (BCA) and ended on June 1, 2018, when the security patches were installed.</p> <p>Specifically, the Entity had one (1) TCA where the [REDACTED]-related security patches were installed, but failed to assess and patch the third-party, non-[REDACTED] related applications for the month of May 2018 before connecting the TCA to a BCA. The TCA was serially connected to a medium impact BCA for one day (May 7, 2018).</p> <p>An extent of condition review determined there were no additional occurrences.</p> <p>The causes of this noncompliance were lack of 1) clarity of internal documentation as to specific team assessment and patching responsibilities; and 2) an automated reminder with escalation.</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>The risk was reduced due to the following 1) the TCA received all [REDACTED]-related security patches and only third-party software applications were not assessed; and 2) the TCA was only used once during the unpatched time frame while attached to a medium impact BCA.</p> <p>No harm is known to have occurred.</p> <p>The Region 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) Performed a root cause analysis; 2) Performed an extent of condition analysis; 3) Updated Operating Instructions with Internal Controls; 4) Created an automated task for TCA patch assessment that is generated monthly with alerts and escalation; 5) Added an account expiration to the TCA device that will disable the TCA after 80 days if patching has not occurred; and 6) Provided training regarding the automated task and revised Operating Instructions. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019026	CIP-009-6	R3	[REDACTED] (the Entity)	[REDACTED]	03/08/2017	03/31/2017	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 November 17, 2017, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-009-6 R3. Specifically, the Entity failed to update a recovery plan within 90 calendar days after completion of a recovery plan test as required by P3.2.</p> <p>The cause of the noncompliance was that the Entity failed to follow its documented process with regard to updating recovery plans.</p> <p>The noncompliance started on March 8, 2017, 91 days after the recovery test, and ended on March 31, 2017 when updates to the applicable recovery plan were 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. Lessons learned from the exercise had been discussed with SMEs during the exercise debriefing, meaning the noncompliance was limited to the failure to update the recovery plan documentation within the 90 days. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the recovery plan; 2) increased the Compliance Group's involvement in recovery tests; and 3) incorporated an applicable workflow into its compliance management system. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020514	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	05/23/2018	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 violation.)			<p>On October 5, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2. One patch associated with multiple BES Cyber Assets, PCAs, and one EACMS was not evaluated within 35 days from the previous evaluation. The Entity states that the patch was actually timely evaluated but incorrectly deemed to be not applicable; upon further review it was later determined that the patch was applicable to multiple Cyber Assets.</p> <p>The cause of the noncompliance was that Entity's process for evaluating patch sources lacked detail when verifying a patch source to applicable Cyber Assets.</p> <p>The noncompliance started on May 23, 2018, 36 days after the last evaluation, and ended on July 17, 2018 when the patch was added to a 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. The Entity reports that the patch was timely applied after the patch was added to the mitigation plan. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) added the patch to a mitigation plan; and 2) updated its patch evaluation process to include an additional review and verification control to ensure the patch source is evaluated accurately. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020515	CIP-010-2	R4	[REDACTED] (the Entity)	[REDACTED]	07/24/2018	07/24/2018	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 October 5, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R4. Per the Entity, on July 24, 2018, a relay specialist connected an unauthorized laptop to three medium impact BES Cyber Assets (relays) at a Transmission Facility to perform relay maintenance. The laptop was not an authorized Transient Cyber Asset (TCA). The issue was identified on July 26, 2018 when the same relay specialist was performing relay maintenance trip check at a different Transmission Facility while using a TCA and realized what had happened on July 24, 2018. The relay specialist then reported the matter.</p> <p>The cause of the noncompliance was that the Entity failed to follow its TCA process.</p> <p>The noncompliance started on July 24, 2018, when the laptop was connected to the relays, and ended later on July 24, 2018, when the laptop was disconnected from the relays.</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 Entity states that the laptop that was used was up to date with security patches and a vulnerability and malware assessment identified no security concerns. The Entity reports that a review of the relays identified no security concerns. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) disconnected the laptop from the BES Cyber Assets; 2) reinforced with relay specialists the TCA processes associated to medium impact BES Cyber Systems; 3) reviewed and updated processes associated to CIP-010-2 R4; 4) increased signage in and around medium impact BES Cyber Systems; and 5) implemented additional reminders of TCA use during bi-weekly staff meetings and monthly safety meetings. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020766	CIP-002-5.1a	R2	[REDACTED] (the Entity)	[REDACTED]	06/01/2018	06/28/2018	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 violation.)			<p>On October 10, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-002-5.1a R2. The Entity failed to gain the CIP Senior Manager's approval for the identifications per CIP-002-5.1a P2.2 within 15 calendar months of the last approval. The Entity states that several reviews of the CIP-002-5.1a R1 identifications were conducted. The SME responsible for tracking CIP-002-5.1a R2 completion mistakenly believed that these reviews fulfilled the CIP-002-5.1a P2.2 requirement. The noncompliance was discovered while performing a mitigating activity associated with CIP-003-6-1 ([REDACTED]), which involved the failure of the CIP Senior Manager to approve a policy document.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for gaining CIP Senior Manager approval of identifications under CIP-002-5.1a R1.</p> <p>The noncompliance started June 1, 2018 when the CIP Senior Manager did not approve the CIP-002-5.1a R1 identifications within 15 calendar months, and ended on June 28, 2018 when the CIP Senior Manager approved the CIP-002-5.1a R1 identifications.</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 Entity states that the assessments were performed under requirement CIP-002-5.1a P2.1 and the noncompliance was limited to failing to have the CIP Senior Manager approve the identifications. Further, the Entity reports that the noncompliance was limited to receiving approval on the review of assets that contain low impact BES Cyber Systems (P1.3) as assets that contain medium impact BES Cyber Systems are on a different review cycle. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) had its CIP Senior Manager review and approve the identifications; 2) created a calendar reminder with a 12 month interval, the reminder is sent to a distribution list that includes staff involved in the reviews and the reminder contains specific information related to CIP-002-5.1a R2; and 3) it added the review and approval document to the Entity's document tracking tool to monitor the lifecycle of the document. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020827	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	03/14/2018	04/23/2018	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 October 9, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1.</p> <p>On April 23, 2018, during a scheduled review, the Entity's IT staff discovered that six Windows security patches were downloaded and installed automatically on PACS controllers without authorization as required by CIP-010-2 P1.2 and P1.4. The Entity reports that the patches were downloaded and installed by the Windows update because of an incorrectly configured [REDACTED] group. This misconfiguration occurred on March 14, 2018 when the IT department performed maintenance on the PACS server.</p> <p>The cause of the noncompliance was that misconfiguration prevented the Entity from following its documented process with regard to authorizing and documenting changes to the baseline.</p> <p>This noncompliance started on March 14, 2018, and ended on April 23, 2018 when the correct [REDACTED] group was assigned and the incorrect [REDACTED] group was removed.</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 Entity states that the noncompliance was limited to PACS controllers that do not directly control the BPS. Further, the Entity reports that the patches would have been installed as part of the normal patching cycle. Additionally, the Entity states that upon discovering the noncompliance, it confirmed that no security controls were adversely impacted by the security patches. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity removed the incorrect active directory group was removed and assigned the devices to a correct [REDACTED] group.</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
MRO2018020828	CIP-007-6	R5	[REDACTED] (the Entity)	[REDACTED]	01/08/2018	07/09/2018	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 October 9, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5. On July 5, 2018, the Entity's IT department was updating the shared passwords as part of an annual shared password change for IT managed assets that are within NERC CIP scope. The Entity found that the default passwords for the two newly installed PACS controllers for the Control Center and the backup Control Center were not changed as required by CIP-007-6 P5.4.</p> <p>The cause of the noncompliance is that the Entity's documented process was deficient, as it did not verify changing default passwords.</p> <p>This noncompliance started on January 8, 2018 when the devices were deployed, and ended on July 9, 2018 when the default 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. The Entity stated that the PACS controllers were located in a DMZ behind a corporate firewall, which blocks access to the controller from the Internet and the PACS controllers were located within a functioning PSP, which would prevent an adversary exploiting the default password through local access. Further, the Entity reports that compromise of the PACS controllers would result in a limited functionality of the door latches that are hardwired to the specific controller, the PACS controller does not have the ability to create additional authorized individuals. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) changed the default passwords for the devices; and 2) created two new fields in the Cyber Asset add or remove workflow to provide a reminder to change the default password. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020830	CIP-007-6	R4	[REDACTED] (the Entity)	[REDACTED]	09/09/2018	09/12/2018	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 violation.)			<p>On October 9, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R4. On September 11, 2018, during an assigned compliance task review, the Entity's compliance department discovered that a review of logged events was not completed by September 8, 2018 as required by CIP-007-6 P4.4.</p> <p>The cause of the noncompliance was that the Entity's implementation of its CIP-007-6 P4.4 process was insufficient with regards to ensuring the review of logged events timely occurred.</p> <p>This noncompliance started on September 9, 2018, 16 days after the last review of logged events, and ended on September 12, 2018 when the review was completed.</p>					
Risk Assessment			This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity states that during the noncompliance it had no gap in its other measures such as baseline monitoring, firewalls, alerts, and methods to prevent malicious code. No harm is known to have occurred.					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed the review of logged events; and 2) updated its compliance management tool, which is used by applicable SMEs, to generate a report to show the compliance tasks due within ten days including the CIP-007-6 P4.4 review. The report is prominently posted on the tool's home screen and the due days are color coded to show the deadline status. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019020981	CIP-010-2	R4	[REDACTED] (the Entity)	[REDACTED]	07/20/2018	07/20/2018	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 January 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R4. Specifically, a substation relay specialist connected a corporate laptop to medium impact BES Cyber Assets (BCAs) to collect intelligent electronic device (IED) information at a substation. The Entity states that after completing the work the technician realized that he should have used a designated CIP Transient Cyber Asset (TCA) laptop to collect the IED information and promptly reported the incident to substation management who informed the compliance department.</p> <p>The cause of the noncompliance was that the Entity failed to follow its documented TCA plan.</p> <p>The noncompliance began on July 20, 2018, when the technician connected the corporate laptop to the BCAs and ended on July 20, 2018, when the corporate laptop was disconnected from the 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. The Entity reports that the substation had no External Routable Connectivity. Additionally, the Entity states that the corporate laptop had anti-virus installed, real-time alerts from the laptop are monitored by the cyber security department, and that a subsequent scan of the laptop did not detect malicious code. Finally, the BCAs that the technician connected the laptop to were reviewed and determined to have no baseline changes. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) disconnected the corporate laptop; 2) installed new D-type port connectors on medium impact BES Cyber Assets to differentiate the pin configuration between the TCA device and the corporate laptops; and 3) added the new cable adaptors to CIP TCA laptop carriers to help ensure that only CIP TCA laptops could be physically connected to medium impact BES 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
MRO2019020982	CIP-011-2	R1	[REDACTED] (the Entity)	[REDACTED]	06/12/2018	08/02/2018	Self-Log	12/31/2019 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 violation.)			<p>On January 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-011-2 R1. Specifically, the Entity failed to implement its procedures for protecting and securely handling BES Cyber System Information (BES CSI). Per the Entity, on July 31, 2018, an employee resigned from the Entity; while cleaning the computer, the manager discovered that BES CSI was stored on the computer. The information contained a vulnerability assessment (VA) report which included a description of risks, Cyber Asset names, IP addresses and how the identified risks could be exploited. The VA report was created on June 12, 2018.</p> <p>The cause of the noncompliance was that the Entity failed to properly implement its documented process for identifying the BCSI storage location.</p> <p>The noncompliance started on June 12, 2018 when the VA report was created and stored on the computer which was not designated as a BES CSI storage location, and ended on August 2, 2018 when the computer was wiped to ensure complete destruction of BES CSI on the computer.</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 Entity states that the former employee's computer was secured on the same day he separated from the Entity. The Entity reports that the information did not provide access information to any BES Cyber Assets. The Entity states that the former employee had permission and access to other BES CSI and the issue was limited to the computer not being designated as BES CSI designated storage location. No harm is known to have occurred.</p> <p>To mitigate the risk of reoccurrence while mitigating activities are being completed, the Entity has updated the applicable process document and provided refresher training to applicable staff.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) wiped the computer to ensure complete destruction of the BES CSI; 2) updated the documented process for identifying BES CSI to assist staff; and 3) had applicable staff review the updated documented process. <p>To mitigate this noncompliance, the Entity will by December 31, 2019, review and revise its CIP training, including the BES CSI training.</p> <p>The amount of time required to complete the mitigating activities is related to the training schedule.</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
MRO2019020983	CIP-004-6	R5	[REDACTED] (the Entity)	[REDACTED]	10/11/2018	11/25/2018	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 January 10 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. After an employee was terminated on October 10, 2018, the manager failed to collect the Control Center keys within 24 hours as required by CIP-004-6 P5.1. The Entity discovered the noncompliance when the terminated employee reported the matter to the Entity; the keys were collected immediately.</p> <p>The cause of the noncompliance was that Entity’s key tracking process was deficient.</p> <p>The noncompliance started on October 11, 2018, 24 hours after the employee was terminated, and ended on November 25, 2018 when the door keys were collected by the Entity’s staff.</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 Entity states that the employee was current on his personnel risk assessment (PRA) and CIP training. Additionally, the Entity reports that terminated employee’s electronic access credentials to BES Cyber Assets had been promptly removed. [REDACTED] Additionally, the Entity states that the Control Center is monitored 24 hours a day. Finally, the Entity reports that the termination was not for cause. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) collected the door key; 2) re-keyed the Control Center; 3) created a spreadsheet to track keys; and 4) stopped issuing physical keys to employees; a lockbox was installed to hold the PSP door key and a group of authorized employees were given access to the lockbox. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021189	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	04/16/2018	05/14/2018	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 violation.)			<p>On January 14, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2. The Entity states that it failed to evaluate one patch applicable to multiple BES Cyber Assets. The Entity states that the patch was released by its EMS vendor but was not included in the next 35-calendar day evaluation cycle. The Entity reports that it detected the patch during a scheduled quality control review and the patch was reviewed during the subsequent evaluation.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for finding new patches released by its identified source to be evaluated.</p> <p>The noncompliance began on April 17, 2018, 36 days after the last evaluation, and ended on May 14, 2018 when the patch was evaluated.</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 did not result in the patch missing multiple patching cycles. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) evaluated the patch; and 2) held a coaching session by a member of the change management team for members of the team that are responsible for performing patch discovery. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2018019594	CIP-010-2	R1	██████████ (the Entity)	██████████	08/16/2017	10/18/2017	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 violation.)			<p>On April 26, 2018, the Entity submitted a Self-Report stating that as a ██████████, it was in noncompliance with CIP-010-2 R1.</p> <p>The Entity states that for two PACS servers, it failed to obtain approval for a change (P1.2) and failed to update the baseline following a change within 30 days (P1.3). The Entity reports that it was commissioning four servers – two for production use as PACS devices and two for non-production use. A last-minute decision to switch the production with the non-production servers resulted in the syslog forwarder software not being installed on the new production servers when deployed on August 3, 2017. The Entity discovered this on August 4, 2017, when the servers were not appearing on the PACS logging reports and installed the software on August 16, 2017 without following its proper change management process, which required updating of the baseline within 30 days. This noncompliance occurred during the Entity’s efforts to mitigate ██████████.</p> <p>The cause of the noncompliance was that the Entity failed to follow its change management process by not generating a change request to kick off its change management process when making a change to two PACS servers, which resulted in steps not being completed (baseline documentation).</p> <p>The issue began on August 16, 2017, when it made an unapproved change, and ended on October 18, 2017 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 Entity states that the issue was resolved through the update of documentation, rather than implementation of a change to the system. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) confirmed the need for the change and updated the baselines for the two servers; 2) performed informal one-on-one training and held multiple refresher sessions with members of the team responsible for the servers; and 3) updated its build specification document to include a section for the deployment of devices subject to CIP Standards. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2018019595	CIP-007-6	R4	██████████ (the Entity)	██████████	08/03/2017	08/16/2017	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 April 26, 2018, the Entity submitted a Self-Report stating that as a ██████████, it was in noncompliance with CIP-007-6 R4. The Entity failed to install a syslog forwarder on its two PACS servers when they were deployed. The Entity states that it relies upon a functional syslog forwarder to fulfill the requirements for alerting (P4.3), log retention (P4.4), and log review (P4.5). As a result, alerting, log retention, and log review did not occur. The noncompliance was discovered on August 4, 2018 when the PACS logging reports did not include the two new PACS servers.</p> <p>The cause of the noncompliance was that the Entity's process lacked sufficient detail to ensure the log forwarding software was installed and functional on its PACS servers prior to deployment.</p> <p>This noncompliance started on August 3, 2017 when the devices were deployed, and ended on August 16, 2017, when the syslog forwarder was installed on 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. Per the Entity, the devices had the ability to locally save approximately 15 days of logs, meaning that the noncompliance did not result in the loss of after-the-fact forensics evidence. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) installed the log forwarding software on the devices; 2) added the installation of the log forwarding software to its server build checklist; and 3) sent a refresher email to its physical security, IT security, and corporate server departments to reiterate its change management procedures. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018020451	CIP-007-6	R4.	[REDACTED]	[REDACTED]	07/01/2016	04/27/2018	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 violation.)			<p>On September 20, 2018, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on April 19, 2018 it was in noncompliance with CIP-007-6 R4. after performing a CIP asset review for the first quarter of 2018.</p> <p>This noncompliance started on July 1, 2016 when the entity failed to generate alerts for security events, for detected failure of event logging. The entity also failed to retain applicable event logs for three (3) [REDACTED] BES Cyber Assets for at least the last 90 consecutive calendar days. The entity further failed to review a summarization or sampling of logged events for the three (3) [REDACTED] BES Cyber Assets. The noncompliance ended on April 27, 2018 when the entity set up a method to identify systems that have stopped logging, configured the three (3) Cyber Assets to send logs to its central monitoring system, and reviewed the logs of the three (3) Cyber Assets to identify undetected Cyber Security Incidents.</p> <p>The root cause of this noncompliance was lack of a control to identify failure of event logging. The three cyber assets were not configured properly in the entity's monitoring system.</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 generating alerts for security events and detected failure of event logging, the entity may not be alerted to a malicious actor that has disabled logging. This could hinder the entity's ability to identify and respond to Cyber Security Incidents that are aimed at misusing or impacting the availability of BES Cyber Systems.</p> <p>The entity reduced the risk of a potential Cyber Asset compromise going unnoticed b [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) Configured logging for the 3 Cyber Assets in scope 2) Reviewed summarization of logs 3) Established process to identify assets that are not logging; and 4) Performed an Extent of Condition 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019967	CIP-005-5	R1.	[REDACTED]	[REDACTED]	07/01/2016	07/31/2019	On-site Audit	7/31/2019
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>During an audit conducted from [REDACTED] NPCC determined that [REDACTED] (the entity), as a [REDACTED] was in noncompliance with CIP-005-5 R1. (1.3.). The entity failed to require inbound and outbound access permissions at Electronic Access Points (EAPs) for [REDACTED] Impact BES Cyber Systems.</p> <p>This noncompliance started on July 1, 2016 when the entity failed to require inbound and outbound access permissions at twenty-one (21) EAPs for [REDACTED] Impact BES Cyber Systems. The noncompliance ended on July 31, 2019, when the entity upgraded its firmware and configured inbound and outbound rules and deny all other access by default.</p> <p>The root cause of this noncompliance was due to limitations of the firewalls that were deployed.</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>Normally, overly permissive firewall rules can provide paths into an ESP that can be exploited to gain unauthorized entry. However, in this case the entity reduced the risk of a malicious individual exploiting an overly permissive firewall rule to gain unauthorized access [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) Replaced the devices in scope with devices that enable support of additional rules. 2) Upgraded the firmware on the twenty-one devices; and 3) Configured the devices with inbound and outbound rules and to deny all other access by default. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019906	CIP-010-2	R4	[REDACTED]	[REDACTED]	4/18/2018	4/18/2018	Self-Report	November 22, 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 June 7, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-010-2 R4. On April 18, 2018, the entity discovered that a contractor plugged his laptop (a non-CIP Cyber Asset) into the front, serial port of an alarm relay [REDACTED] within a substation Electronic Security Perimeter (PSP). This violated the entity's [REDACTED] that prohibits temporarily connected devices, such as laptops, from being connected to the [REDACTED] at CIP substations.</p> <p>The contractor at issue had approved CIP physical and electronic access to the substation, had completed his required CIP training, and had an up-to-date Personnel Risk Assessment (PRA). Additionally, the contractor had completed specific training on the prohibition of direct, serial access to relays in CIP stations, and training on the approved method of connecting a laptop via the entity's intermediate system.</p> <p>This noncompliance involves the management practice of workforce management through ineffective training and asset and configuration management. The contractor made an incorrect assumption that because the alarm relay was a non-protection device it must be on a non-critical network and therefore connecting his laptop directly via the front, serial port was permitted. This assumption was incorrect [REDACTED]. Ineffective training is a contributing cause of this noncompliance because [REDACTED] the contractor did not consult design documentation to verify the network type of the relay. There was also no signage, labeling, or other controls to help the contractor distinguish that the relay was on the critical network. That lack of signage, labeling, or other controls is a root cause of this noncompliance and reflects poor asset and configuration management.</p> <p>This noncompliance started on April 18, 2018, when an entity contractor incorrectly plugged his laptop (a non-CIP Cyber Asset) into an Alarm Relay and ended 20 minutes later on April 18, 2018, when the entity contractor unplugged his laptop from the Alarm 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 based on the following factors. The risk posed by this noncompliance is allowing for the potential compromise of the relay and other systems through a laptop that is not authorized for that purpose and may not be fully protected. The risk is minimized because the contractor did not have a valid password to access the relay. Consequently, the contractor's laptop never obtained electronic access to the relay, which minimizes the risk. (Additionally, the contractor at issue had approved CIP physical and electronic access to the substation, had completed his required CIP training, and had an up-to-date PRA at the time of 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 entity quickly identified, assessed, and corrected the instant noncompliance and the noncompliance posed only minimal risk.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity will complete the following mitigation activities by November 22, 2019:</p> <ol style="list-style-type: none"> 1) instructed the contractor to unplug the laptop and informed him of the entity's policy; 2) modified its [REDACTED] Policy to highlight the specific list of allowable connections to BCS equipment and the allowable uses of company laptops related to BCS equipment; 3) discussed the revised policy with [REDACTED] personnel during a conference call to reinforce the acceptable conditions for laptop connections; 4) [REDACTED] 5) will develop signage and execute a plan to apply signage at 100% of its Medium Impact Substations; and 6) will revise the transmission substation commissioning process to ensure signage is installed. <p>Additional time is needed for this ongoing mitigation because of the large amount of time it will take to develop and apply signage at 100% of the entity's Medium Impact Substations.</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
RFC2018020672	CIP-007-6	R5	[REDACTED]	[REDACTED]	7/20/2018	7/26/2018	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 9, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-007-6 R5. On July 23, 2018, as part of the entity's annual password change process, the entity discovered that the password for a local account with access to a management console, classified as a Protected Cyber Asset (PCA) in support of an [REDACTED] server, had not been changed by the deadline of July 19, 2018. The management console is located within a Physical Security Perimeter (PSP). The entity failed to comply with the annual password change process that requires the entity to change the password within 15 months after its previous password change. The password had previously been changed on April 20, 2017 and was required to be changed by July 19, 2018.</p> <p>On May 30, 2018, the account owner was notified that the password needed to be changed by the July 19, 2018 deadline. The team responsible for monitoring the status of the password change, however, did not perform effective monitoring. The team responsible failed to escalate the needed password change and the password was not changed to meet the 15 month calendar deadline. On July 23, 2018, the team responsible for monitoring the status of the password change notified the end user of the local account of the need to change the password. The end user determined that his access could be removed as the user had minimal need to use the account.</p> <p>This noncompliance involves the management practices of validation and verification. The root cause of the noncompliance is a weakness in the verification control used by the entity to monitor and escalate the 15 month password change requirement. The control lacked sufficient reminders and management escalation to ensure compliance by the required deadline.</p> <p>This noncompliance started on July 20, 2018, when the entity was required to change the password on the management console, and ended on July 26, 2018, when the account owner's access to the account was revoked and the account was removed from the PCA.</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 timely change the password is it makes it easier for a bad actor to compromise the password and access the device. This risk is minimized by the following factors. First, the incident was isolated to one local account used on one PCA. Second, based on retained logs, the account was never used to log into the PCA during the noncompliance. Third, the entity had additional safeguards in place that would make it difficult to compromise the asset. [REDACTED] Physical access to the device required approved access into a PSP where the device was located. Fourth, the entity quickly identified, assessed, and corrected this noncompliance as the duration was only six days. 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 root causes of the prior noncompliances and the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) revoked the account owner's access and the account was removed from the Protected Cyber Asset; 2) performed an Extent of Condition Review and no other account passwords were out of compliance with CIP-007-6 R5.6; and 3) modified an existing preventative control to monitor password change deadlines to include (i) multiple notifications and escalation to account owners and management; (ii) a process to disable or remove accounts (if passwords are not changed) prior to the 15 month deadline; and (iii) perform monitoring of upcoming password changes on a more frequent interval (<i>i.e.</i> weekly). <p>ReliabilityFirst 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
RFC2018020851	CIP-011-2	R1	[REDACTED]	[REDACTED]	4/24/2018	4/24/2018	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 18, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-011-2 R1.</p> <p>On April 24, 2018, during the course of normal business activities, an entity employee went to print out information (a drawing) containing Bulk Electric System Cyber Security Information (BCSI). When this employee went to obtain the printout, the employee discovered that it had not printed. The employee returned to his workstation to print the information again. The employee then returned to the printer and obtained a printout. The printout obtained by the employee was the first attempt to print. The second printout emerged moments later. The employee returned to his workstation unaware that the second copy had printed and had been left on the printer. The employee, who had been trained on how to handle BCSI, incorrectly believed that only one copy of the printout successfully printed.</p> <p>A manager walking by the printer later that day on April 24, 2018 discovered the second printout and, seeing the BSCI classification in the footer of the document, took the printout and returned it to the other manager responsible for the information.</p> <p>The root cause of this noncompliance was ineffective training as the employee did not fully understand the importance of remaining attentive to printouts that contain sensitive BCSI.</p> <p>This noncompliance involves the management practice of workforce management through ineffective training. The entity determined a need for [REDACTED] training and for increased awareness by users to remain attentive to printouts with sensitive BCSI based off of this incident.</p> <p>This noncompliance started on April 24, 2018, when the employee left the printout containing BCSI on the printer and ended on April 24, 2018, when the manager walked by the printer and picked up the printout and returned it to the other manager responsible for the information.</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 unauthorized personnel to view and access BCSI which could be used to harm the BPS. The risk is minimized because the employee that printed the drawing had authorized access to view the drawing. The manager that discovered the drawing was also authorized to view the drawing. The area where the printer is located has physical security controls that restrict access to only entity approved personnel. Additionally, the major devices identified in the drawing have been decommissioned which diminishes the potential harm that could come from a bad actor viewing the drawing. Lastly, this issue was identified, assessed, and corrected quickly by the manager that discovered the printout. The duration of this noncompliance was less than one day. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) provided [REDACTED] training to personnel; 2) directed that required awareness and attentiveness briefing be given to personnel so that printouts with BCSI would be promptly attended to; and 3) provided individuals handling BCSI with a secure printing guide via email to create awareness around safeguarding printed BCSI materials. <p>ReliabilityFirst 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
RFC2018020066	CIP-011-2	R1	[REDACTED]	[REDACTED]	7/1/2016	10/1/2018	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 July 12, 2018, the entity, [REDACTED], submitted a Self-Report stating that, it was in noncompliance with CIP-011-2 R1. During an upgrade to [REDACTED] in the first quarter of 2018, the entity discovered that, [REDACTED] Bulk Electric System Cyber System Information (BCSI) had been automatically forwarded from [REDACTED] to a work management system, [REDACTED], dedicated to IT. [REDACTED] is not maintained by the entities as a CIP Information Repository (CIR). [REDACTED]</p> <p>The entity uses [REDACTED] for incident management (i.e., ticketing) and problem management by support teams. The entity limits access to [REDACTED] to employees and support contractors whose supervisors have reviewed and approved access to the system based on need. The only protected information in the tickets was the IP address and host name. While these tickets are stored in [REDACTED], they must be specifically identified and recalled with a tailored search to see the protected information.</p> <p>The root cause of this noncompliance was the improper design and integration of [REDACTED]. Specifically, the team configuring [REDACTED] failed to adequately consider the impacts of automatically creating [REDACTED] tickets with protected information. This major contributing factor involves the management practices of information management, which includes managing information item confidentiality and privacy, and integration, in that the failure related to the integration of two systems.</p> <p>This noncompliance started on July 1, 2016, when the entity began using [REDACTED] to automatically send logs to [REDACTED] and ended on October 1, 2018, when the entity deleted from [REDACTED] all of the tickets containing BCSI.</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 retain BCSI in an appropriately protected repository is that it increases the likelihood that an unauthorized person could gain access to the BCSI. This risk was mitigated in this case by the following factors. First, it would have been difficult for an unauthorized person to extract the BCSI at risk in this case because [REDACTED] is only accessible from [REDACTED]. In other words, an individual would first need [REDACTED] through a process that requires review and approval by the individual's manager. Then, even if an individual has [REDACTED] access, the individual would still need a high level of knowledge of the targeted system in order to [REDACTED] that would reach the potential ticket containing BCSI. Second, the BCSI at risk in this case was only IP addresses and host names. So, to make use of this information, an individual would still need the same high level knowledge of the targeted system [REDACTED] and must still defeat [REDACTED] in order to have enough information to effectively use the BCSI. Third, the entity protects its systems from attacks with [REDACTED]. So, if an individual had located the BCSI at risk in this case, the individual would still need [REDACTED]. Finally, if an unauthorized person had obtained access to a device, the entity has [REDACTED] tools that would identify and protect against potential cyber incidents. 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 noncompliances were the result of different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) identified a solution for preventing new tickets associated with CIP protected information from being sent to the [REDACTED]; 2) closed all affected tickets from January 1, 2018 to June 7, 2018 in order to archive the tickets in milestone 3; 3) identified all affected [REDACTED] Tickets from January 1, 2014 to June 7, 2018, and created CSV archives of those tickets; 4) deleted the tickets identified in Milestone 3 from [REDACTED]; and 5) implemented a new ticketing system to replace [REDACTED]. <p>ReliabilityFirst 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
RFC2018020067	CIP-011-2	R1	[REDACTED]	[REDACTED]	7/1/2016	10/1/2018	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 July 12, 2018, the entity, [REDACTED], submitted a Self-Report stating that, it was in noncompliance with CIP-011-2 R1. During an upgrade to [REDACTED] in the first quarter of 2018, the entity discovered that [REDACTED] Bulk Electric system Cyber System Information (BCSI) had been automatically forwarded from [REDACTED] to a work management system, [REDACTED], dedicated to IT. [REDACTED] is not maintained by the entities as a CIP Information Repository (CIR). [REDACTED]</p> <p>The entity uses [REDACTED] for incident management (i.e., ticketing) and problem management by support teams. The entity limits access to [REDACTED] to employees and support contractors whose supervisors have reviewed and approved access to the system based on need. The only protected information in the tickets was the IP address and host name. While these tickets are stored in [REDACTED], they must be specifically identified and recalled with a tailored search to see the protected information.</p> <p>The root cause of this noncompliance was the improper design and integration of [REDACTED]. Specifically, the team configuring [REDACTED] failed to adequately consider the impacts of automatically creating [REDACTED] tickets with protected information. This major contributing factor involves the management practices of information management, which includes managing information item confidentiality and privacy, and integration, in that the failure related to the integration of two systems.</p> <p>This noncompliance started on July 1, 2016, when the entity began using [REDACTED] to automatically send logs to [REDACTED] and ended on October 1, 2018, when the entity deleted from [REDACTED] all of the tickets containing BCSI.</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 retain BCSI in an appropriately protected repository is that it increases the likelihood that an unauthorized person could gain access to the BCSI. This risk was mitigated in this case by the following factors. First, it would have been difficult for an unauthorized person to extract the BCSI at risk in this case because [REDACTED] is only accessible from [REDACTED]. In other words, an individual would first need [REDACTED] through a process that requires review and approval by the individual's manager. Then, even if an individual has [REDACTED] access, the individual would still need a high level of knowledge of the targeted system in order to [REDACTED] that would reach the potential ticket containing BCSI. Second, the BCSI at risk in this case was only IP addresses and host names. So, to make use of this information, an individual would still need the same high level knowledge of the targeted system [REDACTED] and must still defeat [REDACTED] in order to have enough information to effectively use the BCSI. Third, the entity protects its systems from attacks with [REDACTED]. So, if an individual had located the BCSI at risk in this case, the individual would still need [REDACTED]. Finally, if an unauthorized person had obtained access to a device, the entity has [REDACTED] tools that would identify and protect against potential cyber incidents. 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 noncompliances were the result of different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) identified a solution for preventing new tickets associated with CIP protected information from being sent to the [REDACTED]; 2) closed all affected tickets from January 1, 2018 to June 7, 2018 in order to archive the tickets in milestone 3; 3) identified all affected [REDACTED] Tickets from January 1, 2014 to June 7, 2018, and created CSV archives of those tickets; 4) deleted the tickets identified in Milestone 3 from [REDACTED]; and 5) implemented a new ticketing system to replace [REDACTED]. <p>ReliabilityFirst 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
RFC2018020068	CIP-011-2	R1	[REDACTED]	[REDACTED]	7/1/2016	10/1/2018	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 July 12, 2018, the entity, [REDACTED], submitted a Self-Report stating that, it was in noncompliance with CIP-011-2 R1. During an upgrade to [REDACTED] in the first quarter of 2018, the entity discovered that [REDACTED] Bulk Electric system Cyber System Information (BCSI) had been automatically forwarded from [REDACTED] to a work management system, [REDACTED], dedicated to IT. [REDACTED] is not maintained by the entities as a CIP Information Repository (CIR). [REDACTED]</p> <p>The entity uses [REDACTED] for incident management (i.e., ticketing) and problem management by support teams. The entity limits access to [REDACTED] to employees and support contractors whose supervisors have reviewed and approved access to the system based on need. The only protected information in the tickets was the IP address and host name. While these tickets are stored in [REDACTED], they must be specifically identified and recalled with a tailored search to see the protected information.</p> <p>The root cause of this noncompliance was the improper design and integration of [REDACTED]. Specifically, the team configuring [REDACTED] failed to adequately consider the impacts of automatically creating [REDACTED] tickets with protected information. This major contributing factor involves the management practices of information management, which includes managing information item confidentiality and privacy, and integration, in that the failure related to the integration of two systems.</p> <p>This noncompliance started on July 1, 2016, when the entity began using [REDACTED] to automatically send logs to [REDACTED] and ended on October 1, 2018, when the entity deleted from [REDACTED] all of the tickets containing BCSI.</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 retain BCSI in an appropriately protected repository is that it increases the likelihood that an unauthorized person could gain access to the BCSI. This risk was mitigated in this case by the following factors. First, it would have been difficult for an unauthorized person to extract the BCSI at risk in this case because [REDACTED] is only accessible from [REDACTED]. In other words, an individual would first need [REDACTED] through a process that requires review and approval by the individual's manager. Then, even if an individual has [REDACTED] access, the individual would still need a high level of knowledge of the targeted system in order to [REDACTED] that would reach the potential ticket containing BCSI. Second, the BCSI at risk in this case was only IP addresses and host names. So, to make use of this information, an individual would still need the same high level knowledge of the targeted system [REDACTED] and must still defeat [REDACTED] in order to have enough information to effectively use the BCSI. Third, the entity protects its systems from attacks with [REDACTED]. So, if an individual had located the BCSI at risk in this case, the individual would still need [REDACTED]. Finally, if an unauthorized person had obtained access to a device, the entity has [REDACTED] tools that would identify and protect against potential cyber incidents. 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 noncompliances were the result of different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) identified a solution for preventing new tickets associated with CIP protected information from being sent to the [REDACTED]; 2) closed all affected tickets from January 1, 2018 to June 7, 2018 in order to archive the tickets in milestone 3; 3) identified all affected [REDACTED] Tickets from January 1, 2014 to June 7, 2018, and created CSV archives of those tickets; 4) deleted the tickets identified in Milestone 3 from [REDACTED]; and 5) implemented a new ticketing system to replace [REDACTED]. <p>ReliabilityFirst 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
RFC2018020070	CIP-011-2	R1	[REDACTED]	[REDACTED]	7/1/2016	10/1/2018	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 July 12, 2018, the entity, [REDACTED], submitted a Self-Report stating that, it was in noncompliance with CIP-011-2 R1. During an upgrade to [REDACTED] in the first quarter of 2018, the entity discovered that [REDACTED] Bulk Electric system Cyber System Information (BCSI) had been automatically forwarded from [REDACTED] to a work management system, [REDACTED], dedicated to IT. [REDACTED] is not maintained by the entities as a CIP Information Repository (CIR). [REDACTED]</p> <p>The entity uses [REDACTED] for incident management (i.e., ticketing) and problem management by support teams. The entity limits access to [REDACTED] to employees and support contractors whose supervisors have reviewed and approved access to the system based on need. The only protected information in the tickets was the IP address and host name. While these tickets are stored in [REDACTED], they must be specifically identified and recalled with a tailored search to see the protected information.</p> <p>The root cause of this noncompliance was the improper design and integration of [REDACTED]. Specifically, the team configuring [REDACTED] failed to adequately consider the impacts of automatically creating [REDACTED] with protected information. This major contributing factor involves the management practices of information management, which includes managing information item confidentiality and privacy, and integration, in that the failure related to the integration of two systems.</p> <p>This noncompliance started on July 1, 2016, when the entity began using [REDACTED] to automatically send logs to [REDACTED] and ended on October 1, 2018, when the entity deleted from [REDACTED] all of the tickets containing BCSI.</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 retain BCSI in an appropriately protected repository is that it increases the likelihood that an unauthorized person could gain access to the BCSI. This risk was mitigated in this case by the following factors. First, it would have been difficult for an unauthorized person to extract the BCSI at risk in this case because [REDACTED] is only accessible from [REDACTED]. In other words, an individual would first need [REDACTED] through a process that requires review and approval by the individual's manager. Then, even if an individual has [REDACTED] the individual would still need a high level of knowledge of the targeted system in order to [REDACTED] that would reach the potential ticket containing BCSI. Second, the BCSI at risk in this case was only IP addresses and host names. So, to make use of this information, an individual would still need the same high level knowledge of the targeted system [REDACTED] and must still defeat [REDACTED] in order to have enough information to effectively use the BCSI. Third, the entity protects its systems from attacks with [REDACTED]. So, if an individual had located the BCSI at risk in this case, the individual would still need [REDACTED]. Finally, if an unauthorized person had obtained access to a device, the entity has [REDACTED] tools that would identify and protect against potential cyber incidents. 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 noncompliances were the result of different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) identified a solution for preventing new tickets associated with CIP protected information from being sent to the [REDACTED]; 2) closed all affected tickets from January 1, 2018 to June 7, 2018 in order to archive the tickets in milestone 3; 3) identified all affected [REDACTED] Tickets from January 1, 2014 to June 7, 2018, and created CSV archives of those tickets; 4) deleted the tickets identified in Milestone 3 from [REDACTED]; and 5) implemented a new ticketing system to replace [REDACTED]. <p>ReliabilityFirst 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
RFC2018020379	CIP-007-6	R1	[REDACTED]	[REDACTED]	7/3/2017	6/4/2018	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 August 31, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R1. As background, according to the entity's procedures, physical ports that are determined not to be necessary must have [REDACTED]</p> <p>In this case, on two separate occasions, the entity identified a wireless mouse dongle in a port of a BCA without the required permission to use the port. A Supervisory Control and Data Acquisition (SCADA) IT analyst originally plugged the dongle into a USB port on his assigned workstation on July 3, 2017. The workstation was located at the entity's [REDACTED] facility and was used exclusively for testing activities.</p> <p>On January 21, 2018, an IT compliance analyst noted the presence of the wireless mouse dongle during the entity's [REDACTED]. The compliance analyst recalled providing verbal reinforcement to the SCADA IT analyst, but did not document the reinforcement at the time. [REDACTED].</p> <p>Subsequently, on [REDACTED], a member of the team that performs Cyber Vulnerability Assessments (CVAs) identified the same mouse dongle plugged into the USB port of the BCA while he was performing a physical walkdown during the CVA. The CVA team also noted that tamper tape was either removed or had not been properly applied to this particular port in question.</p> <p>The root cause of the noncompliance was the SCADA IT analyst's failure to follow the stated signage and company policy regarding restricted port usage. The SCADA IT analyst claimed to not have been aware of the prohibition. This root cause involves the management practice of workforce management, which includes providing training, awareness, and education to employees.</p> <p>This noncompliance started on July 3, 2017, when the SCADA IT analyst first plugged the mouse dongle into the port, and ended on June 4, 2018, when the entity removed the mouse dongle and reapplied tamper tape to the physical port in question.</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 plugging an unauthorized device into a physical port is that the device could be used to inject malicious software into the asset, or it could be used to exfiltrate information from the asset, or it could be used to gain wireless access to the asset. This risk was minimized in this case based on the following factors. First, the wireless mouse dongle did not have removable storage capabilities. Therefore, it could not have been used to inject malicious software into the asset, and could not have been used to exfiltrate information. Second, [REDACTED]. Third, the asset at issue was being monitored for any adverse actions by its operational system management software tool. 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 root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the mouse dongle and re-applied tamper tape to the USB port of the BCA in question; 2) reviewed group policy reports for the BCA to confirm that no removable media storage capabilities were active; 3) reviewed configuration baseline reports [REDACTED] to confirm no baseline variance was caused because of the mouse being plugged into the USB port; 4) confirmed appropriate signage was present in/around the asset's physical location in accordance with its policy; 5) conducted a stand down meeting with the SCADA IT maintenance team and legal to include detailed review of the specific procedures and policies regarding NERC BCA protection; 6) conducted walkdown of the facility to verify physical port protection controls are still in place since the walkdown that was conducted on [REDACTED]; 7) updated applicable relevant documentation to formalize the tracking and closure of identified issues when performing physical port protection walkdowns; and 8) sent communication, via email, of the relevant documentation that formalizes the updates to the physical port protection walkdown process. <p>ReliabilityFirst 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
RFC2018020510	CIP-007-6	R5	[REDACTED]	[REDACTED]	4/4/2018	7/20/2018	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 4, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5. On April 4, 2018, a field engineer installed and connected [REDACTED] to the entity's Supervisory Control and Data Acquisition (SCADA) network. These assets were installed as part of [REDACTED]. Although powered up with some devices connected and communicating to the SCADA network, the field engineer had not yet set up the password settings on these devices.</p> <p>Subsequently, on [REDACTED], during a Cyber Vulnerability Assessment, a field engineer discovered that these devices still had the default passwords on all access levels while they were performing a monitoring and control function on the SCADA network. [REDACTED]</p> <p>The root cause of this noncompliance was the fact that the field engineer misunderstood when an asset is considered to be "in production." The field engineer assumed that because (a) the settings on the devices were being updated throughout the project as additional devices were connected; (b) the site connection was non-routable; and (c) the devices could only be accessed locally, he could change the passwords on these devices any time before the project was completed.</p> <p>This noncompliance started on April 4, 2018, when the field engineer installed the devices and ended on July 20, 2018, when the entity changed the default passwords on 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 risk posed by failing to change default passwords is that it increases the likelihood that an unauthorized individual could have accessed the devices through known default passwords. This risk was mitigated in this case by the following factors. First, the entity identified and corrected the issue quickly through its internal controls. Second, the entity conducted an extent of condition review and determined that issue was limited to these two devices. Third, this location and these two devices are non-routable, meaning that an individual would require physical access to compromise them. This location was physically protected through [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, while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) confirmed that the default passwords on these devices were changed; 2) conducted a stand down to reinforce installation, testing, and commissioning requirements for BCAs devices; 3) updated its procedure to define when a device transitions from physically installed to installed and connected. The entity also issued a read and sign for the roll-out of this procedure update; and 4) conducted an extent of condition to review of field data and ensure that there are no other [REDACTED] on the system with a default password on any of the access levels or accounts. <p>ReliabilityFirst 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
RFC2018020615	CIP-004-6	R5	[REDACTED]	[REDACTED]	9/1/2018	11/21/2018	Self-Report	March 31, 2020
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 23, 2018 and November 26, 2018, the entity submitted Self-Reports stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5.</p> <p>In the first Self-Report, on August 31, 2018 an employee with unescorted physical access to multiple Physical Security Perimeters (PSPs) transferred to another position within the company and no longer required physical access to the PSPs. The entity's [REDACTED] personnel emailed an individual within [REDACTED] around 8:30 AM on August 31, 2018 to remove this employee's access at the end of the day. The email, however, was sent to an individual instead of the [REDACTED] and access did not get removed before the individual left for the day. The entity did not remove the employee's access until September 4, 2018.</p> <p>The second Self-Report included two separate instances. The first instance occurred on November 1, 2018 when an employee with electronic access and Bulk Electric System (BES) Cyber System Information (BCSI) access separated from the company. The employee turned in his badge and [REDACTED] on November 1, 2018, but the entity did not make an internal notification to remove the employee's electronic access until November 20, 2018. [REDACTED] The employee's electronic access was not timely reviewed because without an [REDACTED], the employee would be unable to access the [REDACTED] network. The entity removed electronic and BCSI access on November 20, 2018 following receipt of the notification.</p> <p>The second instance occurred on November 19, 2018. An employee with unescorted physical access to a PSP transferred to another position within the company that no longer required this type of access. The entity did not remove the employee's access until November 21, 2018.</p> <p>These noncompliances involve the management practices of workforce management, work management, and verification. Workforce management is involved because [REDACTED] personnel and [REDACTED] personnel that process employee change notifications were not effectively trained on their access revocation responsibilities. That ineffective training is a root cause of this noncompliance. Work management is involved because the entity determined its procedures for access revocation were confusing and could use some improvement. Verification is involved because the entity did not have an effective internal control in place to verify that access was timely removed.</p> <p>This noncompliance started on September 1, 2018, when the first employee's access should have been removed and ended on November 21, 2018, when the entity completed removing the last employee'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 based on the following factors. The risk posed by this noncompliance and each of the instances is allowing for unauthorized individuals to access BES Cyber Systems. The risk is minimized because two of the three instances involved trusted entity employees that maintained employment with the company and merely changed positions. Those two instances also had short durations of less than five days each. In the third instance, the entity collected the employee's physical access card and collected the employee's [REDACTED] before the employee left the entity. These actions eliminated the potential for physical access and the employee's potential for cyber access to BCSI and CIP related assets. Without the [REDACTED], the employee at issue could not gain electronic access. The entity's physical access records confirmed that none of the employees accessed the associated PSPs after the effective date of their transfers. 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 compliance history and the instant noncompliances posed minimal risk and the entity quickly identified, assessed, and corrected the instances involved in the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the transferred employee's unescorted physical access to the PSP; 2) removed the separated employee's electronic access and BSCI access; 3) removed the transferred employee's unescorted physical access to the PSP; 4) updated the associated procedure to include the correct method of communicating revocations to [REDACTED]; 5) provided notification to all [REDACTED] personnel of the change in the procedure; 6) updated and implemented the [REDACTED] procedure to date base badges to the effective date of transfer upon receipt of notification of transfer; 7) updated [REDACTED] to enhance the off-boarding process in [REDACTED] to provide multiple points of contact when an individual leaves the company; 8) provided ReliabilityFirst with a status update on the mitigation plan progress; 9) included [REDACTED] on a team to run access revocation procedures through the [REDACTED] process to find gaps and create efficiencies; 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020615	CIP-004-6	R5	[REDACTED]	[REDACTED]	9/1/2018	11/21/2018	Self-Report	March 31, 2020
			<p>To mitigate this noncompliance, the entity will complete the following mitigation activities by March 31, 2020:</p> <ol style="list-style-type: none"> 1) will provide the preliminary review results to the stake holders and collect feedback; 2) will create or update documentation for new or revised processes; and 3) will train [REDACTED] personnel on the revised access revocation process. <p>Additional time is needed to complete this ongoing mitigation because of training timing with planned vacations.</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
RFC2018020511	CIP-004-6	R4	[REDACTED]	[REDACTED]	4/16/2018	8/20/2018	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 4, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4. This noncompliance involves two separate instances which arose from the same underlying factual circumstances.</p> <p>First, on April 16, 2018, an unauthorized employee was provisioned access to Bulk Electric System (BES) Cyber System Information (BCSI) in [REDACTED]. The employee did not have requisite qualifications but obtained, in part, two access roles that gave the employee access to data [REDACTED].</p> <p>Second, on June 1, 2018, a separate unauthorized employee was provisioned access to BCSI in [REDACTED]. The employee, although qualified (i.e., completed personnel risk assessment and training), was not authorized for a provisioned role that gave the employee access to data [REDACTED].</p> <p>Both issues were discovered on August 20, 2018, after a manager received a [REDACTED] request from one of his employees for two roles in [REDACTED] that included access to BCSI. [REDACTED]. The [REDACTED] request was initiated from within [REDACTED] by the employee. The manager contacted another employee who supports [REDACTED] and they determined that the [REDACTED] request was not the proper method for requesting access to BCSI and rejected the request. The proper method for requesting access to BCSI (and NERC-classified assets and systems) was to use the entity's access management system, [REDACTED]. In this specific example, a request should have been initiated in [REDACTED]. If the requested access was ultimately approved, then [REDACTED]. The [REDACTED] created the ability to bypass [REDACTED] the entity's access management process for NERC-classified assets, systems, and information. The entity conducted an extent of condition review to determine whether, through the use of past [REDACTED] requests, access to BCSI in [REDACTED] may have been provisioned to unauthorized employees. During this review, the entity discovered the two instances at issue here.</p> <p>In both instances, the employees submitted a [REDACTED] request from within [REDACTED] because [REDACTED]. However, when the [REDACTED] requests were granted, the employees were also provisioned [REDACTED], thereby bypassing the entity's [REDACTED] access management process for NERC-classified assets, systems, and information, which included safeguards to ensure that only authorized personnel were provisioned specific NERC access roles.</p> <p>The root causes of this noncompliance were (a) the ability to request and provision access to BCSI through [REDACTED] and (b) the lack of awareness of the scope and functionality of [REDACTED]. This noncompliance implicates the management practice of workforce management, which includes the need to effectively manage employee permissions and access to assets and information.</p> <p>The first instance started on April 16, 2018, when the entity did not follow its process to authorize access to BCSI and ended on August 20, 2018, when the entity revoked the improperly provisioned access. The second instance started on June 1, 2018, when the entity did not follow its process to authorize access to BCSI and ended on August 20, 2018, when the entity revoked the improperly provisioned 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. Unauthorized access to BCSI could lead to alteration or misuse of the information. The risk was mitigated by the following facts. While neither of the employees were authorized, one had a valid personnel risk assessment and completed requisite training. In addition, both were trusted employees of the entity, and neither of them knew that they had been provisioned access to BCSI, as both intended [REDACTED]. Thus, the risk of alteration or misuse of the BCSI was reduced. It is also worth noting that the employees only had access to specific data in [REDACTED]; they did not have access to actual assets. The [REDACTED] does not have any monitoring or control functions for any BES Cyber Assets. 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 violations involved different factual circumstances, issues, and/or causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) immediately revoked the access roles that were improperly provisioned via [REDACTED] requests once the noncompliance was discovered; 2) sent a communication to all supervisors to reject any further [REDACTED] requests generated from [REDACTED] that included NERC access roles until a permanent fix was implemented; 3) verified that no changes were performed on any date by the two entity employees while they had unauthorized access; 4) wrote an auto-script that strips out all NERC access roles when using [REDACTED]; and 5) blocked from view any NERC access roles when employees request new access using the standard search method. <p>ReliabilityFirst 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
RFC2017018768	CIP-007-6	R3	[REDACTED]	[REDACTED]	6/8/2017	5/2/2018	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 December 1, 2017, the entity, as a [REDACTED], submitted a Self-Report stating that it was in noncompliance with CIP-007-6 R3.</p> <p>As background, [REDACTED]</p> <p>During the week of June 8, 2017, [REDACTED]. On July 24, 2017, as part of ongoing periodic review of anti-virus (AV) signatures, the entity identified that five test devices in the entity test network were not receiving AV signatures beginning on June 8, 2017, as a result of this firewall rule change. [REDACTED] devices. The affected test devices included: [REDACTED].</p> <p>In addition to this issue with the test devices, the firewall rule change also had an effect on the associated production assets. Although production assets continued to receive [REDACTED] updates during this timeframe, these signatures were not tested in accordance with CIP-007-6 R3.3.</p> <p>The root cause of this noncompliance was the firewall rule configuration change that disrupted communication between the two sites that include protective anti-malware servers. Additionally, the change process applicable to this firewall rule change did not cover potential downstream impacts of this nature. These major contributing factors involve the management practices of asset and configuration management, which includes establishing an assets and configuration items inventory, and integration, which includes establishing a list of subsystems that require exchange of information.</p> <p>This noncompliance started on June 8, 2017, when the entity made the firewall rule change that disrupted communication and ended on May 2, 2018, when the entity completed its extent of condition review.</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. This noncompliance involves the following two potential risks. The potential risk associated with failing to provide devices with updated AV signatures is that the devices' AV software would not be able to identify the malicious code associated with those signatures. This risk was mitigated in this case because the only devices that were not receiving updated AV signatures were test devices that had no impact on the BPS. The [REDACTED] associated with these test devices were receiving updated AV signatures. However, these AV signatures were not being tested prior to deployment to the production assets, which presents the second potential risk. The potential risk associated with deploying untested AV signatures is that they could cause unexpected protective anti-malware software latency issues or possible loss of the device. This risk was mitigated in this case by the following factors. First, had the untested AV signatures caused any issue, the entity uses a defense-in-depth strategy to prevent or reduce adverse impact. For example, [REDACTED]. In addition, the entity protected these devices with [REDACTED]. Second, although these AV signatures were not tested for these particular production assets, they were [REDACTED] prior to being installed. No anomalies were detected with those AV signatures. This result reduces the likelihood that the untested deployment of these AV signatures on these [REDACTED] would have caused an unexpected issue. 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 they were all the result of different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) [REDACTED]; 2) updated the 5 test network devices with the appropriate AV signatures; 3) performed an evaluation to determine if all relevant test and production Windows devices are receiving the appropriate AV signatures; 4) reviewed results of evaluation of AV signature deployments with leadership; 5) updated an existing process for the [REDACTED] reports and created a Job Aid to assist personnel on accessing the reports, evaluating the information and determining if there are any discrepancies; 6) conducted a reinforcement session with the appropriate personnel with specific roles within relevant groups to reinforce the importance of ensuring that AV signatures are deployed in accordance with processes on the test and production networks NERC CIP in-scope windows cyber assets; 7) updated AV signatures on additional production network devices discovered during evaluation, if necessary or confirm that no updates were required. (No additional instances were identified.); 8) reviewed the process document and updated the document with the red-lined changes or confirmed that no updates were required; 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018768	CIP-007-6	R3	[REDACTED]	[REDACTED]	6/8/2017	5/2/2018	Self-Report	Completed
			<p>9) approved the process document with the red-lined changes or confirm that no updates were required;</p> <p>10) updated the associated Job Aids to require that change requests for [REDACTED] be reviewed by the entity [REDACTED] prior to implementation;</p> <p>11) distributed the updated Job Aid to the [REDACTED]; and</p> <p>12) updated the [REDACTED] and [REDACTED] to include the [REDACTED] compliance group.</p> <p>ReliabilityFirst 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
RFC2017018769	CIP-007-6	R3	[REDACTED]	[REDACTED]	6/8/2017	5/2/2018	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 December 1, 2017, the entity, as a [REDACTED], submitted a Self-Report stating that it was in noncompliance with CIP-007-6 R3.</p> <p>As background, [REDACTED]</p> <p>During the week of June 8, 2017, [REDACTED]. On July 24, 2017, as part of ongoing periodic review of anti-virus (AV) signatures, the entity identified that five test devices in the entity test network were not receiving AV signatures beginning on June 8, 2017, as a result of this firewall rule change. [REDACTED] devices. The affected test devices included: [REDACTED].</p> <p>In addition to this issue with the test devices, the firewall rule change also had an effect on the associated production assets. Although production assets continued to receive [REDACTED] updates during this timeframe, these signatures were not tested in accordance with CIP-007-6 R3.3.</p> <p>The root cause of this noncompliance was the firewall rule configuration change that disrupted communication between the two sites that include protective anti-malware servers. Additionally, the change process applicable to this firewall rule change did not cover potential downstream impacts of this nature. These major contributing factors involve the management practices of asset and configuration management, which includes establishing assets and configuration items inventory, and integration, which includes establishing a list of subsystems that require exchange of information.</p> <p>This noncompliance started on June 8, 2017, when the entity made the firewall rule change that disrupted communication and ended on May 2, 2018, when the entity completed its extent of condition review.</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. This noncompliance involves the following two potential risks. The potential risk associated with failing to provide devices with updated AV signatures is that the devices' AV software would not be able to identify the malicious code associated with those signatures. This risk was mitigated in this case because the only devices that were not receiving updated AV signatures were test devices that had no impact on the BPS. The [REDACTED] associated with these test devices were receiving updated AV signatures. However, these AV signatures were not being tested prior to deployment to the production assets, which presents the second potential risk. The potential risk associated with deploying untested AV signatures is that they could cause unexpected protective anti-malware software latency issues or possible loss of the device. This risk was mitigated in this case by the following factors. First, had the untested AV signatures caused any issue, the entity uses a defense-in-depth strategy to prevent or reduce adverse impact. For example, [REDACTED]. In addition, [REDACTED]. Second, although these AV signatures were not tested for these particular production assets, they were [REDACTED] prior to being installed. No anomalies were detected with those AV signatures. This result reduces the likelihood that the untested deployment of these AV signatures on these [REDACTED] would have caused an unexpected issue. 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 they were all the result of different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) [REDACTED]; 2) updated the 5 test network devices with the appropriate AV signatures; 3) performed an evaluation to determine if all relevant test and production Windows devices are receiving the appropriate AV signatures; 4) reviewed results of evaluation of AV signature deployments with leadership; 5) updated an existing process for the [REDACTED] reports and created a Job Aid to assist personnel on accessing the reports, evaluating the information and determining if there are any discrepancies; 6) conducted a reinforcement session with the appropriate personnel with specific roles within relevant groups to reinforce the importance of ensuring that AV signatures are deployed in accordance with processes on the test and production networks NERC CIP in-scope windows cyber assets; 7) updated AV signatures on additional production network devices discovered during evaluation, if necessary or confirm that no updates were required. (No additional instances were identified.); 8) reviewed the process document and updated the document with the red-lined changes or confirmed that no updates were required; 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018769	CIP-007-6	R3	[REDACTED]	[REDACTED]	6/8/2017	5/2/2018	Self-Report	Completed
			9) approved the process document with the red-lined changes or confirm that no updates were required; 10) updated the associated Job Aids to require that change requests for [REDACTED] the network to be reviewed by the entity [REDACTED] prior to implementation; 11) distributed the updated Job Aid to the [REDACTED] and [REDACTED] 12) updated the [REDACTED] and [REDACTED] to include the [REDACTED] compliance group. ReliabilityFirst has verified the completion of all mitigation activity.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018771	CIP-007-6	R3	[REDACTED]	[REDACTED]	6/8/2017	5/2/2018	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 December 1, 2017, the entity, as a [REDACTED], submitted a Self-Report stating that it was in noncompliance with CIP-007-6 R3.</p> <p>As background, [REDACTED]</p> <p>During the week of June 8, 2017, [REDACTED]. On July 24, 2017, as part of ongoing periodic review of anti-virus (AV) signatures, the entity identified that five test devices in the entity test network were not receiving AV signatures beginning on June 8, 2017, as a result of this firewall rule change. [REDACTED] devices. The affected test devices included: [REDACTED].</p> <p>In addition to this issue with the test devices, the firewall rule change also had an effect on the associated production assets. Although production assets continued to receive [REDACTED] updates during this timeframe, these signatures were not tested in accordance with CIP-007-6 R3.3.</p> <p>The root cause of this noncompliance was the firewall rule configuration change that disrupted communication between the two sites that include protective anti-malware servers. Additionally, the change process applicable to this firewall rule change did not cover potential downstream impacts of this nature. These major contributing factors involve the management practices of asset and configuration management, which includes establishing assets and configuration items inventory, and integration, which includes establishing a list of subsystems that require exchange of information.</p> <p>This noncompliance started on June 8, 2017, when the entity made the firewall rule change that disrupted communication and ended on May 2, 2018, when the entity completed its extent of condition review.</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. This noncompliance involves the following two potential risks. The potential risk associated with failing to provide devices with updated AV signatures is that the devices' AV software would not be able to identify the malicious code associated with those signatures. This risk was mitigated in this case because the only devices that were not receiving updated AV signatures were test devices that had no impact on the BPS. The [REDACTED] associated with these test devices were receiving updated AV signatures. However, these AV signatures were not being tested prior to deployment to the production assets, which presents the second potential risk. The potential risk associated with deploying untested AV signatures is that they could cause unexpected protective anti-malware software latency issues or possible loss of the device. This risk was mitigated in this case by the following factors. First, had the untested AV signatures caused any issue, the entity uses a defense-in-depth strategy to prevent or reduce adverse impact. For example, [REDACTED]. In addition, [REDACTED]. Second, although these AV signatures were not tested for these particular production assets, they were [REDACTED] prior to being installed. No anomalies were detected with those AV signatures. This result reduces the likelihood that the untested deployment of these AV signatures on these [REDACTED] would have caused an unexpected issue. 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 they were all the result of different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) [REDACTED]; 2) updated the 5 test network devices with the appropriate AV signatures; 3) performed an evaluation to determine if all relevant test and production Windows devices are receiving the appropriate AV signatures; 4) reviewed results of evaluation of AV signature deployments with leadership; 5) updated an existing process for the [REDACTED] reports and created a Job Aid to assist personnel on accessing the reports, evaluating the information and determining if there are any discrepancies; 6) conducted a reinforcement session with the appropriate personnel with specific roles within relevant groups to reinforce the importance of ensuring that AV signatures are deployed in accordance with processes on the test and production networks NERC CIP in-scope windows cyber assets; 7) updated AV signatures on additional production network devices discovered during evaluation, if necessary or confirm that no updates were required. (No additional instances were identified.); 8) reviewed the process document and updated the document with the red-lined changes or confirmed that no updates were required; 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018771	CIP-007-6	R3	[REDACTED]	[REDACTED]	6/8/2017	5/2/2018	Self-Report	Completed
			<p>9) approved the process document with the red-lined changes or confirm that no updates were required;</p> <p>10) updated the associated Job Aids to require that change requests for [REDACTED] be reviewed by the entity [REDACTED] prior to implementation;</p> <p>11) distributed the updated Job Aid to the [REDACTED]; and</p> <p>12) updated the [REDACTED] and [REDACTED] to include the [REDACTED] compliance group.</p> <p>ReliabilityFirst 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
RFC2017018773	CIP-007-6	R3	[REDACTED]	[REDACTED]	6/8/2017	5/2/2018	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 December 1, 2017, the entity, as a [REDACTED], submitted a Self-Report stating that it was in noncompliance with CIP-007-6 R3.</p> <p>As background, [REDACTED]</p> <p>During the week of June 8, 2017, [REDACTED]. On July 24, 2017, as part of ongoing periodic review of anti-virus (AV) signatures, the entity identified that five test devices in the entity test network were not receiving AV signatures beginning on June 8, 2017, as a result of this firewall rule change. [REDACTED] devices. The affected test devices included: [REDACTED].</p> <p>In addition to this issue with the test devices, the firewall rule change also had an effect on the associated production assets. Although production assets continued to receive [REDACTED] updates during this timeframe, these signatures were not tested in accordance with CIP-007-6 R3.3.</p> <p>The root cause of this noncompliance was the firewall rule configuration change that disrupted communication between the two sites that include protective anti-malware servers. Additionally, the change process applicable to this firewall rule change did not cover potential downstream impacts of this nature. These major contributing factors involve the management practices of asset and configuration management, which includes establishing assets and configuration items inventory, and integration, which includes establishing a list of subsystems that require exchange of information.</p> <p>This noncompliance started on June 8, 2017, when the entity made the firewall rule change that disrupted communication and ended on May 2, 2018, when the entity completed its extent of condition review.</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. This noncompliance involves the following two potential risks. The potential risk associated with failing to provide devices with updated AV signatures is that the devices' AV software would not be able to identify the malicious code associated with those signatures. This risk was mitigated in this case because the only devices that were not receiving updated AV signatures were test devices that had no impact on the BPS. The [REDACTED] associated with these test devices were receiving updated AV signatures. However, these AV signatures were not being tested prior to deployment to the production assets, which presents the second potential risk. The potential risk associated with deploying untested AV signatures is that they could cause unexpected protective anti-malware software latency issues or possible loss of the device. This risk was mitigated in this case by the following factors. First, had the untested AV signatures caused any issue, the entity uses a defense-in-depth strategy to prevent or reduce adverse impact. For example, [REDACTED]. In addition, [REDACTED]. Second, although these AV signatures were not tested for these particular production assets, they were [REDACTED] prior to being installed. No anomalies were detected with those AV signatures. This result reduces the likelihood that the untested deployment of these AV signatures on these [REDACTED] would have caused an unexpected issue. 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 they were all the result of different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) [REDACTED]; 2) updated the 5 test network devices with the appropriate AV signatures; 3) performed an evaluation to determine if all relevant test and production Windows devices are receiving the appropriate AV signatures; 4) reviewed results of evaluation of AV signature deployments with leadership; 5) updated an existing process for the [REDACTED] reports and created a Job Aid to assist personnel on accessing the reports, evaluating the information and determining if there are any discrepancies; 6) conducted a reinforcement session with the appropriate personnel with specific roles within relevant groups to reinforce the importance of ensuring that AV signatures are deployed in accordance with processes on the test and production networks NERC CIP in-scope windows cyber assets; 7) updated AV signatures on additional production network devices discovered during evaluation, if necessary or confirm that no updates were required. (No additional instances were identified.); 8) reviewed the process document and updated the document with the red-lined changes or confirmed that no updates were required; 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018773	CIP-007-6	R3	[REDACTED]	[REDACTED]	6/8/2017	5/2/2018	Self-Report	Completed
			9) approved the process document with the red-lined changes or confirm that no updates were required; 10) updated the associated Job Aids to require that change requests for [REDACTED] be reviewed by the entity [REDACTED] prior to implementation; 11) distributed the updated Job Aid to the [REDACTED]; and 12) updated the [REDACTED] and [REDACTED] to include the [REDACTED] compliance group. ReliabilityFirst has verified the completion of all mitigation activity.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020642	CIP-011-2	R1	[REDACTED]	[REDACTED]	8/16/2018	11/5/2018	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 26, 2018, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-011-2 R1. On August 22, 2018, the entity conducted a check for CIP Protected Bulk Electric System (BES) Cyber System Information (BCSI) on its intranet. One of these searches provided a link to a single document in a CIP repository that contained BCSI [REDACTED] pertaining to [REDACTED] BES Cyber Assets. The employee conducting the search had valid CIP training and a current Personnel Risk Assessment (PRA), but did not have a business need to actually access the BCSI. Upon accessing the BCSI, the employee escalated the issue to the appropriate manager the same day.</p> <p>The entity performed an extent of condition review on all active CIP repositories to determine whether any users who had access were not properly authorized. As a result of this review, the entity determined that four users were not properly authorized because, although they had valid PRAs, current CIP training, and a business need to access the information, they lacked an authorized role in the entity's access management database. [REDACTED]</p> <p>The root cause of this noncompliance was two-fold. First, with respect to the original instance, the root cause was a mistake an IT services technician made while attempting to make changes to automated email reports sent from [REDACTED] to the CIP repository. After completing troubleshooting to accomplish this task, the technician mistakenly [REDACTED]. This oversight allowed users to access the document at issue. Second, with respect to the additional issues the entity identified during the extent of condition review, the root cause was insufficient detail in the processes for managing access to the CIP repository.</p> <p>This root cause involves the management practices of workforce management because the IT technician performing the troubleshooting did not have sufficient familiarity with the system to perform this task correctly, and reliability quality management, which includes maintaining a system for deploying internal controls.</p> <p>This noncompliance started on August 16, 2018, when the IT technician made the changes to the permissions and ended on November 5, 2018, when the entity removed the 4 users with unauthorized access to the CIP repository.</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 not properly restricting access to BCSI is that an unauthorized person could obtain the BCSI. This risk was mitigated in this case by the following factors. First, the BCSI at issue in this case included [REDACTED] but did not contain any password information that would be needed to gain access to these devices. Second, even if access had been obtained, the entity has monitoring and alerting tools in place that would identify and protect against potential cyber incidents. Third, only four people had access to the information that were not authorized to have that access. Furthermore, those four people had current CIP training and valid PRAs. ReliabilityFirst also notes that the entity did not observe any incidents related to the devices noted within the document since the time that the document was available for retrieval. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) changed permissions to correctly restrict access to member of the entity IT [REDACTED] Team; 2) conducted a review of all active entity CIP repository sites and corrected all entity associated permissions to match the approved authorization [REDACTED]; 3) created/updated the Job Aid containing detailed technical information and best practices on the configuration, maintenance and changes to a CIP repository; 4) communicated the Job Aid; 5) updated a process document to provide clarification and context on CIP repository; and 6) updated the current training to include CIP repository permission information. The entity also distributed the updated document to all users [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
SERC2017016826	CIP-004-6	R4.1, P4.1.1	[REDACTED]	[REDACTED]	12/04/2016	01/12/2017	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 January 23, 2017, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-004-6 R4, P4.1.1. The Entity granted two employees electronic access to Bulk Electric System (BES) Cyber Systems (BCSs) without documenting authorization of such access.</p> <p>On January 6, 2017, while conducting a monthly quality review of active electronic access, a [REDACTED] discovered that the authorization of electronic access to BCSs granted to two individuals had not been documented. Specifically, on December 4, 2016, the Entity provisioned two employees with electronic access without generating an access tracking ticket to serve as a record of access authorization as required in its documented access management procedure. Although the change tickets for provisioning electronic access to the two individuals were entered into the access tracking system, personnel responsible for provisioning access to the two employees prematurely provisioned access without waiting for management approval. Because the two employees needed electronic access, on January 12, 2017, the Entity's [REDACTED] generated the missing access tickets and documented the required access authorization.</p> <p>This noncompliance started on December 4, 2016, when the Entity provisioned two employees electronic access to BCSs without documenting authorization of such access, and ended on January 12, 2017, when the Entity documented the access authorization.</p> <p>The root cause of this non-compliance was lack of training. Personnel responsible for provisioning access should not have granted access prior to management approval of the access change tickets that had been entered into the access tracking system.</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 correctly implementing the documented process for provisioning electronic access, the possibility increased for erroneously granting electronic access to unauthorized individuals. In those situations, malicious actors could potentially gain operational control of cyber assets and bulk power system facilities and caused misoperations or grid disturbances. Notwithstanding, these two instances were documentation deficiencies. Both employees needed electronic access to perform their duties, were current on cyber security training, and had a current personnel risk assessment on file. Additionally, [REDACTED] personnel monitored the shared token these two employees utilized for access at all times. Moreover, the Entity placed accessible assets within Electronic Security Perimeters and protected them with configuration change monitoring and alerting. 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) reviewed the employees' PRA and CIP training to validate they were completed prior to them gain electronic access to BCSs; 2) confirmed with the employees' supervisors of their need for access along with the date that they began to use the shared token to gain access; 3) created [REDACTED] tickets to document the need for access; 4) added the employees to the access list; 5) revised its access management procedure to include additional steps to notify [REDACTED] of [REDACTED] and [REDACTED] requiring cyber access; 6) researched alternative methods of authentication to determine an optimal solution for the [REDACTED] and [REDACTED]; 7) developed a plan for implementation of the recommended method of authentication; 8) implemented the recommended method of authentication; and 9) trained affected personnel of the revised procedure. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018018918	CIP-010-2	R1: P1.1	[REDACTED]	[REDACTED]	07/01/2016	11/29/2017	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 29, 2017, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED], [REDACTED], and [REDACTED], it was in noncompliance with CIP-010-2 R1, P1.1. The Entity did not update its baseline configuration to reflect two open ports after installing two intermediate devices.</p> <p>On July 1, 2016, the Entity reconfigured two intermediate devices used for interactive remote access to ensure redundancy while patching and maintenance. However, the Entity did not update the port list on the baselines to reflect two open ports associated with the intermediate devices. On October 3, 2017, during an Entity Cyber Vulnerability Assessment (CVA), an Entity administrator discovered the open ports that were not included on the baselines.</p> <p>On October 16, 2017, the Entity updated its baseline for both intermediate devices to include the ports in question.</p> <p>On April 12, 2018, the Entity submitted an additional Self-Report related to CIP-010-2 R1, P1.1 [REDACTED], which was dismissed and consolidated into the instant noncompliance. Although the Entity submitted this Self-Report under CIP-010-2 R1, P1.4, SERC determined that the appropriate standard and requirement is CIP-010-2 R1, P1.1.</p> <p>On July, 25, 2017, the Entity installed [REDACTED] new Electronic Access Control or Monitoring System (EACMS) servers associated with its [REDACTED] Medium Impact Bulk Electric System (BES) Cyber Systems in its [REDACTED] with an incomplete listing of its ports. The Entity had [REDACTED] open ports that were required, but the Entity did not list them on its ports and services documentation. The Entity created its ports and services documentation from the vendor supplied ports and services list prior to placing the servers onto the network in the [REDACTED]. However, the Entity did not validate that those were the only ports needed and opened when it installed the servers onto the production network in the [REDACTED].</p> <p>In addition, On July, 25, 2017, during the change management process, the Entity created [REDACTED] temporary internal accounts used during installation of the new EACMS servers but forgot to take the accounts off after installation, and they were not on the list of accounts on the access control list.</p> <p>On October 11, 2017, the Entity discovered these last two instances of noncompliance through its required, annual Cyber Vulnerability Assessment. On November 29, 2017, the Entity updated the EACMS baselines to match the ports that were open and needed. At this time, the Entity also deleted the temporary accounts that it deemed unnecessary on the EACMS.</p> <p>This noncompliance started on July 1, 2016, when, in the first instance, the Entity reconfigured two intermediate devices that opened up the port that was not reflected in its baselines, and ended on November 29, 2017, when the Entity updated its baselines with the [REDACTED] additional open ports and deleted its [REDACTED] temporary accounts.</p> <p>The root cause for all three instances of noncompliance was inadequate training on the baseline and account Change Management process.</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 Entity's failure to update the port list on the baselines could have afforded an opportunity for potential malicious actors to access and modify or compromise the operation of BES Cyber Systems because the Cyber Asset would have a vulnerable port open to their intermediate servers that the Entity was not sufficiently protecting or tracking. Also, enabling temporary internal accounts for testing and not removing them afterwards, could provide a means for a malicious actor to gain access through a temporary account which the Entity did not track. However, there is a second connection required to access the Electronic Security Perimeter and BES Cyber Systems from the intermediate servers that requires a valid username and 2-factor authentication (VPN). The Entity would log any unsuccessful attempts and alert the Entity administrator to the unsuccessful attempts. In addition, with regard to the EACMSs ports and temporary accounts, in the second and third instances, the unlisted ports were needed by the system software to operate, but were left off of the baselines because of incomplete vendor documentation. Also, the temporary accounts that the Entity did not remove, had no rights and the Entity did not configure the temporary accounts to be able to obtain or grant access. Furthermore, the servers were located in a [REDACTED]. The Entity authorized only those administrators and key users for this remote access. Also, the server was located inside a Physical Security Perimeter, which is restricted to authorized personnel who are current on NERC CIP training and an up-to-date personnel risk assessment on file. 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>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the baseline documentation for the [REDACTED] intermediate devices to include needed ports; 2) provided one-on-one training with the system administrator on the Entity Procedure; 3) modified the change management and documentation review process to include another layer of review; and 4) trained all system administrators on the modification to 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
SERC2016016518	CIP-010-2	R1, P1.1	[REDACTED]	[REDACTED]	07/01/2016	06/01/2017	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 November 16, 2016, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1, P1.1. The Entity reported [REDACTED] instances where it did not properly update baseline configuration documentation.</p> <p>In the first instance, on September 28, 2016, during a risk-based scheduled internal audit of CIP requirements, on March 15, 2016, an engineer updated the Entity's baseline configuration record with an incorrect relay firmware version indicated in a [REDACTED] [REDACTED] which the field personnel incorrectly recorded.</p> <p>In the second instance, on March 24, 2016, although the [REDACTED] relay firmware version recording was correct for a relay, an engineer mistyped the firmware version when updating the baseline configuration record.</p> <p>To assess the extent-of-condition, on June 8, 2017, the Entity conducted the 2017 Cyber Vulnerability Assessment, and reviewed applied firmware for other Cyber Assets and discovered [REDACTED] additional instances where incorrect firmware versions were recorded on the baseline configuration record. On June 16, 2017, the Entity submitted additional findings as scope expansions to the Self-Report.</p> <p>For all these instances, the incorrect firmware version was recorded in the baseline configuration record, including: (i) [REDACTED] programmable logic controller used to periodically perform testing on power line carrier radios; (ii) [REDACTED] protective relays; and (iii) [REDACTED] remote terminal unit (RTU).</p> <p>The noncompliance affected [REDACTED] medium impact facilities containing a total of [REDACTED] impacted BES Cyber Assets.</p> <p>This noncompliance started on July 1, 2016, when the standard became mandatory and enforceable, and ended on June 1, 2017, when the Entity updated its baseline configuration documentation.</p> <p>The root causes of the noncompliance were insufficient preventative controls, specifically, a secondary reviewer of baseline configuration documentation, and training during CIP Version 5 implementation.</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 Entity not reflecting correct versions of firmware in documented baseline configurations potentially could have prevented new security patches from being implemented, which could have afforded a security-related opportunity for a malicious hacker to change relay configurations and compromise grid security. However, none of the affected Cyber Assets were remotely accessible and none had External Routable Connectivity. All Cyber Assets are inside a Physical Security Perimeter, which requires proper credentials to access. Additionally, for the relays, which were used as secondary (transformer) protection, the Entity had changed the default passwords. Moreover, for the RTU, the firmware was related to non-security updates. 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) recorded the correct firmware versions on the [REDACTED]; 2) revised its CIP [REDACTED] process to prohibit manual and copying and pasting of data into the [REDACTED] and require a second engineer to validate screenshot evidence before sign-off of storage of baseline configuration documentation; and 3) trained all affected personnel in the [REDACTED] Department on the new [REDACTED] 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
SERC2017016992	CIP-007-6	R5, P5.6	[REDACTED]	[REDACTED]	09/01/2016	11/02/2016	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 violation.)			<p>On February 13, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED], it was in noncompliance with CIP-007-6 R5, P5.6. The Entity failed to timely change passwords on [REDACTED] Electronic Access Control or Monitoring System (EACMS) Cyber Assets (servers).</p> <p>The Entity discovered this noncompliance during a November 2, 2016 vulnerability assessment required by CIP-010-2 R1, P3.1. The default administration account on the [REDACTED] EACM servers could not be disabled due to technical feasibility reasons. Thus, the Entity default passwords on the [REDACTED] servers were changed, but weren't not changed since May 5, 2015. The Entity's CIP task-scheduling tool generated the alert to change the password on May 5, 2016, but the employee who was the account owner failed to complete the change. The [REDACTED] servers perform authentication, accounting, and authorization services to network devices and are associated with high impact Bulk Electric System Cyber Systems. [REDACTED] server is located at the primary control center and the other at the backup control center.</p> <p>The extent-of-condition effort, which was the vulnerability assessment that led to this discovery, did not identify additional instances of non-compliance with CIP-007-6 R5, P5.6.</p> <p>This noncompliance started on August 6, 2016, when the Entity was required to have changed the passwords on the [REDACTED] ECMS servers, and ended on November 2, 2016, when the passwords were changed.</p> <p>The root cause of this noncompliance was inadequate preventative controls to ensure adherence to the password procedures. The task owner prematurely signed off on the task as completed but forgot to complete the task. The Entity now requires the task owner to submit evidence to demonstrate the task was completed prior to marking the task as complete, and a secondary approver has been added to review the evidence prior to signing the task is 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. The Entity's failure to change account passwords could have permitted individuals with malicious intent a longer period to guess or hack the existing passwords and gain unauthorized access to the EACM servers. [REDACTED]</p> <p>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 prior noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) modified the scheduled task description to require the individual assigned a compliance task to attach a screen shot of the accounts on the Cyber Assets with the account password change shown; and 2) modified the scheduled task description to require the task approver to review and approve attached evidence prior to signing the task as complete. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019715	CIP-006-6	R2, P2.2	[REDACTED]	[REDACTED]	11/1/2017	1/30/2018	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 April 16, 2018 through April 19, 2018, SERC determined that the Entity, as a [REDACTED] and [REDACTED], was in noncompliance with CIP-006-6 R2, P2.2. The Entity failed to maintain complete visitor logs for visitors entering Physical Security Perimeters (PSPs).</p> <p>On December 10, 2017, an Entity employee who had authorized access, escorted a visiting contractor who only signed his first name in the PSP logbook. Additionally, on January 30, 2018, an Entity employee who had authorized access, escorted a visiting vendor into the PSP. The escort did not sign the visitor out after the visitor left the PSP.</p> <p>During an extent-of-condition, the Entity discovered that the cleaning crew only signed their first name on numerous occasions during the months of November 2017 and December 2017. Also, the Entity discovered no other instances where the escort did not log out the visitor. The Entity discovered no other missing visitor information in the PSP logs in either the Primary Control Center or the Backup Control Center.</p> <p>This noncompliance started on November 1, 2017, the earliest instance when the escort did not properly fill out the name of the visiting contractor, and ended on January 30, 2018, the latest instance when the escort failed to fill out the exit time of the visiting vendor.</p> <p>The root cause of this noncompliance was inadequate training. The Entity escorts did not properly explain the requirements to the visitors and the escorts did not verify completion or correctness of the log information.</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's failure to capture required information for its visitors into its PSPs could have hindered any future investigations had an incident occurred. However, authorized control room employees continuously escorted the visitors at all times during their visit. In addition, the Entity staffs the Control Center 24/7, and the PSP door is within eyesight of the system operators and the shift supervisor.</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) implemented electronic logging that prohibits sign-in if required fields are not properly completed; 2) updated Access Control Policy to reflect electronic logging; and 3.) trained Control Center Staff (who could be potential visitor escorts) on the updated Access Control Policy. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017018450	CIP-011-2	R1; Part 1.2	[REDACTED] (the "Entity")	[REDACTED]	07/20/2017	08/11/2017	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 violation.)			<p>On [REDACTED], the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-011-2 R1. Specifically, the Entity failed to implement its documented procedure for protecting and securely handling BES Cyber System Information, as required by CIP-011-2 R1, Part 1.2.</p> <p>The Entity has a documented information protection program ("program") that details its process to identify and protect BES Cyber System Information. According to the Entity's program, information identified as BES Cyber System Information is [REDACTED]</p> <p>On [REDACTED] The email contained a diagram of [REDACTED]</p> <p>[REDACTED] The employee was on the phone working with the vendor on a project involving [REDACTED] and sent the [REDACTED] for discussion purposes. The impacted [REDACTED] BES Cyber Systems. On [REDACTED], the Entity's [REDACTED] team discovered during a routine review of quarantined emails from its detection software that the email containing BES Cyber System Information was sent unencrypted to an external email address. On [REDACTED]</p> <p>The root cause of this noncompliance was insufficient awareness and training to comply with requirements to protect and securely handle BES Cyber System Information. [REDACTED] Further, encrypting emails is a task that has to be manually executed. The potential for error exists when a task must be manually executed.</p> <p>The noncompliance started on July 20, 2017, when the email was sent. The noncompliance ended on August 11, 2017, when the vendor provided an attestation that the email and diagram were deleted and no copies were distributed. The duration of the noncompliance was 22 days.</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 of this issue is minimal based on the following factors. First, the duration of the noncompliance was short, only 22 days. Second, the vendor that received the BES Cyber System Information had a valid engagement with the Entity [REDACTED] and had fully executed a contract with the Entity containing confidentiality statements. Further, the issue was detected by an internal control that monitors emails for keywords to detect when protected information is being sent unencrypted. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were relevant instances of noncompliance. However, the Entity's compliance history should not serve as a basis for aggravating the risk.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) obtained an attestation from the vendor that the email and copy of the diagram had been deleted and no copies were distributed; 2) provided the manager of the employee with information protection program documentation to review with the manager's team during the next staff meeting; 3) began including CIP knowledge articles in the monthly security newsletter distributed to employees; 4) designed and implemented a rule [REDACTED] to identify and block attempts to send outbound, unencrypted emails containing BES Cyber System Information [REDACTED]; 5) developed [REDACTED]; 6) tested the [REDACTED] to validate functionality; and 7) implemented the [REDACTED]. <p>Texas RE has verified 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
TRE2018019854	CIP-010-2	R4	<div style="background-color: black; width: 100%; height: 15px;"></div> (the "Entity")	<div style="background-color: black; width: 100%; height: 15px;"></div>	04/17/2018	06/04/2018	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 violation.)			<p>On June 7, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-010-2 R4. Specifically, the Entity failed to implement its documented plan for Removable Media on one occasion.</p> <p>The Entity's documented plan requires that Removable Media be registered and inventoried, authorization obtained before use, and a malicious code scan be conducted and mitigated prior to connecting the Removable Media. On April 17, 2018, Removable Media in the form of a DVD was connected to a [REDACTED] BES Cyber Asset (BCA) that is part of a high impact BES Cyber System. The DVD was used to restore the BCA during a recovery. On May 9, 2018, during a discussion between employees [REDACTED], the Entity discovered that Removable Media had been connected to a BCA without following the Entity's documented plan. On June 4, 2018, the Entity added the DVD to its [REDACTED] Removable Media inventory, thereby ending the noncompliance.</p> <p>The root cause of the noncompliance was insufficient controls to ensure that Removable Media requirements were met during recovery and change management processes.</p> <p>The noncompliance started on April 17, 2018, when the Removable Media was connected to the BCA. The noncompliance ended on June 4, 2018, when the Removable Media was added to the Entity's inventory. The duration of the noncompliance was less than 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. The potential risk in connecting Removable Media to a BCA, [REDACTED] without first implementing appropriate security controls is that malicious code could be introduced into a system that is critical to operating the BES. This risk was minimized by the following factors. First, only [REDACTED] Cyber Asset was impacted. Second, no malicious code was detected when the Removable Media was scanned after discovery of the issue. Third, the Removable Media was created from a trusted source. Lastly, the Entity performed a compliance verification on the Cyber Asset and found that no unauthorized baseline configuration changes occurred, no unauthorized local accounts were introduced, anti-virus was working properly, and logging was working properly. No harm is known to have occurred.</p> <p>Texas RE 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) performed a malicious code scan on the DVD; 2) added the DVD to the Removable Media inventory; 3) updated the applicable recovery process document to include Removable Media requirements; 4) integrated Removable Media requirements into the change management process; and 5) completed training on Removable Media requirements. <p>Texas RE has verified 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
TRE2017018193	CIP-010-2	R2, Part 2.1	[REDACTED] (the "Entity")	[REDACTED]	12/01/2016	04/07/2017	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 August 11, 2017, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-010-2 R2, Part 2.1. Specifically, the Entity failed to monitor for changes to the baseline configurations at least once every 35-calendar days.</p> <p>The Entity initially met the requirement to monitor for changes to baseline configurations every 35-calendar days following the July 1, 2016 enforcement date for CIP-010-2 R2. However, during a [REDACTED] spot check the Entity subsequently discovered that for a four-month period it did not complete full reports that met all of the requirements for monitoring changes to baseline configurations as identified in CIP-010-2 R1, Part 1.1, and the monitoring reports were not completed every 35-calendar days. This issue impacted [REDACTED] Cyber Assets.</p> <p>The root cause of this issue was an insufficient process to ensure compliance with CIP-010-2 R2, Part 2.1. The employee responsible for producing the monthly baseline delta monitoring reports misunderstood the compliance requirements for the Standard and the employee's manager did not properly oversee the baseline delta reporting process.</p> <p>This noncompliance started on December 1, 2016, 36 days following the previous fully compliant report to monitor changes to the baseline configurations, and ended on April 7, 2017, when the next fully compliant report to monitor for changes to baseline configurations 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 based on the following factors. First, for the time period at issue the Entity was monitoring for changes to baseline configurations; however, the reports were incomplete and not completed within 35-calendar days. Second, the Entity discovered the issue during an internal spot check, indicating that it has effective detective controls. Lastly, the Entity employs defense-in-depth measures including [REDACTED]. No harm is known to have occurred.</p> <p>Texas RE 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) completed its required review of baseline configuration changes for the Cyber Assets at issue; 2) reprimanded the manager responsible for overseeing the baseline configuration monitoring report process; and 3) additional personnel began reviewing baseline configuration monitoring reports. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017018194	CIP-010-2	R1, Part 1.2	[REDACTED] (the "Entity")	[REDACTED]	07/27/2016	06/15/2018	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 August 11, 2017, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. Specifically, the Entity failed to authorize a change that deviated from the existing baseline configuration as required by CIP-010-2 R1, Part 1.2.</p> <p>During a [REDACTED] spot check, the Entity discovered that [REDACTED]. The noncompliance occurred when the employee installed software on [REDACTED] Cyber Assets. Although a [REDACTED] the employee did not [REDACTED]. Additionally, the employee at issue did not [REDACTED].</p> <p>The root cause of this noncompliance was failure to follow the documented process for compliance with CIP-010-2 R1, Part 1.2. The Entity has a written process for compliance with CIP-010-2 R1, Part 1.2 that requires [REDACTED] to the baseline configuration for applicable devices. However, for this issue the employee did not follow the Entity's process to [REDACTED].</p> <p>This noncompliance started on July 27, 2016, when software was installed on the applicable Cyber Assets without the required authorization to deviate from the existing baseline configurations. This noncompliance ended on June 15, 2018, when the Entity obtained the required written authorization for the deviation to the existing baseline configurations for the applicable Cyber 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 based on the following factors. First, the Entity provided evidence that a manager orally approved the deviations to the existing baseline configurations for the Cyber Assets prior to the work being completed. Second, this issue was discovered during a [REDACTED] spot check demonstrating that the Entity has effective detective controls. Third, the Entity has [REDACTED]. Lastly, the Entity has a process to [REDACTED]. No harm is known to have occurred.</p> <p>Texas RE 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) [REDACTED]; and 2) the employee at issue is no longer employed by the Entity. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018020236	CIP-004-6	R5, Part 5.1	[REDACTED] (the "Entity")	[REDACTED]	08/19/2017	05/21/2018	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 violation.)			<p>On August 14, 2018, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-004-5 R5. Specifically, the Entity did not initiate and complete the removal of an individual's unescorted physical access to applicable BES Cyber Systems within 24 hours of termination, as required by CIP-004-5 R5, Part 5.1.</p> <p>An individual working as an intern with the Entity had authorized unescorted physical access to applicable BES Cyber Systems as required by the individual's job duties. The individual's internship ended on August 18, 2017, but their unescorted physical access was not removed until May 21, 2018.</p> <p>The root cause of this noncompliance was the lack of a control to ensure that unescorted physical access removal requests are completed within 24 hours of a termination action. Additionally, the supervisor was relatively new in the position, and during training for onboarding and offboarding processes, the importance of the offboarding process was not emphasized. As a result, the intern's supervisor did not timely submit a request to remove the intern's access upon a termination action.</p> <p>This noncompliance started on August 19, 2017, 24 hours after the termination action at issue, and ended on May 21, 2018, when the unescorted physical access was removed.</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 individual's card key was returned at the time of the termination action, reducing the risk of unauthorized physical access to a Physical Security Perimeter (PSP). Second, the Entity monitored physical access to its PSPs during the time period at issue, and the Entity's compliance personnel reviewed access control records to confirm that the intern did not access a PSP after the internship ended on August 18, 2017. Third, the Entity discovered this issue on May 20, 2018, during a routine review of user accounts to BES Cyber Assets, demonstrating that the Entity had effective detective controls in place. No harm is known to have occurred.</p> <p>Texas RE 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) removed the individual's unescorted physical access to PSPs; 2) counseled the supervisor regarding the importance of completing an access revocation request for any termination actions; 3) implemented a new onboarding and offboarding process using an added control to ensure that additional personnel track and monitor that access revocations are timely completed; 4) implemented a revised process to address the new onboarding and offboarding process; and 5) completed training on the new onboarding and offboarding process for all managers and personnel who authorize and implement access authorizations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019021079	CIP-007-6 R2	R2, Part 2.2	[REDACTED] (the "Entity")	[REDACTED]	12/26/2018	01/02/2019	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 February 15, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-007-6, R2, Part 2.2. Specifically, the Entity failed to evaluate one security patch within 35 days from its release from the source.</p> <p>While performing a patch assessment on January 2, 2019, the Entity discovered a security patch for one Cyber Asset was not timely evaluated.</p> <p>The root cause of this issue was that the patch source initially identified a vulnerability as a security advisory but did not release the patch until a later date. [REDACTED] On October 11, 2018, one source issued a security advisory and identified a vulnerability, but a patch was not released at that time. The Entity [REDACTED]. On November 20, 2018, the source released a security patch for the vulnerability, however the Entity did not assess the patch because the subject matter expert believed the patch was captured during the October 2018 patch review cycle [REDACTED]. When the discrepancies in the assessment dates were noticed on January 2, 2019, and brought to the attention of management the Entity completed the evaluation of the security patch the same day, ending the noncompliance.</p> <p>This noncompliance started on December 26, 2018, 36 calendar days following release of the applicable security patch from the source, and ended on January 2, 2019, when the Entity evaluated the applicable security patch and added it to an existing 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. First, the Entity assessed the vulnerability in October of 2018 and was aware of the associated risk. Second, the duration of the noncompliance was only eight days. Lastly, the security patch at issue was added to an existing mitigation plan and is not required to be applied until the end of March 2019; therefore, the application of the patch is on schedule pursuant to the mitigation plan. No harm is known to have occurred.</p> <p>Texas RE 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) Evaluated the security patch at issue; and 2) applied the security patch at issue in the test environment and added it to an existing mitigation plan. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017017563	CIP-004-6	R4, Part 4.1	[REDACTED] (the "Entity")	[REDACTED]	01/21/2017	02/02/2017	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 May 15, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R4. Specifically, the Entity failed to implement its documented access management program when [REDACTED] were allowed electronic access to [REDACTED] without the required authorization.</p> <p>On January 21, 2017, the Entity discovered that contractor operators at its security center shared their individual credentials to the Physical Access Control System (PACS) with two contractor trainees who did not have authorized electronic access to the [REDACTED]. Following an investigation, The Entity determined that a total of [REDACTED].</p> <p>The root cause of this noncompliance was an insufficient process to staff the security center with personnel who have authorized electronic access. The Entity has a documented access management program that addresses all of the applicable requirements in CIP-004-6 R4. However, due to insufficient staffing at its security center, the Entity [REDACTED]. The Entity utilizes contractors to staff its security center, and its process requires [REDACTED]. On January 21, 2017, the contractor vendor staffed [REDACTED] due to a shortage of authorized operators with authorized electronic access. Because the contractor trainees did not have the required electronic access, the staff from the previous shift [REDACTED]. The Entity discovered the issue on the same day, and took immediate steps to investigate and mitigate the noncompliance.</p> <p>This noncompliance started on January 21, 2017, when the [REDACTED] received [REDACTED], and ended on February 2, 2017, when the required electronic access for the [REDACTED] at issue was authorized.</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 [REDACTED]. Second, the [REDACTED]. Third, the [REDACTED] during the time period at issue. Lastly, the duration of the noncompliance was relatively short – less than two weeks. No harm is known to have occurred.</p> <p>The Entity has [REDACTED]; however, both are distinguishable from the instant noncompliance. In [REDACTED]. In [REDACTED]. In contrast, the current noncompliance related to failing to grant authorized access to [REDACTED] prior to the contractors at issue gaining access to the applicable Cyber Assets. Therefore, Texas RE 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) authorized electronic access to the applicable Cyber Assets for the [REDACTED] at issue; 2) [REDACTED]; 3) communicated to the contractor vendor the importance of compliance with NERC Reliability Standards and that any future violation of written procedures will result in the termination of the vendor contract; 4) [REDACTED] occur; and 5) [REDACTED]. <p>Texas RE has verified the completion of all mitigation 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
TRE2017018359	CIP-006-6	R1, Part 1.3	[REDACTED] (the "Entity")	[REDACTED]	07/01/2016	05/17/2017	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 violation.)			<p>On September 19, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R1.3. On September 20, 2017, the Entity submitted additional information stating that, as a [REDACTED] it was in noncompliance with the same Requirement. Specifically, the Entity failed to utilize [REDACTED] different physical access controls to allow unescorted physical access into one Physical Security Perimeter (PSP) to only those individuals who have authorized unescorted access.</p> <p>The Entity has a documented process that requires the use of [REDACTED] different physical access controls for PSPs that contain [REDACTED]. On May 17, 2017, an employee alerted the Entity that [REDACTED]. Within the control center, the Entity has a [REDACTED]. The host Cyber Assets [REDACTED]. However, the host devices also had [REDACTED]. The Entity immediately investigated, determined that the PSP required dual authentication for authorized unescorted physical access, and installed a second, different physical access control for the PSP that day to end the noncompliance.</p> <p>The root cause for this issue of noncompliance was the insufficient identification of PSPs that require [REDACTED] physical access controls.</p> <p>This noncompliance started on July 1, 2016, the enforcement date of the Standard, and ended on May 17, 2017, when the Entity implemented a second, different physical access control for the PSP 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 based upon the following factors. First, the PSP at issue was [REDACTED] for the time period at issue, allowing entry only to individuals with authorized unescorted physical access. Additionally, the PSP at issue [REDACTED]. The [REDACTED]. Second, once the issue was discovered, the Entity took immediate steps to end the noncompliance and [REDACTED]. Third, [REDACTED]. Lastly, if a working port for the BES Cyber System assets at issue is [REDACTED]. Additionally, [REDACTED]. No harm is known to have occurred.</p> <p>Texas RE 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) [REDACTED] issue; 2) [REDACTED] properly; and 3) [REDACTED]. <p>Texas RE has verified the completion of all mitigation 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
TRE2017018372	CIP-009-6	R2; R2.1; R2.2	[REDACTED] (the "Entity")	[REDACTED]	07/01/2017	10/03/2018	Compliance 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 violation.)			<p>Issue No. 1 During a Compliance Audit conducted [REDACTED] Texas RE determined that the Entity, as a [REDACTED] was in noncompliance with CIP-009-6 R2.2. Specifically, the Entity failed to test a representative sample of information used to recover BES Cyber System functionality by the initial performance date of July 1, 2017, as outlined by the Implementation Plan for Version 5 CIP Cyber Security Standards and the Implementation Plan Project 2014-02 CIP Version 5 Revisions.</p> <p>The Implementation Plan for Version 5 CIP Cyber Security Standards lists the initial performance of certain periodic requirements in the Version 5 CIP Standards, including CIP-009-5 R2.2, which was given an initial performance date of within 12 calendar months after the effective date of the Version 5 CIP Cyber Security Standards. Implementation Plan Project 2014-02 CIP Version 5 Revisions did not change the initial performance date for CIP-009-6 R2.2. CIP-009-6 became effective on July 1, 2016, and as such, the initial performance date of CIP-009-6 R2.2 was July 1, 2017. During its audit, the Entity provided evidence that its initial performance of CIP-009-6 R2.2 occurred on August 15, 2017. As such, the Entity is unable to demonstrate compliance for CIP-009-6 R2.2 beginning July 1, 2017, and ending August 15, 2017.</p> <p>The root cause of this noncompliance was a lack of awareness of the initial performance date mandated by the CIP Implementation Plans, which was based on 12 calendar months after the effective date of the Version 5 CIP Cyber Security Standards and not the 15 calendar months test periodicity indicated in the requirement. The Entity erroneously interpreted CIP-009-6 R2.2 as the initial performance date periodicity, which states that a representative sample of information used to recover BES Cyber System functionality must be tested at least once every 15 calendar months.</p> <p>Issue No. 2 On December 19, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-009-6 R2.1 and R2.2. The Entity submitted the Self-Report to Texas RE [REDACTED]. Specifically, the Entity self-reported that it did not test each of its recovery plans referenced in CIP-009-6 R1 at least once every 15 calendar months.</p> <p>The Entity completed its initial testing of their CIP-009-6 R1 recovery plan on June 28, 2017. The Entity completed its subsequent testing of their CIP-009-6 R1 recovery plan on October 3, 2018. CIP-009-6 R2.1 requires that recovery plans referenced in CIP-009-6 R1 are tested at least once every 15 calendar months. As such, the Entity is unable to demonstrate compliance with CIP-009-6 R2.1 beginning October 1, 2018, and ending October 3, 2018.</p> <p>The root cause of this noncompliance was an insufficient process implementation. The Entity has implemented [REDACTED] to ensure that periodic CIP tasks are not missed. [REDACTED]. The Entity added a CIP-009-6 R2.1 task to this system; however, when the task was not closed within the appropriate timeframe a follow-up notification was not sent to the manager of the team responsible for performing the task.</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 in not testing a representative sample of information used to recover BES Cyber System functionality is that the information used to recover BES Cyber System functionality may not be in a usable condition when it is needed. The risk in not testing recovery plans within 15 calendar months is that the recovery plans may be out of date and not in a usable state when it is needed. The risk for these instances of noncompliance is reduced due to the following:</p> <p>Issue No. 1 1) The Entity did test a representative sample of information used to recover BES Cyber System functionality within 15 calendar months, as prescribed the standard. This noncompliance occurred because the initial performance of this requirement was 12 months from the effective date of the standard, which the Entity did not comply with.</p> <p>Issue No. 2 1) The duration of noncompliance was very short, lasting less than three days.</p> <p>No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>Issue No. 1 To end this noncompliance the Entity performed the following mitigating activities: 1) performed a test of a representative sample of information used to recover BES Cyber System functionality.</p> <p>Issue No. 2 To end this noncompliance the Entity performed the following mitigating activities: 1) tested their CIP-009-6 R1 recovery plan.</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
TRE2017018188	CIP-004-6	R4; Parts 4.1 and 4.4	[REDACTED] (the "Entity")	[REDACTED]	07/01/2016	03/09/2018	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 violation.)			<p>On August 14, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] it had three instances of noncompliance with CIP-004-6 R4. Upon further investigation, Texas RE determined that the Entity was in noncompliance with CIP-004-6 R4 in only two instances.</p> <p>In the first instance, on September 07, 2016, an employee was reviewing system permissions and [REDACTED], as required by CIP-004-6 R4, Part 4.1. The [REDACTED] the Entity's transition to CIP Version 5. The [REDACTED] employees had been granted access via local accounts on the servers prior to CIP Version 5 and the patching system being onboarded into the Entity's access management system. After the patching system was onboarded into the access management system, access was configured to be provisioned at the domain-level using an Active Directory group and access was requested for existing users so there were authorization records on file. For the [REDACTED], the Entity did not have authorization records. After discovery of the issue, access requests were entered in the access management system for the [REDACTED] employees. Access was approved for [REDACTED]. Access was rejected and removed for [REDACTED].</p> <p>For the first instance, the noncompliance started on July 1, 2016, when CIP-004-6 R4 became mandatory and enforceable. The noncompliance ended on September 26, 2016, when access was rejected and removed for the last impacted employee. The duration of the noncompliance was less than three months.</p> <p>In the second instance, on October 13, 2016, the Entity discovered that it had not included its [REDACTED] in its access management system as part of its CIP Version 5 transition. As a result, the Entity did not implement a process to authorize access based on need for the application, as required by CIP-004-6 R4, Part 4.1. Further, the Entity failed to timely perform a verification that access privileges are correct and are those that the Entity determined are necessary for performing assigned work functions, as required by CIP-004-6 R4, Part 4.4. On December 6, 2017, the Entity onboarded the application into its access management system as designated storage location of BES Cyber System Information, thereby implementing a process to authorize access based on need. On March 9, 2018, the Entity completed a review to verify access privileges are correct and are those that the Entity determined are necessary for performing assigned work functions.</p> <p>For the second instance, the noncompliance started on July 1, 2016 when CIP-004-6 R4 became mandatory and enforceable. The noncompliance ended on March 9, 2018, when the Entity completed a review to verify access privileges are correct and are those that the Entity determined are necessary for performing assigned work functions. The duration of the noncompliance was approximately 20 months.</p> <p>The root cause of the noncompliance is insufficient process and controls to ensure that access is properly managed. First, the Entity lacked a consistent method to provision access. Second, gaps existed in the process of implementing access management controls for systems that were being brought into CIP scope as part of the transition to CIP Version 5. The [REDACTED]. As a result, during the CIP Version 5 transition, access was either not appropriately onboarded in the access management system and included in the required access management processes and controls.</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 was minimized by the following factors. In both instances, all employees with access to the impacted systems had completed cyber security training and had a Personnel Risk Assessment (PRA) on file. For the first instance, the duration was short, lasting less than three months. For the second instance, the issue was limited to the application-level as access to the system at the Cyber Asset-level was being appropriately controlled for EACMS Cyber Assets. Further, for the second instance, the only users permitted to access the system for the duration of the noncompliance were employees who required access to support the vulnerability management process. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were relevant instances of noncompliance. However, the Entity's compliance history should not serve as a basis for aggravating the risk as the prior noncompliance involved different facts and root cause.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) corrected the first instance by requesting and approving the access for some employees and removing the access for other employees; 2) corrected the second instance by [REDACTED] and completing a review to verify access privileges are correct and are those that [REDACTED] determined are necessary for performing assigned work functions; 3) performed an extent of condition review; 4) [REDACTED]; 5) [REDACTED] ioning; and 6) implemented a detective control to identify when access is not provisioned through Active Directory. <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
TRE2019021059	CIP-003-6	R3	[REDACTED] (the "Entity")	[REDACTED]	12/01/2018	02/08/2019	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 February 13, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-003-6 R3. In particular, the Entity failed to identify its CIP Senior Managers by name and document any change within 30 calendar days of the change. According to the Entity, [REDACTED] and this neglected to keep the timeline for reporting within their written compliance program.</p> <p>This noncompliance started on December 1, 2018, which is the date 31 days after the previous CIP Senior Manager terminated employment with the Entity and ended on February 8, 2018, when the Entity identified its new CIP Senior Manager by name.</p> <p>The root cause of this noncompliance was a lack of proper procedures. The Entity had an internal CIP-003-6 policy within its compliance program; however, this policy only included entries for CIP-003-6 R1 and R2.</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 CIP Senior Manager has overall authority and responsibility for leading and managing implementation of and continuing adherence to the NERC CIP Standards. The risk in not identifying a CIP Senior Manager is it may result in a lack of guidance that can result in an entity not complying with NERC CIP Requirements. No harm is known to have occurred.</p> <p>Texas RE 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) identified its new CIP Senior Manager by name. 2) updated its procedures to include verbiage around the identification of a CIP Senior Manager and updates upon a change to the designation of a CIP Senior Manager. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019021060	CIP-003-6 R4	R4	[REDACTED] (the "Entity")	[REDACTED]	09/30/2018	02/08/2019	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 February 13, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-003-6 R4. In particular, the Entity failed to document a change in delegation within 30 days of the change. According to the Entity, [REDACTED] and this neglected to keep the timeline for reporting within their written compliance program.</p> <p>This noncompliance started on September 30, 2018, which is the date 31 days after the termination of employment of the individual with delegated authority and ended on February 8, 2019, when the Entity's documentation was updated to reflect the removal of delegated authority.</p> <p>The root cause of this non-compliance was a lack of proper procedures. The Entity had an internal CIP-003-6 policy within its compliance program; however, this policy only included entries for CIP-003-6 R1 and R2.</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. A CIP Senior Manager delegate has the authority to act on behalf of the CIP Senior Manager on a subset of CIP Requirements where CIP Senior Manager approval is needed. The risk in not updating a delegation after a change to the delegation is an individual who is no longer authorized to act on behalf of the entity may make authorizations that the CIP Senior Manager would not normally approve of.</p> <p>The risk of this noncompliance is reduced due to the following:</p> <ol style="list-style-type: none"> 1) The BES Cyber Systems owned by the Entity are all [REDACTED] BES Cyber Systems. As such, the only CIP Standards that apply to the Entity are CIP-002-5.1a and CIP-003-6. Of these standards, the only requirement where a delegate can act on behalf of the CIP Senior Manager is CIP-002-5.1a R2.2, the approval of identifications of BES Assets and BES Cyber Systems in CIP-002-5.1a R1. <p>No harm is known to have occurred.</p> <p>Texas RE 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) updated documentation to indicate the change in delegation. 2) updated their procedure to include verbiage around the delegation of CIP Senior Manager authority and updating of documentation around delegations after a change. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018020691	CIP-009-6	R2	[REDACTED] (the "Entity")	[REDACTED]	07/01/2017	06/11/2018	Compliance 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 violation.)			<p>During a [REDACTED], Texas RE determined that the Entity, as a [REDACTED] was in noncompliance with CIP-009-6 R2.2. In particular, the Entity was unable to demonstrate it had tested a representative sample of information used to recover system functionality for a [REDACTED] by the initial performance date of CIP-009-6 R2.2.</p> <p>This noncompliance started on July 1, 2017, which is the initial performance deadline for CIP-009-6 R2.2 and ended on June 11, 2018, when the Entity tested information necessary to recover the functionality of the sampled [REDACTED].</p> <p>The root cause of this noncompliance was a failure to follow documented procedures. The Entity has a documented procedure covering the testing of their recovery plans. This document is scoped to include the testing of PACS and requires the testing be conducted at least once every 15 calendar 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. The risk in not testing a representative sample of information used to recover system functionality and ensuring that the information is useable and compatible with current configurations is that in the event of device or system failure the recovery information may be in a non-usable condition. This can increase recovery time during which time the cyber asset or system is potentially unavailable or operating in a degraded condition.</p> <p>The risk posed by this noncompliance is reduced due to the following:</p> <ul style="list-style-type: none"> 1) The Entity's [REDACTED] for which the recovery information was not tested performs daily backups. <p>No harm is known to have occurred.</p> <p>Texas RE 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> <ul style="list-style-type: none"> 1) Tested the information necessary to recover the functionality of the [REDACTED] t. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018020692	CIP-008-5	R2	[REDACTED] (the "Entity")	[REDACTED]	07/01/2017	07/27/2018	Compliance 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 violation.)			<p>During a [REDACTED] Texas RE determined that the Entity, as a [REDACTED], was in noncompliance with CIP-008-5 R2.1. In particular, the Entity's test of their Cyber Security Incident response plan was not performed using a Reportable Cyber Security Incident.</p> <p>This noncompliance started on July 1, 2017, when CIP-008-5 R2.1 was required to be tested with a Reportable Cyber Security Incident and ended on July 27, 2018, when the Entity [REDACTED].</p> <p>The root cause of this noncompliance was a failure to follow documented procedures. The Entity's Cyber Security Incident Response Plan includes a section for plan testing and requires that the Entity test the plan at least once every 15 calendar months using one of the following methods:</p> <ol style="list-style-type: none"> 1) By responding to a Reportable Cyber Security Incident; 2) By performing a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or 3) By performing an operational exercise of a Reportable Cyber Security Incident. 					
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. An entity that fails to test their Cyber Security Incident Response plan using a Reportable Cyber Security Incident is at risk of not detecting gaps in the plan or of failing to identify potential improvements in the plan. This can lead to an entity being unprepared should a Reportable Cyber Security Incident occur.</p> <p>The risk posed by this non-compliance is mitigated due to the following:</p> <ol style="list-style-type: none"> 1) The Entity [REDACTED]; and 2) [REDACTED]. <p>No harm is known to have occurred.</p> <p>Texas RE 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) [REDACTED]. <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
TRE2019021290	CIP-003-6	R1	[REDACTED] (the "Entity")	[REDACTED]	11/01/2018	01/17/2019	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 2, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-003-6 R1. According to the Entity, it failed to review and obtain CIP Senior Manager approval for its documented Cyber Security Policy at least once every 15 calendar months.</p> <p>The Entity [REDACTED]. The Entity's subsequent review and [REDACTED].</p> <p>This noncompliance started on [REDACTED], when the Entity performed a review of its cyber security policy and acquired CIP Senior Manager approval.</p> <p>The root cause of this noncompliance was a lack of internal controls. The Entity was not tracking the annual review timeline prior to this incident.</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 in not reviewing cyber security policies in a timely manner is this can result in policies being out of date and no longer applicable to the environment they are intended to protect.</p> <p>The risk posed by this noncompliance is mitigated as upon reviewing their cyber security policies the Entity determined that no meaningful changes were needed. No harm is known to have occurred.</p> <p>Texas RE 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) Reviewed their cyber security policy; and 2) Received CIP Senior Manager approval of their cyber security policy. <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
TRE2019021291	CIP-011-2	R1.2	██████████ (the "Entity")	██████████	01/31/2019	03/29/2019	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 March 29, 2019, the Entity submitted a Self-Log stating that, as a ██████████ it was in noncompliance with CIP-011-2 R1. Specifically, the Entity discovered that drawing files for ██████████ that contain ██████████ BES Cyber Systems were stored in an electronic repository that had not been identified as a designated storage location for BES Cyber System Information.</p> <p>This noncompliance started on January 31, 2019, when the Entity uploaded drawing files containing BES Cyber System Information to an unauthorized storage location and ended on March 29, 2019, when the Entity removed the BES Cyber System Information from the unauthorized storage location.</p> <p>The root cause of this noncompliance was a failure to follow established procedure. The Entity has a documented procedure covering its BES Cyber System Information Protection Program, in accordance with CIP-011-2 R1. The Entity's procedure identifies ██████████ where BES Cyber System Information is authorized to be stored. The drawing files related to this self-log were stored in a location that is not identified in the Entity's procedure as an authorized storage location.</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 in storing BES Cyber System Information in unauthorized storage locations is the storage locations may not have the level of security controls commensurate to the sensitivity of the stored data. This can lead to the exfiltration of data that can be used to plan an attack against one or more BES Assets or BES Cyber Systems.</p> <p>The risk posed by this noncompliance is reduced due to the following:</p> <ol style="list-style-type: none"> 1) The documents were stored in a secure repository that required administrator approval to gain access. 2) Administrator approval for access to the repository was only granted to individuals that had a business need for access. <p>No harm is known to have occurred.</p> <p>Texas RE 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) Moved the documents to a designated storage location. <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
WECC2017018873	CIP-007-6	R5: P5.7	[REDACTED]	[REDACTED]	7/1/2016	5/22/2018	Compliance 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 violation.)			<p>During a Compliance Audit conducted [REDACTED], WECC determined that the entity, as a [REDACTED], had a potential noncompliance with CIP-007-6 R5 P5.7.</p> <p>Specifically, the entity failed to request a Technical Feasibility Exception (TFE) for [REDACTED] Bulk Electric System (BES) Cyber Assets (BCAs) associated with a High Impact BES Cyber System (HIBCS) at its primary and backup Control Centers, that were technically incapable of limiting the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful authentication attempts as required by Part 5.7.</p> <p>After reviewing all relevant information, WECC Enforcement concurred with the audit findings as stated above. The root cause of the issue was insufficient controls in the Cyber Asset onboarding process. Specifically, the entity had a documented process that provided instructions as to how to request a TFE; however, the entity did not have controls in place to confirm that a TFE was requested, when required to meet compliance.</p> <p>This issue began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on May 22, 2018 when the entity submitted a TFE request to WECC, for a total of 691 days.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to request a TFE for [REDACTED] BCAs that were technically incapable of limiting the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful authentication attempts as required by CIP-007-6 R5 Part 5.7.</p> <p>However, the entity's failure was limited to a documentation deficiency. Additionally, the [REDACTED] BCAs were located inside locked cabinets within two different Physical Security Perimeters. As further compensation, the entity implemented passwords which were unique to each of the [REDACTED] BCAs and any compromise to a single BCA would be restricted to that BCA only. No harm is known to have occurred.</p> <p>The entity has no relevant previous noncompliance of this or similar Standards and Requirements.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) submitted a TFE request for the [REDACTED] BCAs; 2) reviewed its Cyber Asset onboarding process for opportunities to strengthen the process and controls; and 3) implemented additional controls, including oversight and procedural tools, such as an onboarding checklist and a TFE eligibility form. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020256	CIP-004-6	R4	[REDACTED]	[REDACTED]	7/1/2017	4/2/2018	Self-Report	Complete
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 17, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4. Specifically, the entity did not verify that the electronic access to two designated logical storage locations for Bulk Electric System (BES) Cyber System Information (BCSI) was correct and necessary for performing assigned work functions within 12 calendar months after July 1, 2016 as per the NERC CIP Version 5 Implementation Plan. The two BCSI storage locations were not listed in the entity's documented processes; therefore, were not included in the email notifications sent out by the entity as part of its review and verification process for the other BCSI storage locations.</p> <p>After reviewing all relevant information, WECC determined the entity failed to verify by July 1, 2017 that access to all its BCSI storage locations, whether physical or electronic, were correct and necessary for performing assigned work functions as required by CIP-004-6 R4 Part 4.4. The root cause of the issue was less than adequate processes. Specifically, the entity had a list of BCSI storage locations which included the two in scope of this issue; however, its documented processes for access review of BCSI storage locations did not point to that specific list but rather included a list of BCSI storage locations, which had not been updated to include the two locations in scope of this issue.</p> <p>This issue began on July 1, 2017, when access to all BCSI storage locations should have been verified and ended on April 2, 2018, when access was verified for the two BCSI storage locations in scope, for a total of 276 days.</p>					
Risk Assessment			<p>WECC determined 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, the entity failed to verify by July 1, 2017 that access to all its BCSI storage locations whether physical or electronic were correct and necessary for performing assigned work functions as required by CIP-004-6 R4 Part 4.4</p> <p>However, as compensation, the few individuals with electronic access to the BCSI storage locations had authorization for said access and once the verification was performed, it was determined that the access was correct and necessary for performing assigned work functions. Additionally, a review of access controls determined that no unauthorized access to the two BCSI storage locations occurred during the noncompliance duration. Lastly, any BCSI that could have been compromised during the noncompliance became obsolete due to the entity's implementation of a new Energy Management System. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) performed a verification of access for the two BCSI storage locations; 2) created a designated storage location management procedure to document the process for identifying BCSI storage locations and how to protect BCSI, to include how BCSI storage locations are established; how to monitor access authorizations, roles and responsibilities; and what evidence must be collected; 3) updated its access management program by creating an appendix that defines the roles and responsibilities for access authorization, revocation, granting, and the review of access; 4) updated its information protection program to include references to the BCSI storage location management procedure; and 5) conducted training to applicable personnel on the created and updated program documents. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018363	CIP-004-6	R5; P5.1; P5.2; P5.3	[REDACTED]	[REDACTED]	Instance #1 11/23/2016 Instance #2 10/2/2016 Instance #3 3/9/2017 Instance #4 10/2/2016	Instance #1 12/22/2016 Instance #2 10/3/2016 Instance #3 3/18/2017 Instance #4 10/3/2016	Compliance 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 violation.)			<p>During a Compliance Audit conducted [REDACTED], WECC determined that the entity, as a [REDACTED], had a potential noncompliance with CIP-004-6 R5. Specifically, for four separate instances the entity's evidence demonstrated that the completion of access revocation did not occur as required by CIP-004-6 R5. For the first and second instances, the removal access was not completed within 24 hours as required by Part 5.1 of CIP-004-6 R5. In these two instances one employee had unescorted physical access to High Impact Bulk Electric System (BES) Cyber Systems (HIBCS) and the other employee had unescorted physical access to Medium Impact BES Cyber Systems (MIBCS). For the third instance, the removal of unescorted physical access to MIBCS was not completed after a reassignment by the end of the next calendar day following the date the employee no longer required retention of that access, as required by Part 5.2 of CIP-004-6 R5. The employee had unescorted physical access to HIBCS. Lastly, for the fourth instance, the removal of access to a designated storage location for BES Cyber System Information (BSCI) was not completed by the end of the next calendar day following the effective date of the termination action, as required by Part 5.3 of CIP-004-6 R5.</p> <p>After reviewing all relevant information, WECC concurred with the audit finding as stated above. The root cause of these instances was a less than adequate process for the tracking of offboarding and training of employees who perform offboarding to ensure tasks are completed on time.</p> <p>These issues started when access removals were not performed within the required timeframe of CIP-004-6 R5 and ended when access removals were completed as described as follows: For the first issue, the start date is November 23, 2016 and the end date is December 22, 2016, for a total of 30 days; for the second issue the start date is October 2, 2016 and the end date is October 3, 2016, for a total of two days; for the third issue, the start date is March 9, 2017 and the end date is March 18, 2017 for a total of 10 days; and for the fourth issue, the start date is October 2, 2016 and the end date is October 3, 2016, for a total of two days.</p>					
Risk Assessment			<p>WECC determined 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 the entity failed 1) for a termination of two employees...to complete the removals of unescorted physical access within 24 hours of a termination action as required by CIP-004-6 R5 Part 5.1; 2) for a reassignment...revoke unescorted physical access that was not necessary by the end of the next calendar day following the date that the retention of that access was no longer required as required by CIP-004-6 R5 Part 5.2; and 3) for a termination action revoke...access to a designated storage location for BSCI...by the end of the next calendar day following the effective date of the termination action as required by CIP-004-6 R5 Part 5.3.</p> <p>The entity had implemented good controls in its documented processes that centralized the access revocation process to its Human Resources administrator and the CIP Senior Manager. The entity had initiated access removals in all four instances; however, did not complete the removals in a timely manner. The employees in scope had either retired, resigned, or were reassigned and were in good standing with the entity and the entity had initiated the removal of these employee's ability for unescorted physical access and Interactive Remote Access upon the termination action. No harm is known to have occurred.</p> <p>WECC determined the entity's compliance history should not serve as a basis for pursuing an enforcement action and/or applying a penalty as the root cause and fact pattern of this CE are separate and distinct from the prior noncompliance.</p>					
Mitigation			<p>To mitigate these instances, the entity has:</p> <ul style="list-style-type: none"> a) collected all the hard keys that could be used to access the PSPs; b) implemented a program procedure to include deadline reviews related to granting and revoking access; and c) performed annual training on the access revocation process to improve awareness on appropriate access revocation processes and deadlines. <p>As an additional measure, the entity will complete by June 30, 2019 the implementation of a Sharepoint workflow to improve the onboarding, role change, and exit process for personnel. The workflow will ensure the correct people receive timely information on personnel changes. This will increase transparency and prove an internal control for deadlines and notifications.</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
WECC2019021066	CIP-004-6	R5	[REDACTED]	[REDACTED]	2/7/2019	2/12/2019	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.)			On February 15, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5. Specifically, on January 7, 2019 the entity terminated two employees who had access to a shared account on a Physical Access Control System (PACS) and the password was not changed within 30 calendar days of the termination action which would have been no later than February 6, 2019. The entity changed the password on February 12, 2019, for a total of six days late. The root cause of the issue was a lack of an internal control to ensure that activities were completed in a timely manner. The entity had a process in place to perform the requirement; however, no internal control to prevent this issue.					
Risk Assessment			<p>WECC determined 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, the entity failed, for two termination actions, to change the passwords for a shared account known to the users within 30 calendar days of the termination action as required by CIP-004-6 R5 Part 5.5.</p> <p>However, the entity had implemented good detective controls. Specifically, this issue was identified quickly utilizing the entity's Internal Compliance Program. As compensation, the terminated employees only had on-site unescorted physical access to Cyber Assets. No harm is known to have occurred.</p> <p>The entity has no relevant noncompliance with this Standard and Requirement.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) changed the password on the shared account; 2) created a control intended to enhance its procedure by adding a Compliance Department review of termination and password changes; and 3) added a process for an email to be sent from the compliance team to the manager of the system admin to verify if the person had shared accounts. The Compliance team will then request the system admin change the password. This step is created as an additional oversight and control to ensure this action is completed within 30 days of the termination action. <p>WECC has verified completion of all 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
WECC2019021268	CIP-006-6	R2	[REDACTED]	[REDACTED]	3/18/2019	3/18/2019	Self-Report	Completed OR 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 violation.)			<p>On March 26, 2019, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-006-6 R2. Specifically, on March 18, 2019 an entity employee continuously escorted a visitor into the Physical Security Perimeter (PSP) that was protecting [REDACTED] without first obtaining a visitor badge and appropriately logging the visitor's exit from the PSP, per the entity's documented program. The visitor was there to empty shredding boxes. The entity employee had received visitor escorting training two months prior. The root cause of the issue was a failure in judgement by the entity employee in that they did not follow the Physical Security Plan which requires visitors to be issued a visitor's badge and be recorded in the visitor logbook. This issue began on March 18, 2019 when the entity's documented visitor control program was not implemented correctly and ended on March 18, 2019, when the logbook was appropriately filled out, for a total of one day.</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 BPS. In this instance, the entity failed to properly implement its documented visitor control program as required by CIP-006-6 R2 Part 2.2.</p> <p>However, the entity had implemented good internal controls. Specifically, the entity had a video surveillance system which is how this issue was promptly discovered. As compensation, the escort performed continuous escorting of the visitor while in the PSP and the visitor was in the PSP for a short period of time to perform legitimate business activities. No harm is known to have occurred.</p> <p>WECC determined the entity's compliance history should not serve as a basis for pursuing an enforcement action and/or applying a penalty because the entity's relevant compliance history is limited to one violation.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) recorded the visitor's entry into and exit from the PSP in the logbook; 2) discussed with the employee, the requirements for escorting visitors; and 3) sent the Physical Security Plan and visitor awareness documents to all employees as a refresher to the training received in January of 2019. <p>WECC has verified completion of all 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
WECC2016016694	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/1/2016	10/22/2018	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 violation.)			<p>On December 16, 2016, the entity submitted a Self-Report, stating that as a [REDACTED] ([REDACTED]), it was in noncompliance with CIP-010-2 R1. Specifically, in July of 2016, during a post-implementation of CIP Version 6, the entity discovered that initial baseline configurations for three Cyber Assets within an Electronic Security Perimeter (ESP) had not been obtained. The Cyber Assets included two control panels classified as Physical Access Control Systems (PACS) and one printer classified as a Protected Cyber Asset (PCA) associated with its Medium Impact Bulk Electric System (BES) Cyber System (MIBCS) located at the primary and backup Control Centers.</p> <p>After reviewing all relevant information, WECC Enforcement determined the entity failed to develop a baseline configuration, individually or by group for three Cyber Assets, as required by CIP-010-2 R1 Part 1.1. During WECC's review of this CIP-010-2 R1 Part 1.1 issue, it was also determined that the entity failed to document enabled logical network accessible ports that were determined to be needed by the entity as required by CIP-007-6 R1 Part 1.1. WECC did not request the entity submit a separate Self-Report for the CIP-007-6 R1 Part 1.1. issue because the mitigation was not complex, and the root cause was the same as the CIP-010-2 R1 Part 1.1 issue.</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable, and ended on October 22, 2018, when the entity developed baseline configurations and documented enabled logical network accessible ports for the two PACS and one PCA, for a total of 844 days.</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. In these instances, the entity failed to develop a baseline configuration, individually or by group for three Cyber Assets, as required by CIP-010-2 R1 Part 1.1 and document enabled logical network accessible ports that were determined to be needed by the entity, including port ranges or services where needed to handle dynamic ports, as required by CIP-007-6 R1 Part 1.1.</p> <p>However, as compensation, the Cyber Assets in scope were located within a secure Physical Security Perimeter (PSP) and ESP. The entity utilized badge access cards to gain access to the PSP and monitored all ESP access through its intrusion detection system. Additionally, the PACS [REDACTED]. The entity monitors and operates less than [REDACTED] miles of transmission lines, one generating facility that is rated less than [REDACTED] MW and [REDACTED]. No harm is known to have occurred.</p> <p>WECC determined the entity did not have any applicable compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated baseline configurations for the two PACS and one PCA; 2) documented enabled logical network accessible ports that have been determined to be needed and provide business justification for the two PACS and one PCA; 3) provided training to appropriate personnel on the requirements of initial baseline configurations; 4) updated its procedure to include the Requirements which allow for Technical Feasibility Exceptions; and 5) distributed the new procedures to appropriate personnel. <p>WECC 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
WECC2017018244	CIP-007-6	R5	[REDACTED]	[REDACTED]	7/1/2016	09/01/2017	Compliance 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 violation.)			<p>During a Compliance Audit conducted [REDACTED] through [REDACTED], WECC determined the entity, as a [REDACTED], [REDACTED], [REDACTED], [REDACTED] and [REDACTED] had a potential noncompliance with CIP-007-6 R5 Parts 5.1, 5.2, 5.4, and 5.5. Specifically, the entity failed to submit a Technical Feasibility Exception (TFE) for two Physical Access Control Systems (PACS) that were not capable of enforcing authentication of interactive user access as required by CIP-007-6 R5 Part 5.1; failed to identify and inventory all known enabled default or other generic account types as required by CIP-007-6 R5 Part 5.2; failed to change known default passwords, per Cyber Asset capability as required by CIP-007-6 R5 Part 5.4; and failed to enforce password parameters as required by CIP-007-6 R5 Part 5.5.</p> <p>After reviewing all relevant information, WECC Enforcement concurred with the audit findings as stated above.</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable, and ended on September 1, 2017, when for the two PACS, the entity submitted a TFE; documented the default or other generic accounts; and updated the default passwords to meet the length and complexity requirements, for a total of 428 days.</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. In this instance, the entity failed to submit a TFE for two PACS that were not capable of enforcing authentication of interactive user access as required by CIP-007-6 R5 Part 5.1; identify and inventory all known enabled default or other generic account types for two PACS as required by CIP-007-6 R5 Part 5.2; for two PACS, change known default passwords, per Cyber Asset capability as required by CIP-007-6 R5 Part 5.4; and enforce password parameters for two PACS as required by CIP-007-6 R5 Part 5.5.</p> <p>However, as compensation, the Cyber Assets in scope were located within a secure Physical Security Perimeter (PSP) and Electronic Security Perimeter (ESP). The entity utilized badge access cards to gain access to the PSP and monitored all ESP access through its intrusion detection system. Additionally, the PACS [REDACTED]. The entity monitors and operates less than [REDACTED] miles of transmission lines, one generating facility that is rated less than [REDACTED] MW and [REDACTED]. No harm is known to have occurred.</p> <p>WECC determined the entity did not have any applicable compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, WECC:</p> <ol style="list-style-type: none"> 1) submitted TFEs for the two PACS; 2) documented the default or other generic account(s) for the two PACS; 3) updated passwords on the two PACS to meet the length and complexity requirements; 4) implemented new software which will allow the entity to update the PACS without vendor support; 5) updated its tracking document to include the PACS passwords on its 15-calendar month cycle; 6) updated its procedure to include the Requirements which allow for TFEs; and 7) distributed the new procedures to appropriate personnel. <p>WECC 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
WECC2018020468	CIP-007-6	R5	[REDACTED]	[REDACTED]	7/1/2016	10/27/2017	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 October 2, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED] it had a potential noncompliance with CIP-007-6 R5. Specifically, when implementing security controls in preparation for CIP Version 6 implementation, entity personnel discovered they could not apply the necessary protective measures of CIP-007-6 R5 Part 5.7 on two Physical Access Control Systems (PACS) and two Protected Cyber Asset (PCA) due to device capability limitations. Entity personnel were not aware that they needed to submit Technical Feasibility Exception (TFEs) for these four Cyber Assets.</p> <p>After reviewing all relevant information, WECC Enforcement determined the entity failed to submit a TFE for four Cyber Assets (two PACS and two PCAs), that were not capable of limiting the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful authentication attempts as required by CIP-007-6 R5 Part 5.7.</p> <p>The root cause of all these issues was attributed to a less than adequate process for transitioning to CIP Version 6. Specifically, the entity was unaware of how the Standards and Requirements applied to the Cyber Assets in scope and therefore did not properly document or communicate the necessary steps to be compliant.</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable, and ended on October 27, 2017, when the entity submitted a TFE for all four Cyber Assets, for a total of 484 days.</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. In this instance, the entity failed to submit a TFE for four Cyber Assets that were not capable of limiting the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful authentication attempts as required by CIP-007-6 R5 Part 5.7.</p> <p>However, as compensation, the Cyber Assets in scope were located within a secure Physical Security Perimeter (PSP) and Electronic Security Perimeter (ESP). The entity utilized badge access cards to gain access to the PSP and monitored all ESP access through its intrusion detection system. Additionally, the PACS [REDACTED]. The entity monitors and operates less than [REDACTED] miles of transmission lines, one generating facility that is rated less than [REDACTED] and [REDACTED]. No harm is known to have occurred.</p> <p>WECC determined the entity did not have any applicable compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) submitted TFEs for all four Cyber Assets; 2) updated its procedure to include the Requirements which allow for TFEs; and 3) distributed the new procedures to appropriate personnel. <p>WECC has verified the completion of all mitigation activity.</p>					

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	SPP2017018669	Yes		Yes	Yes					Yes	Yes		Yes	Category 1: 3 years; Category 2 – 12: 2 year
2	MRO2017018151			Yes	Yes					Yes	Yes			Category 2 – 12: 2 years
3	MRO2018019579	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
4	MRO2018019582			Yes	Yes									Category 2 – 12: 2 years
5	MRO2018019583			Yes	Yes									Category 2 – 12: 2 years
6	MRO2018020834			Yes	Yes									Category 2 – 12: 2 years
7	MRO2018020842			Yes	Yes									Category 2 – 12: 2 years
8	MRO2018020843			Yes	Yes									Category 2 – 12: 2 years
9	MRO2018020162	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
10	MRO2018020170	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
11	MRO2018020275			Yes	Yes					Yes				Category 2 – 12: 2 years
12	MRO2018020276	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
13	MRO2018020791			Yes	Yes					Yes				Category 2 – 12: 2 years
14	MRO2019020940			Yes	Yes					Yes				Category 2 – 12: 2 years
15	MRO2019020941			Yes	Yes					Yes				Category 2 – 12: 2 years
16	MRO2019020942			Yes	Yes					Yes				Category 2 – 12: 2 years
17	MRO2019020943			Yes	Yes					Yes				Category 2 – 12: 2 years
18	MRO2019020944			Yes	Yes					Yes				Category 2 – 12: 2 years
19	MRO2019020950			Yes	Yes					Yes				Category 2 – 12: 2 years
20	RFC2018020503	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
21	RFC2018020607	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
22	RFC2018020251	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
23	RFC2018020025	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
24	RFC2018020024	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
25	RFC2018020756	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
26	RFC2018019286	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
27	RFC2019021331	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
28	SERC2016016281			Yes	Yes					Yes				Category 2 – 12: 2 year
29	SERC2017017231			Yes	Yes					Yes				Category 2 – 12: 2 year

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)
30	SERC2017018403			Yes	Yes									Category 2 – 12: 2 year
31	SERC2017018549			Yes	Yes					Yes				Category 2 – 12: 2 year
32	SERC2018019232			Yes	Yes				Yes	Yes	Yes	Yes		Category 2 – 12: 2 year
33	SERC2016016174			Yes	Yes				Yes	Yes	Yes	Yes		Category 2 – 12: 2 year
34	SERC2017017711			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
35	SERC2017017712			Yes	Yes									Category 2 – 12: 2 year
36	SERC2017018140			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
37	SERC2016016095			Yes	Yes						Yes	Yes		Category 2 – 12: 2 year
38	SERC2016015989			Yes	Yes					Yes	Yes	Yes		Category 2 – 12: 2 year
39	SERC2018019392			Yes	Yes						Yes			Category 2 – 12: 2 year
40	SERC2018020087			Yes	Yes									Category 2 – 12: 2 year
41	SERC2016015942		Yes	Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
42	SERC2016016675			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
43	SERC2017016977			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
44	SERC2017017797			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
45	SERC2017018381			Yes	Yes					Yes				Category 2 – 12: 2 year
46	SERC2018018993			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
47	SERC2017017233			Yes	Yes									Category 2 – 12: 2 year
48	SERC2017017234			Yes	Yes								Yes	Category 2 – 12: 2 year
49	SERC2018019099			Yes	Yes									Category 2 – 12: 2 year
50	SERC2018019267			Yes	Yes									Category 2 – 12: 2 year
51	SERC2017017037			Yes	Yes									Category 2 – 12: 2 year
52	SERC2017018100			Yes	Yes									Category 2 – 12: 2 year
53	SERC2016016170			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
54	SERC2016016508			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
55	SERC2017016786			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
56	TRE2017017014	Yes		Yes	Yes							Yes		Category 1: 3 years; Category 2 – 12: 2 year
57	TRE2017017015	Yes		Yes	Yes							Yes		Category 1: 3 years; Category 2 – 12: 2 year
58	TRE2017017016	Yes		Yes	Yes							Yes		Category 1: 3 years; Category 2 – 12: 2 year
59	TRE2017017019	Yes		Yes	Yes							Yes		Category 1: 3 years; Category 2 – 12: 2 year
60	TRE2017017023	Yes		Yes	Yes							Yes		Category 1: 3 years; Category 2 – 12: 2 year
61	TRE2017017707	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
62	TRE2017018092	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
63	WECC2017018482		Yes	Yes										Category 1: 3 years; Category 2 – 12: 2 year
64	WECC2017018435	Yes	Yes	Yes									Yes	Category 1: 3 years; Category 2 – 12: 2 year
65	WECC2017018877	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year

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)
66	WECC2018020556	Yes		Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 year
67	WECC2018019943			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
68	WECC2018020224			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
69	WECC2018020715	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
70	WECC2018019243	Yes		Yes	Yes									Category 1: 3 years; 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
SPP2017018669	CIP-005-5	R1	[REDACTED]	[REDACTED]	07/01/2016	[REDACTED]	Compliance 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 violation.)			<p>As the result of a Compliance Audit conducted from [REDACTED], MRO determined [REDACTED], was in noncompliance with CIP-005-5 R1. The audit team discovered that [REDACTED] Protected Cyber Assets (PCAs) were allowed outbound traffic to internet based IP addresses that were owned by multiple service providers; these IP addresses were not included in the reason for granting access in the rule set as required by P1.3. [REDACTED] and the audit team determined that one access rule set included three different access reasons and that each reason should have had its own rule set.</p> <p>The noncompliance was caused by [REDACTED] failing to implement its process for permitting access out of its Electronic Access Point.</p> <p>This noncompliance started on July 1, 2016, when the standard and requirement became enforceable and ended on [REDACTED], when the noncompliant rule set was removed and replaced with three separate rule sets that each had a documented reason for granting 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 noncompliant rule set was limited to traffic that originated within the Electronic Security Perimeter (ESP) and did not allow access from the internet based IP addresses into the ESP. The noncompliance was limited to PCAs and did not impact BES Cyber Assets. Further, the impacted PCAs were logically separated from the BES Cyber Assets; [REDACTED]</p> <p>[REDACTED] No harm is known to have occurred.</p> <p>MRO reviewed [REDACTED] relevant CIP-005-5 R1 compliance history. [REDACTED] relevant compliance history includes a moderate risk violation of CIP-005-1 R2 that was mitigated on [REDACTED] 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 the current noncompliance would not constitute noncompliance under CIP-005-1.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) removed the rule set and replaced it with three separate rule sets; and 2) updated its firewall rule change process to better address destination IP addresses. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2017018151	CIP-007-6	R4	[REDACTED]	[REDACTED]	7/1/2016	[REDACTED]	Compliance 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 violation.)			<p>During a Compliance Audit conducted from [REDACTED], MRO determined that [REDACTED], was in noncompliance with CIP-007-6 R4. Specifically, a sampled BES Cyber Asset was not configured to log detected successful and failed login attempts as required by P4.1.1 and P4.1.2. [REDACTED] initially believed that the device was incapable of logging as required by the Standard and Requirement, but discovered during audit preparation that it had such capability. After discovering the sampled noncompliant device, [REDACTED] discovered the same issue with a similar non-sampled BES Cyber Asset at its [REDACTED].</p> <p>The noncompliance was caused by [REDACTED] not having a sufficient understanding of the devices' capability or a sufficient process for determining the devices' capability.</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became enforceable and ended on [REDACTED], when the two BES Cyber Assets were configured to properly log.</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] had enabled basic device logging on the BES Cyber Assets, but the basic logging did not have the granularity that is required by P4.1.1 and P4.1.2. Additionally, the noncompliance did not impact [REDACTED] ability to identify malicious code events as required by P4.1.3. Finally, [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) enabled logging on the BES Cyber Assets; 2) re-evaluated all devices that were marked as not logging due to Cyber Asset/System incapability; and 3) updated its procedure to elevate issues that require interpretation (such as device capability) to require review by the Compliance Department. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019579	CIP-002-5.1a	R1	[REDACTED]	[REDACTED]	05/26/2017	03/02/2018	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 10, 2018, [REDACTED] submitted a Self-Log stating that [REDACTED], it was in noncompliance with CIP-002-5.1a R1. Specifically, [REDACTED] states that it failed to identify each medium impact BES Cyber System as required by P1.2 [REDACTED] states that during its CIP-002-5.1a R2 review, it discovered two BES Cyber Assets that were not identified during inventorying. [REDACTED] states that the two BES Cyber Assets were not configured for logging as required by CIP-0007-6 R4. [REDACTED] states that this discrepancy occurred because [REDACTED] created its risk assessment for this substation from a non-final design diagram that did not include these two Cyber Assets.</p> <p>The noncompliance was caused by weakness in [REDACTED] processes that allowed a risk assessment to be completed before the final construction diagrams had been released.</p> <p>The noncompliance began on May 26, 2017, when the BES Cyber Assets were deployed, and ended on March 2, 2018, when the BES Cyber System documentation was 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. [REDACTED] states that the BES Cyber Assets were not accessible via External Routable Connectivity and therefore the [REDACTED] enabled on the devices exceeded the required controls. Additionally, the required Cyber Security controls were applied to the BES Cyber Assets except for logging (CIP-007-6 R4) which is a detective or forensic measure as opposed to an active defense control. 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 two BES Cyber Assets to the inventory tracking system; 2) enabled logging on the two BES Cyber Assets; and 3) revised its substation risk assessment checklist to require a second review when the final construction copies of the diagrams are released. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019582	CIP-007-6	R5	██████████)	██████████	12/14/2017	02/01/2018	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 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.</p> <p>██████ states that in the first instance of noncompliance it discovered that three medium impact BES Cyber Assets failed to have their default passwords changed as required by P5.4. The BES Cyber Assets were deployed by contractors on December 14, 2017. The cause of the noncompliance is that the substation testing and commissioning specifications that were provided to contractors did not contain steps on changing default passwords. ██████ states that the passwords were changed on January 10, 2018.</p> <p>██████ states that the second instance of noncompliance involved a generic account on an Electronic Access Control or Monitoring Systems (EACMS) device that was not identified and inventoried as required by P5.2. The EACMS was deployed on December 14, 2017. The cause of the noncompliance is that ██████ failed to follow its process test guides including account verification. ██████ states that the account was inventoried on February 1, 2018.</p> <p>The noncompliance began on December 14, 2017, when the Cyber Assets were deployed, and ended on February 1, 2018 when the account in the second instance was 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. The first instance was minimal per ██████, as the BES Cyber Assets were not accessible via External Routable Connectivity and therefore the ██████ enabled on the devices exceeded the required controls and the physical access controls for the substation exceeded the required controls ██████. ██████ states that the second instance was minimal because the generic account does not provide interactive user access and is only used by an application to read information. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, ██████:</p> <p>To mitigate the first instance of noncompliance, ██████:</p> <ol style="list-style-type: none"> 1) changed the passwords of the BES Cyber Assets; 2) updated the substation testing and commissioning specifications that are provided to contractors to include the direction to change the default passwords to the supplied passwords; and 3) updated the substation testing and commissioning specifications that are provided to contractors to include a confirmation with the substation operations representative that all compliance documentation has been completed. <p>To mitigate the second instance of noncompliance, ██████:</p> <ol style="list-style-type: none"> 1) identified and inventoried the generic account; and 2) reviewed the test guides with applicable personnel on two occasions. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019583	CIP-011-2	R1	[REDACTED]	[REDACTED]	02/01/2018	03/22/2018	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 violation.)			<p>On April 10, 2018, [REDACTED] submitted a Self-Log stating that [REDACTED], it was in noncompliance with CIP-011-2 R1. The self- log identified two instances of noncompliance.</p> <p>In the first instance, [REDACTED] states that on February 1, 2018, BES Cyber System Information (BES CSI) was incorrectly attached to an internal information technology (IT) work order. [REDACTED] reports that this made six BES Cyber Asset names and associated IP addresses available to IT employees that did not have a need for this information under its CIP-011-2 program in noncompliance with P1.2. [REDACTED] states that the BES CSI was removed from the work order on February 2, 2018. [REDACTED] reports that the noncompliance was detected by automated internal detective controls.</p> <p>In the second instance, [REDACTED] states that on March 21, 2018, BES CSI was incorrectly attached to an internal IT work order. [REDACTED] reports that this made the names of 3 Electronic Access Control or Monitoring Systems (EACMS) and 1 Physical Access Control Systems(PACS) and their associated IP addresses available to IT employees that did not have a need for this information under its CIP-011-2 program in noncompliance with P1.2. [REDACTED] states that the BES CSI was removed from the work order on March 22, 2018. [REDACTED] reports that the noncompliance was detected by automated internal detective controls.</p> <p>The cause of the noncompliance is that [REDACTED] failed to follow its process for protecting and securely handling BES CSI.</p> <p>This noncompliance was noncontiguous; the noncompliance started on February 1, 2018, when BES CSI was attached to the first work order, and ended on March 22, 2018, when BES CIS was removed from the second work order.</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], technical access control measures that meet the CIP-011-2 program had been in place at the storage location where the work orders and change requests had been saved, limiting the exposure of the BES CSI to only IT personnel who are trusted with similar information. Further, [REDACTED] states that the information included in the work order did not provide access or control of 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) removed the work orders; and 2) reviewed the handling procedures with the applicable employees and their supervisors. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020834	CIP-009-6	R1	████████████████████	████████	07/01/2016	05/09/2018	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 June 18, 2018, █████ submitted a Self-Log stating that █████, it was in noncompliance with CIP-009-6 R1. Specifically, █████ states that on May 8, 2018 it discovered it had insufficient controls in place to verify the successful completion of a subset of backup processes and to address any backup failures of that subset as required by P1.4.</p> <p>The cause of the noncompliance is that █████ did not have sufficient processes during the CIP v5 transition to confirm that controls for verifying all necessary backups had been implemented.</p> <p>The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on May 9, 2018, when █████ implemented a short term solution to review daily reports for successful and failed backups.</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 █████, there was an informal process in place that verified successful backups following maintenance activities, which occurred in 16 of the 23 months since the requirement became enforceable. Additionally, █████ states that the subset of data did not include operating systems or firmware. █████ reports that if an incident occurred, the lack of a backup on the subset of the data would not prevent a restoration, but delay a restoration. Finally, █████ states that a historical review of the backups demonstrate a high success rate and the backup failures were usually resolved during the next backup. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, █████:</p> <ol style="list-style-type: none"> 1) implemented a short-term solution to review daily reports for successful and failed backups; 2) implemented a log of backup failures and how they were addressed; 3) implemented a new procedure to produce a daily report for system administrators to verify successful backup completion and address any failures; and 4) provided training to applicable system administrators on the new 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
MRO2018020842	CIP-007-6	R5	[REDACTED]	[REDACTED]	07/01/2016	09/07/2018	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 October 9, 2018, [REDACTED] submitted a Self-Log stating that [REDACTED], it was in noncompliance with CIP-007-6 R5. The Self-Log identified two instances of noncompliance with P5.2.</p> <p>[REDACTED] states that the first instance of noncompliance was discovered during an internal compliance review. [REDACTED] reports that it discovered a BES Cyber Asset had an enabled default shared application account that was not listed on the account inventory. [REDACTED] states that the account was inventoried on June 21, 2018.</p> <p>[REDACTED] conducted an extent of conditions analysis after the discovery of the first instance. [REDACTED] reports that it discovered an Electronic Access Control or Monitoring Systems (EACMS) device that had two enabled default shared application accounts that were not listed on the account inventory. [REDACTED] states that the accounts were inventoried on August 30, 2018 and September 7, 2018.</p> <p>The cause of the noncompliance was that [REDACTED] process for identifying default accounts was insufficient and did not list all sources that needed to be reviewed.</p> <p>The noncompliance began on July 1, 2016, when the Standard and Requirement went into effect and ended on September 7, 2018 when all the accounts were 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. Per [REDACTED], all individuals with access to the accounts were authorized as required by P5.3, had current personnel risk assessments, and CIP training. Further, [REDACTED] states that one of the accounts on the EACMS was limited to reporting information only. Finally, [REDACTED] reports that the account on the BES Cyber Asset was a “nested” account, meaning that a user must login with a separate individual account prior to logging into the default shared application account; additionally, the account was limited to modifying displays. 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 accounts to the account inventory; and 2) modified its internal control review process to include steps to review additional sources to verify the identification of enabled default shared application accounts. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020843	CIP-004-6	R5	████████████████████	████████	05/08/2018	06/06/2018	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 June 18, 2018, ██████ submitted a Self-Log stating that ██████, it was in noncompliance with CIP-004-6 R5. The Self-Log identified two instances of noncompliance.</p> <p>██████ reports that it has multiple internal controls in place to protect against unauthorized access by the employee of a contractor. ██████ states that access for the employee of a contractor is automatically revoked after 45 days unless the contractor requests an extension and notes the need. Additionally, ██████ states that it requires contractors to verify the employment and continuing need of employees with access on a weekly basis.</p> <p>In the first instance of noncompliance, ██████ states that a project manager determined on May 6, 2018, that two individuals employed by a contractor no longer required unescorted physical access. The project manager failed to notify the compliance personnel of the determination at that time. ██████ reports that on May 8, 2018, in response to the weekly email, the contractor submitted the revocation request to ██████, but sent the email to an incorrect email address, the contractor forwarded the email to the correct email address on May 10, 2018; physical access was revoked on May 10, 2018. The cause of the noncompliance is that ██████ failed to follow its process for access revocation. The noncompliance began on May 8, 2018, after access was not revoked by the end of the next calendar day, and ended on May 10, 2018 when the access was revoked.</p> <p>In the second instance of noncompliance, ██████ states that a contractor's employee who had access to BES Cyber System Information (BES CSI) was terminated on June 1, 2018 and the access was not revoked by the end of the next calendar day as required by P5.3. ██████ states that in this instance, the contractor terminated the employee on June 1, 2018 and failed to inform ██████ of the termination. ██████ reports that the contractor then inaccurately stated that the individual was still employed in the following weekly verification. ██████ reports that on June 6, 2018, the individual's access was automatically revoked pursuant to the 45-day internal control after the contractor did not request an extension. The cause of the noncompliance is that the contractor failed to follow ██████ process for access revocation. The noncompliance began on June 3, 2018, after access was not revoked by the end of the next calendar day, and ended on June 6, 2018 when the access was revoked.</p> <p>The noncompliance was noncontiguous; the noncompliance began on May 8, 2018, when the access in the first instance was not revoked, and ended on June 6, 2018 when the access in the second instance 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. The first instance was minimal as ██████ states the revocation was due to a change in need as opposed to the termination of the individuals' employment. The second instance was minimal per ██████, as the employee's access was limited to BES CSI, additionally, the employee was a former employee of ██████ who still had current CIP training and a personnel risk assessment; the employee was in good standing with ██████ and was re-hired in August 2018. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, ██████:</p> <ol style="list-style-type: none"> 1) revoked the individuals' access; 2) reviewed the access revocation requirements, procedures, and access revocations tip document with the project manager in the first instance, responsible supervisor, and associated manager; and 3) reviewed the access revocation requirements, procedures, and access revocations tip document with the contractor in the second instance. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020162	CIP-007-6	R5	[REDACTED]	[REDACTED]	7/1/2016	03/14/2018	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 violation.)			<p>On April 10, 2018, [REDACTED] submitted a Self-Log stating that, [REDACTED], it was in noncompliance with CIP-007-6 R5. The noncompliance impacted two Electronic Access Control or Monitoring Systems (EACMS) devices that operate as Intermediate Systems. The two devices failed to have a method to enforce authentication of interactive user access for connections via the devices' serial port.</p> <p>The cause of the noncompliance was that [REDACTED] process for deploying methods to enforce authentication lacked sufficient detail pertaining to serial port management.</p> <p>The noncompliance began on July 1, 2016 when the standard became enforceable and ended on March 14, 2018 when authentication was properly configured.</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 limited to devices that were physically connected to the devices via the serial connection; this reduced the capability of compromise of the unauthenticated interactive user access. [REDACTED]</p> <p>[REDACTED] inally, the impacted EACMS devices and the devices that they were serially connected to are located in a functioning Physical Security Perimeter (PSP). No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) configured the devices with the proper authentication; 2) created a device management document that identifies the authentication configuration of serial ports as part of the onboarding of like devices; and 3) trained applicable staff on the device management document. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020170	CIP-010-2	R1	[REDACTED]	[REDACTED]	07/01/2016	05/03/2018	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 10, 2018, [REDACTED] submitted a Self-Log stating that, [REDACTED], it was in noncompliance with CIP-010-2 R1. The Self- Log contained two instances of noncompliance.</p> <p>In the first instance of noncompliance, [REDACTED] identified multiple Physical Access Control Systems (PACS) devices (hypervisors) that did not have completed baselines. The reason that the devices did not have completed baselines is because they were not identified as PACS devices during deployment. Additionally, [REDACTED] reports that two of the PACS devices did not have security event monitoring as required by CIP-007-6 P4.1. The cause of the noncompliance was that [REDACTED] process for identifying PACS devices lacked sufficient detail. The noncompliance began on November 29, 2017 when the PACS devices were put into service and ended on March 28, 2018 when the baselines were completed and all required security controls were put in place on the PACS devices.</p> <p>In the second instance of noncompliance, [REDACTED] identified BES Cyber Assets (servers) that did not have complete CIP-010-2 R1 baseline information because the baseline failed to include a module. Additionally, [REDACTED] states that it did not disable all unnecessary ports and services (CIP-007-6 P1.1) or identify all known and enabled accounts associated with the module (CIP-007-6 P5.2). The cause of the noncompliance is that [REDACTED] server management documentation lacked sufficient detail. The noncompliance began on July 1, 2016 when the standard became enforceable and ended on May 3, 2018 when the module was disabled.</p> <p>This noncompliance started on July 1, 2016, when the standard became enforceable and ended on May 3, 2018, when the module in the second instance of noncompliance 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. The first instance was minimal because per [REDACTED], the two devices that did not have sufficient logging protections were receiving some level of protection through an associated [REDACTED] and [REDACTED]. Further, the devices were located within a functioning Physical Security Perimeter (PSP) and were located within a segmented network. The second instance was minimal because per [REDACTED], the module was not configured for use limiting the capability of the module from impacting the host server; the module was not configured with an IP address or capable of ports being bound to the interface. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <p>To mitigate the first instance of noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) applied the required security controls to the devices; 2) developed baselines for the devices; 3) updated the device management documentation that would be applicable to this type of device; 4) provided training on the updated device management documentation. <p>To mitigate the second instance of noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) disabled the modules; and 2) updated its server device management document to address the disabling of these specific modules during onboarding. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020275	CIP-008-5	R3	[REDACTED]	[REDACTED]	06/20/2017	11/17/2017	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 violation.)			<p>On June 5, 2018, [REDACTED] submitted a Self-Report stating that [REDACTED], it was in noncompliance with CIP-008-5 [REDACTED]</p> <p>[REDACTED] states that it failed to update its Cyber Security Incident response plan within 90 days of a test. The test was completed on March 21, 2017 and [REDACTED] states that it documented lessons learned (P3.1.1) and notified each person or group with a defined role (P3.1.3) within 90 days, but it failed to update the Cyber Security Incident response plan within 90 days as required by P3.1.2.</p> <p>The cause of the noncompliance is that [REDACTED] documented process lacked sufficient detail and did not track assignments and due dates.</p> <p>The noncompliance began on June 20, 2017, 90 days after the test, and ended on November 17, 2017, when the Cyber Security Incident response plan was 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. [REDACTED] produced a document that demonstrated the test report documented the lessons learned and that document was distributed, therefore the noncompliance was limited to a failure to timely update the Cyber Security Incident response plan. [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) updated its Cyber Security Incident response plan; 2) augmented its Cyber Security Incident response plan to include the tracking of assignments, due dates, and the monitoring of CIP-008-5 requirements; and 3) held training sessions on the changes. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020276	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/1/2016	8/22/2018	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 violation.)			<p>On June 5, 2018, [REDACTED] submitted a Self-Report stating that [REDACTED], it was in noncompliance with CIP-010-2 R1. [REDACTED]</p> <p>[REDACTED] states that it did not conduct the proper authorizations (P1.2) or assessments on impacted security controls (P1.4) when it permitted unmanaged automatic updates for its anti-malware software on multiple BES Cyber Assets.</p> <p>The cause of the noncompliance is that [REDACTED] documented process lacked sufficient detail and did not contain sufficient instructions for managing the anti-malware’s agent/engines updates.</p> <p>The noncompliance began on July 1, 2016 when the Standard and Requirement and ended on August 22, 2018 when [REDACTED] modified how future updates would be applied and updated its documented process.</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] demonstrated that it was adding the changes to the baselines within 30 days of the updates taking place which demonstrates an awareness that the updates were taking place. Additionally, the noncompliance was limited to automatic updates to the anti-malware application and not for the signatures or patterns; it is MRO’s understanding that updates to an application has a reduced potential for impacting the security controls in CIP-005-5 and CIP-007-6 as compared to updates to the signatures or patterns. Further, [REDACTED] reports that it has [REDACTED], and other network protections in place that reduced the risk of unauthorized access. [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) modified automatic updates from the anti-malware vendor to target a console which is managed and maintained by the applicable SME; and 2) developed instructions for testing and configuring the updates and deployments from the anti-malware agent/engine. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020791	CIP-004-6	R4	[REDACTED]	[REDACTED]	07/01/2016	06/22/2018	Self-Report	06/30/2019
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 violation.)			<p>On November 8, 2018, [REDACTED], submitted a Self-Report to MRO stating that, [REDACTED], it was in noncompliance with CIP-004-6 R4. [REDACTED]. The Self-Report identified two instances of noncompliance. The noncompliance impacted [REDACTED].</p> <p>In the first instance of noncompliance, [REDACTED] states that for BES Cyber System Information (BES CSI) it did not verify at least once every 15 calendar months that all accounts, user groups, or user role categories, and associated privileges were correct and necessary as required by P4.3. [REDACTED] states that it deployed a new SharePoint environment, this new SharePoint environment was designed as a place for two groups that have their own BES CSI access to share documents. [REDACTED] reports that it failed to identify this SharePoint environment as a BES CSI location as required by CIP-011-2 R1. The cause of the noncompliance was that [REDACTED] did not identify the SharePoint environment as a BES CSI location, which resulted in [REDACTED] not tracking the 15 month calendar review. The noncompliance began on July 1, 2016, when the standard became enforceable and ended on May 15, 2018, when all access to the new SharePoint environment was revoked.</p> <p>In the second instance of noncompliance, [REDACTED] reports that after the access was revoked, during a live training session, the trainer learned that many of the field technicians in the training session were not part of the new access control group (created after the access was revoked in instance one). [REDACTED] reports that the trainer added all the impacted field technicians to the new access control group so that the training could be completed. A subsequent review determined that the trainer did not follow the established process to provide access and that not all of the impacted field technicians had a documented business need to access the BES CSI in the new access control group. The cause of the noncompliance was that [REDACTED] failed to follow its process to grant access to BES CSI storage locations based on need. The noncompliance began on June 1, 2018, when the trainer granted access, and ended on June 22, 2018, when the access was revoked for individuals that did not have a business need.</p> <p>The noncompliance was noncontiguous; the noncompliance began on July 1, 2016, when the standard became enforceable and ended on June 22, 2018 when the access in the second instance of noncompliance 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. The first instance of noncompliance was minimal because per [REDACTED], [REDACTED] had a business need for the access; the remaining 21 individuals were no longer employed by [REDACTED] and [REDACTED] states that it had revoked their Interactive Remote Access at the time of the termination as required by P5.1. Additionally, per [REDACTED], [REDACTED] had authorized access to a separate BES CSI storage location. Further, [REDACTED] states that the new SharePoint environment required that access requests be submitted and approved, but that [REDACTED] did not maintain those records because it was not a designated BES CSI storage location. The second instance of noncompliance was minimal because per [REDACTED], [REDACTED] had a business need for the access; the remaining [REDACTED] individuals had authorized access to a separate BES CSI storage location. Finally, [REDACTED] states that the information for both instances was limited to information about medium impact BES Cyber Systems. No harm is known to have occurred.</p> <p>[REDACTED] has implemented a new secondary control (procedure) regarding access control around the affected BES CSI storage location to reduce the risk of reoccurrence during mitigation.</p> <p>MRO reviewed [REDACTED] CIP-004-6 R4 compliance history. MRO determined that [REDACTED] relevant compliance history does not serve as a basis to impose a penalty.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) identified the SharePoint environment in instance one as a BES CSI storage location; 2) revoked the access for all individuals without a business need in instance two; and 3) created a standard operating procedure to detail the access control around this affected BES CSI storage location. <p>To mitigate this noncompliance, [REDACTED] will complete the following mitigation activities by June 30, 2019:</p> <ol style="list-style-type: none"> 1) augment the substation CIP team annual information protection assessment process to improve the identification of BES CSI; and 2) update an email distribution list for all BES CSI storage site owners and inform them of the improved process. <p>The length of time needed for mitigation is due to the need to augment a 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
MRO2019020940	CIP-003-6	R1	[REDACTED]	[REDACTED]	06/21/2018	12/10/2018	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 January 10, 2019, [REDACTED], submitted a Self-Log to MRO stating that, [REDACTED], it was in noncompliance with CIP- 003-6 R1. [REDACTED] The noncompliance impacted [REDACTED]</p> <p>[REDACTED] stated that it failed to obtain CIP Senior Manager approval of its cyber security policies at least every 15 months. [REDACTED] stated that the last approval was completed on March 20, 2017. [REDACTED] reports that a new employee was given ownership responsibilities for tracking this review and this employee was unfamiliar with the process. [REDACTED] states that it discovered the noncompliance during a review of time-based due dates; the goal of the review was to verify compliance and enhance internal controls.</p> <p>The cause of the noncompliance was that [REDACTED] failed to follow its process for approval of its cyber security policies.</p> <p>This noncompliance started on June 21, 2018, when [REDACTED] failed to obtain CIP Senior Manager approval of its cyber security policies at least every 15 months, and ended on December 10, 2018, when the CIP Senior Manager reviewed and approved the cyber security 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] states that there were no changes to the existing cyber security policies as a result of the review. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) had its CIP Senior Manager review and approve the cyber security policies; and 2) created a reoccurring task in its compliance tool to track the completion of the approval 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
MRO2019020941	CIP-004-6	R2	[REDACTED]	[REDACTED]	05/16/2018	11/13/2018	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 January 10, 2019, [REDACTED], submitted a Self-Log to MRO stating that, [REDACTED], it was in noncompliance with CIP- 004-6 R4. [REDACTED]. The noncompliance occurred in the [REDACTED].</p> <p>[REDACTED] states that on November 13, 2018, while researching a separate process issue, it discovered that an employee with access to Electronic Access Control or Monitoring Systems (EACMS) devices was not current on CIP Training as required by CIP- 004-6 P2.3. [REDACTED] reports that the initial access request ticket was created on November 10, 2017, [REDACTED] states that at this time it confirmed the employee was up to date on a Personnel Risk Assessment (PRA) and CIP training. However, [REDACTED] states that the initial access request ticket was not promptly completed as the employee did not respond to an information request until May 16, 2018; the employee's CIP training had lapsed in that six months and there was no re-verification of training on the date that access was granted. The annual CIP training requests are created at year-end based on current entitlements. [REDACTED] reports that since the employee did not have a CIP entitlement at the end of 2017, the employee was not included in the 2018 CIP training.</p> <p>The cause of the noncompliance was that [REDACTED] process did not have sufficient controls to verify that the individual had valid training at the time that access was granted.</p> <p>The noncompliance began on May 16, 2018, when [REDACTED] granted access to an employee who did not have current CIP training and ended on November 13, 2018, when the employee received CIP training.</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 a single employee who was in good standing, had a criminal background check, had a current PRA on file, and had received CIP training in the previous year. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) had the individual immediately complete CIP training; 2) developed a new process to address delays in the fulfillment of an access request ticket. The system generates a duration breach notification if the fulfillment does not occur within 14 days. The new process requires all duration breach notifications to be followed up by administrative staff who will facilitate processing to prevent gaps in fulfilling an access request ticket; and 3) validated against the 2019 CIP training due day to confirm that no individual with CIP access missed training due to a new access request. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019020942	CIP-004-6	R5	[REDACTED]	[REDACTED]	08/18/2018	12/06/2018	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 January 10, 2019, [REDACTED], submitted a Self-Log to MRO stating that, [REDACTED], it was in noncompliance with CIP- 004-6 R5. [REDACTED] The Self-Log contained four instances of noncompliance with P5.1. The noncompliance [REDACTED]</p> <p>In the first instance, an intern resigned on August 17, 2018. [REDACTED] states that removal of logical access to a system was delayed due to technical difficulties in creating the revocation form and the supervisor being unaware of the 24 hour requirement contained in P5.1. The access was revoked on August 21, 2018. [REDACTED] states that it discovered the noncompliance through the execution of an internal control, the monthly CIP termination spot check. The cause of the noncompliance was that the supervisor was new to the role and failed to follow [REDACTED] process for removal of access permissions.</p> <p>In the second instance, a contract employee with physical access to a [REDACTED] substation, resigned late in the day on Friday, October 5, 2018 and surrendered their badge. [REDACTED] states that the supervisor was unaware of the 24 hour requirement contained in P5.1 and did not complete the revocation form until Monday October 8, 2018 (access was promptly revoked later that day). The cause of the noncompliance was that the supervisor was new to the role and failed to follow [REDACTED] process for removal of access permissions.</p> <p>In the third instance, a contract employee with physical access to a [REDACTED] substation, needed to have a break in service for administrative reasons. The employee resigned on Friday November 23, 2018 and was re-hired on Monday, November 26, 2018. [REDACTED] states that the supervisor could not submit the revocation form due to technical difficulties on November 23, 2018 and did not attempt to submit the form until November 29, 2018 (access was promptly revoked later that day). The cause of the noncompliance was that the revocation system was unavailable on the day that it needed to be submitted.</p> <p>In the fourth instance, a contract employee with physical access to a [REDACTED] data center, resigned on November 3, 2018 and surrendered their security badge. [REDACTED] states that the supervisor was not aware of the requirement to submit a revocation form and did not submit the form until December 6, 2018 (access was promptly revoked later that day). The cause of the noncompliance was that the supervisor was new to the role and failed to follow [REDACTED] process for removal of access permissions.</p> <p>This noncompliance was noncontiguous; the noncompliance started on August 18, 2018, 24 hours after the termination in instance one, and ended on December 6, 2018, when access in instance four 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. The first instance was minimal because per [REDACTED], the intern was current on CIP training, had a valid Personnel Risk Assessment (PRA), the intern's badge and computer were secured in the supervisor's office during the noncompliance, and it confirmed that the intern did not access the network after the resignation. The second instance was minimal because per [REDACTED], the employee was current on CIP training, had a valid PRA, the employee's badge was secured in the supervisor's office during the noncompliance, it confirmed that the employee did not access the substation after the resignation, and the substation that the employee had access to was surrounded by a seven-foot barbed wire fence and a locked gate, and the employee did not have access to the gate's key. The third instance was minimal because per [REDACTED], the employee was current on CIP training, had a valid PRA, it confirmed that the employee did not use the badge to gain access during the break in service, and the break in service was for administrative reasons. The fourth instance was minimal because per [REDACTED], the employee was current on CIP training, the employee's badge was secured in the supervisor's office during the noncompliance, had a valid PRA, the employee did not have electronic access to any BES Cyber Assets, and the resignation was not a termination based on cause. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) revoked the access for all individuals; 2) the supervisor's manager in the first instance discussed and reviewed CIP-004-6 R5 compliance requirements and the revocation process, and the 24-hour access removal procedure during a weekly regional lead meeting; 3) the supervisor's manager in the first instance requested a confirmation email that a revocation form had been timely submitted for all future terminations; 4) in response to the second instance, a senior operations manager sent a reminder to all leaders about the required steps to be taken and the required timeframe to revoke access to medium impact substations upon an employee termination; 5) in response to the third instance, it updated its policies and procedures to allow a supervisor to contact security personnel directly when the revocation system is unavailable; 6) sent a reminder to all business units regarding the required steps to remove access and what to do if the system is unavailable (this reminder was sent on two separate occasions); and 7) sent a counselling letter to the supervisors in instance three and four. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019020943	CIP-007-6	R1	[REDACTED]	[REDACTED]	07/01/2016	12/05/2018	Self-Log	01/15/2020
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 10, 2019, [REDACTED], submitted a Self-Log to MRO stating that, [REDACTED], it was in noncompliance with CIP- 007-6 R1. [REDACTED] The Self-Log contained four instances of noncompliance with P1.1. The noncompliance [REDACTED].</p> <p>The noncompliance was discovered through conducting a Network Mapping (NMAP) scan in the substation environment, which is an enhancement over the required vulnerability assessment. The NMAP scan returned Cyber Asset information indicating that ports were open on multiple devices where the baseline documentation indicated that the ports should have been closed.</p> <p>In the first instance, there was an Electronic Access Control or Monitoring Systems (EACMS) at a [REDACTED] substation that had a necessary port whose need had not been documented and the port was not included in the baseline. The noncompliance for this instance began on July 1, 2016 and ended when the baseline documentation was updated on November 20, 2018.</p> <p>In the second instance, there was a Protected Cyber Assets (PCA) at a [REDACTED] substation that had a necessary port whose need had not been documented and the port was not included in the baseline. The noncompliance for this instance began on October 1, 2017, and ended when the baseline documentation was updated on October 25, 2018.</p> <p>In the third instance, there was a PCA at a [REDACTED] substation that had an enabled but unnecessary port that was not included in the baseline. The noncompliance for this instance began on March 1, 2018, and ended when the unneeded port was blocked by an additional firewall on December 4, 2018.</p> <p>In the fourth instance, there were two BES Cyber Assets at a [REDACTED] substation that had two enabled but unnecessary ports that were not included in the baseline. The noncompliance for this instance began on March 1, 2018, and ended when the unneeded ports were disabled on December 5, 2018.</p> <p>The cause of the noncompliance is that [REDACTED] did not follow the baseline instruction process when deploying the devices which allowed for unneeded ports to remain open and [REDACTED] failed to follow its process to document the need for the necessary ports in the baseline documentation.</p> <p>The noncompliance started on July 1, 2016, when the Standard and Requirement became enforceable and, and ended on December 5, 2018, when the ports in instance four were 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. [REDACTED] reports that the impacted Cyber Assets were current in terms of security patches and the passwords met the complexity requirements. Further, the noncompliance instance one and two involved ports that were necessary for operations which reduced the potential risk. Finally, per [REDACTED], the ports in the third and fourth instance, which should not have been enabled, were blocked from being accessed via Interactive Remote Access. [REDACTED] states that to access the ports in those instances, an adversary would need to gain access to the Physical Security Perimeter (PSP) and then log in with a valid user name and password. No harm is known to have occurred.</p> <p>While mitigation is ongoing, [REDACTED] is going to reduce the risk of recurrence by continuing to perform the NMAP scan that detected the noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) documented the necessary ports and disabled the unnecessary ports; and 2) committed to performing and improving the semi-monthly port scanning process. <p>To mitigate this noncompliance, [REDACTED] will complete the following mitigation activities by January 15, 2020:</p> <ol style="list-style-type: none"> 1) revise the baseline instructions to add additional detail regarding setting up the ports and baseline details; and 2) conduct training for the field technicians on the updated baseline instructions. <p>The length of the mitigating activities is due to the creation of a new “device life cycle process” that needs to be scoped and then fully developed prior to completing the remaining 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
MRO2019020944	CIP-007-6	R2	[REDACTED]	[REDACTED]	11/16/2018	11/18/2018	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 violation.)			<p>On January 10, 2019, [REDACTED] submitted a Self-Log to MRO stating that, [REDACTED], it was in noncompliance with CIP- 007-6 R2. [REDACTED] The noncompliance [REDACTED]</p> <p>During a security patch coordination meeting, [REDACTED] discovered that security patches released from a patch source had not been evaluated at least once every 35 days. [REDACTED] states that the patch source released two patches near each other and that applicable staff had focused on evaluating the later patch first.</p> <p>The noncompliance was caused by [REDACTED] failing to follow its process regarding patch evaluation.</p> <p>The noncompliance began on November 16, 2018, 35 days since the last patch source evaluation, and ended on November 18, 2018, when the patch was evaluated.</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 duration of the noncompliance was brief. Additionally, [REDACTED] reports that the patch was promptly applied. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) evaluated and applied the security patch; and 2) reinforced the process for completing the patch evaluation during the security patch coordination meeting. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019020950	CIP-010-2	R4	[REDACTED]	[REDACTED]	08/05/2017	08/06/2017	Self-Log	06/30/2019 Expected
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 10, 2019, [REDACTED], submitted a Self-Log to MRO stating that, [REDACTED], it was in noncompliance with CIP- 010-2 R4. [REDACTED] The noncompliance [REDACTED].</p> <p>Specifically, [REDACTED] states that a substation relay field technician was dispatched to a substation to investigate a Programmable Logic Controller (PLC) failure. The relay technician could not use the authorized Transient Cyber Asset (TCA) because the PLC software was not installed on the TCA. [REDACTED] states that there was a desktop computer in the substation with the required software installed, and the technician connected that computer to the PLC. [REDACTED] reports that a few days later, the technician contacted a CIP Compliance resource and alerted them of the issue.</p> <p>The cause of the noncompliance is that [REDACTED] did not follow its process to identify all software that needed to be installed on the TCA devices.</p> <p>The noncompliance began on August 5, 2017, when the technician connected the desktop computer to the system, and ended when the technician disconnected the desktop from the system.</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 the noncompliance is limited to one substation that did not have External Routable Connectivity (ERC) or Interactive Remote Access (IRA) to that substation. Additionally, per [REDACTED] the desktop computer that was improperly utilized, was located within a secured area, limiting an adversary's physical access; further the desktop computer was not connected to the Internet, limiting the risk of software vulnerabilities and the introduction of malicious code. No harm is known to have occurred.</p> <p>[REDACTED] has taken steps to ensure that the necessary PLC software is installed on an authorized TCA device; the mitigation that still needs to occur is limited to receiving information from the vendor regarding how this software can be installed on other potential TCA devices with different capabilities and operating systems.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) disconnected the desktop computer; and 2) installed the PLC software on an authorized TCA device. <p>To mitigate this noncompliance, [REDACTED] will complete the following mitigation activities by June 30, 2019:</p> <ol style="list-style-type: none"> 1) receive a whitepaper from the PLC vendor on how to install the PLC software on other potential TCA devices with different capabilities and operating systems to help maintain full compliance. <p>The length of time to complete mitigation is related to activities that are being completed by a third party.</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
RFC2018020503	CIP-009-6	R2	[REDACTED]	[REDACTED]	8/11/2018	8/17/2018	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 October 2, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-009-6 R2. The entity utilizes an [REDACTED] for multi-factor authentication. The [REDACTED] is classified as an Electronic Access Control or Monitoring System associated with High Impact Bulk Electric System (BES) Cyber Systems. A test of a representative sample of information used to recover [REDACTED] was performed on May 11, 2017, and, therefore, the next test of such information should have been completed on or before August 11, 2018, in accordance with CIP-009-6 R2.2. The test was not completed until August 17, 2018, which was six days late. The noncompliance was identified during a recurring compliance meeting on August 11, 2018.</p> <p>The root cause of this noncompliance was a gap in the process for monitoring, tracking, and communicating due dates for recovery plan testing. The entity relied on [REDACTED] subject matter experts (SMEs) [REDACTED] to communicate testing dates and deadlines during recurring compliance meetings. In this case, [REDACTED] SMEs who were responsible [REDACTED] were on vacation at the same time and missed four consecutive compliance meetings preceding the instant noncompliance. The existing process did not account for such an occurrence, as no one else was aware of the approaching deadline.</p> <p>This noncompliance implicates the management practice of workforce management, which includes the need to account for and manage events such as employee absences, position changes, and terminations. This can be achieved by implementing controls to ensure adequate oversight of employees' functions and responsibilities. Further, an entity can utilize escalation steps relating to tasks that are essential to the reliable operation of the BES.</p> <p>This noncompliance started on August 11, 2018, when the entity failed to test a representative sample of information used to recover [REDACTED] within a 15-month interval and ended on August 17, 2018, when the entity completed the test.</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. Outdated and untested recovery plans and information may be unusable or incompatible with existing configurations, which could lead to an inability to recover from various hazards affecting BES Cyber Systems in a timely manner. The risk was mitigated by the following facts. First, even though the entity did not test a representative sample of information used to recover [REDACTED] within a 15-month interval, it had conducted a tabletop exercise of the [REDACTED] recovery procedure on February 9, 2018. The tabletop exercise showed that the asset was recoverable. Second, there were no significant changes (e.g., SME, technology, etc.) since the last test of a representative sample of information on May 11, 2017, thus further reducing the risk of harm. 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. The prior Settlement Agreement related to serious and systemic issues, including a complete lack of procedures, and the prior noncompliance resulted from a different cause. Further, the current noncompliance relates to a limited issue that the entity quickly identified and resolved.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) tested the disaster recovery procedure for the [REDACTED]; 2) set up a Work Management process, which will provide notifications when something is due or updated; and 3) implemented an embedded test within the recurring compliance meeting targeting SME attendance and escalation. <p>ReliabilityFirst 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
RFC2018020607	CIP-004-6	R5			9/26/2018	10/1/2018	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 19, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. On October 1, 2018, [REDACTED] analyst discovered, during the daily review of [REDACTED] to-do list, that an entity employee's access to one Bulk Electric System (BES) Cyber Security Information (BCSI) electronic storage location was not timely revoked when that employee no longer required access. The [REDACTED] to-do list is a list of items consisting of all future-dated electronic access removals, and is manually reviewed each business day by an [REDACTED] analyst.</p> <p>In this case, the employee's access to the BCSI electronic storage location had been requested to be retained for a transition period while the employee was transferring from one role to another. However, the access was not timely revoked upon the employee's transition. After identifying the late access removal issue, the [REDACTED] analyst immediately removed access for the employee. Upon investigation, the [REDACTED] analyst discovered both that the removal date was inadvertently documented in the to-do list as September 28 instead of the required date of September 26; and that access was not properly removed as of September 28. The entity did not remove the access until October 1, 2018.</p> <p>The root cause of this noncompliance was the lack of a documented process regarding the use of the [REDACTED] to-do list. The date entered into the to-do list was incorrect. Additionally the [REDACTED] analyst failed to document the daily task to review the pending access removal, meaning the [REDACTED] analyst had to rely on memory to complete the task. The [REDACTED] analyst failed to review the to-do list for any pending access removals.</p> <p>The noncompliance involves the management practices of workforce management and verification management. Workforce management is involved because the [REDACTED] analyst was not properly trained to document the daily task nor were they properly trained to review the necessary process to-do list. Verification is involved because the [REDACTED] analyst failed to confirm that a necessary access change was made in accordance with CIP-004-6 R5.</p> <p>This noncompliance started on September 26, 2018, when the entity failed to comply with CIP-004-6 R5 by not timely revoking a transitioning employee's access and ended on October 1, 2018, when the entity removed the employee'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 allowing an individual to access BES Cyber Systems is that an individual who is no longer authorized to have access could act to harm the reliable operation of the BPS. This risk was mitigated in this case by the following factors. First, the employee was simply changing roles and remained a trusted employee. Second, the employee was current on CIP training as well as an identity and criminal history background check. Third, the duration of the noncompliance was short, only lasting five days. Fourth, the entity confirmed that the employee had not accessed, or even attempted to access, the electronic storage location during the time his access should have been removed. 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 current noncompliance resulted from different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) implemented an automated email notification workflow in [REDACTED] so that all members of the [REDACTED] team are notified on a daily basis via email which items on the to-do list are due that day; 2) emailed a communication reminder to the team reinforcing the responsibility of reviewing and addressing the [REDACTED] to-do list each business day; and 3) documented the processes of: daily checks of the [REDACTED] to-do list, verifying as part of daily QA activities that access removals on the [REDACTED] to-do list were correctly processed, as well as a process for additional verification of to-do list entries to ensure dates and information are entered correctly. <p>ReliabilityFirst 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
RFC2018020251	CIP-007-6	R3	[REDACTED]	[REDACTED]	2/5/2018	5/11/2018	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 August 16, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R3. The entity failed to protect one [REDACTED] server at the Primary Operations Center and an identical [REDACTED] server at the Alternative Operations Center from potential malicious code because the entity did not fully install all components of the antivirus (AV) application software. The two [REDACTED] servers were built and configured using an automated build process that includes the installation of AV agent software. The AV agent software is pre-configured to communicate between the AV console and the AV agent in order to add the servers to the console and initiate the installation of AV definitions.</p> <p>In this incident, the AV console had been upgraded, but the AV agent installed was not compatible with the newer version of the AV console. [REDACTED]</p> <p>[REDACTED]</p> <p>The root cause of this noncompliance was the lack of an effective review process to determine whether the AV agent version installed was compatible. In addition, the entity checklist process did not include a verification step to confirm the servers were successfully communicating with the AV console once they were built.</p> <p>The noncompliance involves the management practices of asset and configuration management and verification management. Asset and configuration management is involved because the entity's change control process did not prevent this instance of noncompliance. Verification management is involved because the entity's internal process did not include a verification step to confirm that the servers in question were communicating with the AV console.</p> <p>This noncompliance started on February 5, 2018, when the entity did not fully install all components of the AV application software and thus did not fully protect the [REDACTED] servers and ended on May 11, 2018, when the entity updated the AV agent software and the AV definitions were successfully installed.</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 risk posed by failing to prevent, detect, or mitigate the threat of malicious code on Bulk Electric System (BES) Cyber Systems has the potential to affect the reliable operation of the BPS by permitting a bad actor to use or compromise BES Cyber Assets. This risk was mitigated in this case by the following factors. First, the entity has a strong defense-in-depth system in place. [REDACTED] [REDACTED] ([REDACTED] is deployed to all CIP [REDACTED] workstations and servers where technically feasible which would alert to any new software (or malware) installed or any configuration changes to these systems. [REDACTED] also has access to network devices and pulls the configuration at least once every 35 days for comparison which would alert to configuration changes. [REDACTED] [REDACTED] continued to collect security log files during this period and no security events were found.) [REDACTED]</p> <p>[REDACTED]. This includes a virus scan, as well as confirmation of origination via either confirming digital signatures or verifying the integrity of the software via a hashing algorithm. Lastly, ReliabilityFirst notes that the entity performed full system antivirus scans on the impacted systems and detected no malicious code. 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 root causes between the prior noncompliance and the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) implemented a daily health check to validate that antivirus definitions in the CIP environment are being updated in compliance with CIP regulations. On a daily basis, a detailed report generated by [REDACTED] [REDACTED] is reviewed showing the version date of the antivirus definitions on all CIP [REDACTED] Impact [REDACTED] assets. This report lists all individual nodes and their current status and any associated issues. In addition, an executive summary dashboard including the status of all CIP [REDACTED] Impact asset [REDACTED] antivirus protection is also sent to Cybersecurity and Infrastructure Senior Management; 2) updated the Cybersecurity Change Request Task List for new CIP Cyber Assets to include a verification by Cybersecurity to ensure all new assets, installed with antivirus software, are actively communicating with the antivirus console and receiving antivirus definitions; 3) performed independent reviews and verified that all applicable servers and workstations in the entity's system of record are in the antivirus console; 4) updated with the compatible version of the antivirus agent software the entity's application packages; 5) updated the server build checklist to include a verification section to ensure applications installed by the automated build process are communicating and compatible 6) developed and implemented a process to review and update application packages installed as part of the automated server build process on a regular basis to ensure software compatibility between agent versions and console versions; 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020251	CIP-007-6	R3			2/5/2018	5/11/2018	Self-Report	Completed
			<p>7) engaged a third party vendor to perform an active vulnerability assessment; 8) completed the field work for the active vulnerability assessment; and 9) reviewed and finalized the vulnerability assessment report including the plan to address any required mitigation actions.</p> <p>ReliabilityFirst 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
RFC2018020025	CIP-004-6	R2	[REDACTED]	[REDACTED]	5/24/2018	9/3/2018	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 July 10, 2018 and October 15, 2018, the entity submitted Self-Reports stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R2. The entity did not comply with CIP-004-6 R2 or CIP-006-6 R2 in two similar instances.</p> <p>The first instance occurred on May 24, 2018. A new security guard was having trouble opening some gates and called in to the Security Operations Center (SOC) for assistance. The new security guard met the security guard in charge in the SOC and exchanged places at 06:27. The new security guard remained at the SOC alone. Inside the SOC, the system monitor (a Physical Access Control System (PACS)) was active. [REDACTED] The new security guard (in the SOC alone) had not received annual CIP training and had not completed his Personnel Risk Assessment (PRA). Therefore, he should not have had the ability to access the system monitor.</p> <p>The new security guard also should not have been left alone inside the SOC because he had not received annual CIP training and had not completed his PRA. The new security guard was left unescorted in the SOC for 26 minutes. The Supervisor of Security Operations arrived at the SOC for the day at 06:53 and found the guard alone. He remained to supervise the guard's access until the original guard returned at 07:44 after making the security rounds.</p> <p>The second instance occurred on September 3, 2018. A senior guard was assigned to work in the SOC while the system monitor was active. The senior guard was assigned to work in the SOC from 23:00 on September 2, 2018 to 07:00 on September 3, 2018. At approximately 03:31 on September 3, 2018 during the senior guard's shift, she requested a new guard to relieve her for a break. The new guard swiped in and was left alone in the SOC beginning at 03:31, while the PACS system was active, for approximately 39 minutes. The new guard was not trained in CIP protocol (had not received the annual CIP training) and therefore should not have been left unsupervised. The senior guard swiped back in at 04:10.</p> <p>This noncompliance involves the management practices of workforce management, work management, and verification. The root cause of both noncompliances is ineffective training of the other security guards as the new security guards should not have been left alone without having received the annual CIP training. Additionally, the entity did not ensure that all guards on duty had received annual CIP training and had completed PRAs which involves ineffective verification. That lack of verification is a root cause of this noncompliance.</p> <p>The first noncompliance started on May 24, 2018, when the first security guard that had not received his annual CIP training and had not completed his PRA was left unescorted in the SOC and ended 26 minutes later on May 24, 2018 when the guard that had not received his annual CIP training was no longer left alone in the SOC.</p> <p>The second noncompliance started on September 3, 2018, when the new guard that had not received his annual CIP training was left unescorted in the SOC, and ended 39 minutes later on September 3, 2018 when the new guard was no longer left alone in the SOC.</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 both noncompliances is allowing guards to access the PACS system without the proper qualifications (valid CIP training and current PRA). (If an alarm had occurred on one of the Physical Security Perimeter access points during the time the new guard was left alone, he would not have known the proper actions to take to investigate the cause of the alarm and document the results. This, however, did not occur during the 26 minute time period or the 39 minute time period the guards were left alone.) The risk is minimized for both instances because the guard desk workstation (the PACS) [REDACTED] is only able to acknowledge alarms and create reports. That account is not able to create badging, grant access, or do any other administrative tasks. The entity confirmed that no actions took place during the 26 minute time period on May 24, 2018 and the 39 minute time period on September 3, 2018 that the unauthorized guards were left alone and had the opportunity to access the system. 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) arrived at the SOC (the Supervisor of Security of Operations) and remained, monitoring the unauthorized guard until the original guard returned; 2) posted a list of authorized guards in the SOC to ensure that all guards would be aware of which guards are authorized to remain unescorted in the SOC; and 3) created a training document that all authorized security team members are required to review and sign-off on acknowledging their responsibilities under the CIP program. <p>ReliabilityFirst 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
RFC2018020024	CIP-006-6	R2	[REDACTED]	[REDACTED]	5/5/2018	9/17/2018	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 July 10, 2018 and October 15, 2018, the entity submitted Self-Reports stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R2. The entity did not comply with CIP-006-6 R2 on two similar instances. The first instance occurred on May 5, 2018.</p> <p>A contractor was working with an escort in a NERC CIP Physical Security Perimeter (PSP) while the contractor was testing systems and functionality. On May 5, 2018, the entity scheduled work with several groups from the entity to test systems and functionality. During the work, the internet went out in various locations throughout the company. The escort left to communicate with the Control Center to determine the extent of the issue at 09:42. While the escort was out of the room, the vendor remained unescorted inside of the PSP for a period of ten minutes. At 09:48, a member of the entity security team arrived at the PSP to get an update on the work, and found the contractor to be unescorted. The security team member left to call in additional security team support. Two security team members returned at 09:52 and stayed with the contractor until the named escort returned at 09:55.</p> <p>The second instance occurred on September 17, 2018, while an entity employee was escorting a contractor who was completing work in the data center (a NERC CIP PSP). The escort left the room and the contractor remained unescorted for a period of one minute and 39 seconds. The Security Operation Center received a forced door alarm on the data center door at 14:59:21. A member of the entity security team walked to the data center to investigate the alarm and found the assigned escort outside the data center door making a cell phone call. The security team member confirmed with the escort that the escort forgot to badge out of the data center and that the escort left the visitor inside the data center unescorted. The security team member sent the escort back into the data center and reminded him that as the escort, he needed to ensure that the visitor was in his continuous line of light. The employee badged back into the data center and resumed his escorting duties at 15:01:14.</p> <p>This noncompliance involves the management practice of workforce management. The root cause of this noncompliance was ineffective training because, in both instances, the employees were not effectively trained on their escorting responsibilities.</p> <p>This noncompliance started on May 5, 2018, when the entity employee left the first contractor unescorted inside the PSP in the first instance and ended on September 17, 2018, when, in the second instance, the entity employee resumed his escorting duties after leaving the contractor unescorted inside the PSP for one minute and 39 seconds.</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 unauthorized individuals to access [REDACTED] without supervision. The risk is minimized for both instances because the contractors were left alone inside the PSP for just ten minutes and for one minute and 39 seconds respectively. Additionally, the contractors had no electronic access to devices inside the PSP and would not have been able to access any devices. The entity confirmed the contractors did not leave the rooms while left unescorted inside the PSP and did not access any electronic devices inside the PSP. 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) remained (security team members) at the location and remained with the contractor until the assigned escort returned and resumed escort duties; 2) created and placed a sign in the PSP areas to remind escorts of what their duties are while escorting visitors in the PSPs; and 3) sent a reminder email to all employees with CIP access reminding them of their escort responsibilities within PSPs. These reminders will help prevent recurrence. <p>ReliabilityFirst 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
RFC2018020756	CIP-004-6	R3	[REDACTED]	[REDACTED]	5/31/2018	9/21/2018	Self-Report	August 2, 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 November 21, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R3.</p> <p>In June 2018, while preparing for an Internal Mock Audit, an entity CIP Compliance Specialist working on completing a sample evidence request was unable to find evidence demonstrating that the evaluation of authorization records was performed at least once within the last 15 calendar months for a Physical Access Controls System (PACS) [REDACTED] Role. Upon review of the CIP-004-6 Part 4.3 evidence, the entity determined that the role was inadvertently excluded from the 15-month review process. The entity last completed the authorization in February 2017 for this access and the authorization next needed to be completed in May 2018. The entity did not complete the authorization until August 2018.</p> <p>The entity conducted an investigation in July 2018 to determine if the access review issue identified was an isolated incident or if other [REDACTED] roles were also excluded from the review. The entity determined the five access roles were also not verified (all of the members are part of the [REDACTED]).</p> <p>These exclusions all occurred due to a process failure. The entity's process is to copy the names of the individuals and access clearances from a very large Excel Workbook and send them via email to the Approving Manager for approval. These access clearances were missed as part of that process. The Manager of these clearances was never notified of the need for approval.</p> <p>This noncompliance involves the management practices of work management and verification. Work management is involved because the entity did not have an effective work process in place to ensure authorizations and verifications were completed timely. The process involves a very large excel spreadsheet that is e-mailed to the approving manager. These access clearances were missed as part of the process. The Manager of these clearances was never notified of the need for approval. That lack of an effective work process is a root cause of this noncompliance. Verification is involved because the entity did not verify that the authorizations and verifications were completed on time.</p> <p>This noncompliance started on May 31, 2018, when the entity first failed to complete the evaluation of authorization records within 15 calendar months for a PACS [REDACTED] Role and ended on September 21, 2018, when the entity completed all of the overdue authorizations.</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 not properly reviewing authorization records within the required 15 month period which would have allowed users to retain escalated privileges after those privileges should have been removed. The risk is minimized because all of the [REDACTED] users are part of the [REDACTED] Team and have [REDACTED] Privileges to perform their daily duties, which reduces the possibility of unauthorized access. And, in each case, access was appropriately provisioned. Additionally, the entity's Access Management System removes user access rights within 24 hours after a role change unless approved by a manager. This mitigates the risk of users being assigned escalated privileges or being retained in a group with privileges because access is removed within 24 hours. 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) reauthorized the electronic access for the five different [REDACTED] to the [REDACTED] systems; 2) completed an investigation of the potential noncompliance and presented the evidence to the entity [REDACTED] Manager; and 3) met with the technical team to give guidelines on the implementation of the new feature to include the 15 month reauthorization feature into the software. <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by August 2, 2019:</p> <ol style="list-style-type: none"> 1) will implement the 15 month approval process in the software. This will eliminate the use of the spreadsheet and email method; and 2) will perform an initial set of 15 month reviews on the software. <p>The use of the automated system will eliminate the need for the manual process. The system will disable or remove users if reauthorization does not occur.</p> <p>The entity will implement 15 month approvals in the software. The process of designing and implementing the new feature to include the 15 month reauthorization feature in the software is a long process and that explains the extended duration of this Mitigation Plan</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
RFC2018019286	CIP-004-6	R4	[REDACTED]	[REDACTED]	12/19/2016	9/5/2018	Self-Report	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 February 21, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4. [REDACTED]</p> <p>On October 2, 2017, the entity identified two users that were removed from the [REDACTED], but had been reactivated automatically by the access management tool. The entity removed access for both of those users that same day after the reactivation. These reactivated accounts only allowed users to physically logon to an EMS console. If a user did physically logon to an EMS console, that person would not be able to access the actual EMS application or any of the servers running the EMS application to perform any functions on the Bulk Electric System because the entity manages these [REDACTED].</p> <p>The entity's [REDACTED] conducted an extent of condition review of all accounts in the entity [REDACTED] and identified [REDACTED] being reactivated. Again, none of these accounts contained any actual access to the entity EMS system, which prevented any users from making any changes to the EMS. Subsequently, until a technical fix could be implemented, the entity instituted a manual process to identify and correct any reactivations as they occurred. This manual process identified and corrected 4 more instances of accounts being reactivated.</p> <p>The root cause of this noncompliance was [REDACTED]. This major contributing factor involves the management practices of implementation, which includes ensuring requirements from operations and maintenance have been communicated and implemented, and workforce management, which includes managing employee permissions and access to assets.</p> <p>This noncompliance started on December 19, 2016, when the first deactivated account was reactivated and ended on September 5, 2018, when the entity implemented a technical fix in the access management tool to prevent the reactivations from occurring.</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, none of these accounts contained any actual access to the entity EMS system, which prevented any users from making any changes to the EMS. Second, all employees who had a reactivated account were currently employed by the company, with an up-to-date Personnel Risk Assessment (PRA) and recently completed NERC CIP Cyber Security training. ReliabilityFirst also notes that the entity indicated, through the extent of condition review, that none of the accounts were logged into after the users associated with the credentials were removed from authorized access. 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 noncompliances arose from different root causes, which ReliabilityFirst determined 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) provided evidence for the disable access for the initial two users identified on October 2, 2017 who had an account changed from inactive to active; 2) disabled access for the [REDACTED] on February 16, 2018; 3) disabled access for the [REDACTED]; 4) identified the root cause of the [REDACTED]; 5) disabled access for the April 9, 2018 user [REDACTED]; 6) disabled access for the April 12, 2018 user [REDACTED]; 7) reviewed the entity [REDACTED] and provided evidence for other [REDACTED] during April-June; 8) monitored the entity [REDACTED]; 9) performed an extent of condition to identify user accounts on other access management connected systems that have been reactivated by the access management system; 10) developed a Job Aid to monitor connected systems for reactivated accounts; 11) implemented technical fixes in the access management system; 12) provided documentation that the system has been disconnected; and 13) reviewed the entity [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
RFC2019021331	CIP-007-6	R5: P6			6/6/2017	10/17/2017	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 December 31, 2017, the entity submitted a self-log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5.6. On October 16, 2017, an entity Relay Test technician was updating a password on [REDACTED] Cyber Assets at a Substation. While performing the change, the Relay Test Technician questioned if the account on the same device type was updated at a different substation. The entity Relay Test Supervisor and technician researched the condition and determined the password on the [REDACTED] Cyber Asset was changed from the default on March 30, 2016. However, the password was not changed again by June 30, 2017 as required to meet the 15 month cycle.</p> <p>This noncompliance involves the management practices of work management and verification. The root cause of this noncompliance was the entity relay test process for changing passwords did not include reconciliation between the work order and the Cyber Asset list to ensure all Cyber Asset accounts were changed.</p> <p>This noncompliance started on June 6, 2017, when the entity should have changed the password on the Cyber Asset and ended on October 17, 2017 when the entity changed the password on the Cyber Asset.</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 potential harm to the reliability of the BPS that could have occurred during this situation was using an out of date password makes it easier to compromise the Cyber Asset at issue. The risk is minimized because the Cyber Asset that did not have the password changed performed an alarm function only meaning it had no control of Bulk Electric System equipment. Therefore, a loss of visibility to the alarm would not have a significant impact to situational awareness. Additionally, the entity had already changed the password on the Cyber Asset from the default password, a limited number of people have authorized access to the passwords, and the entity had electronic and physical protections in place for the Cyber Asset. Lastly, the entity reviewed the history of the Cyber Asset and there were no configuration changes during the time when the password on the Cyber Asset was not updated and changed. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the password; 2) implemented a preventive control of a new report at the Cyber Asset level to identify needed password changes prior to password required change dates; and 3) performed an extent of condition to identify any other Cyber Assets requiring password changes and changed the password, as necessary. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016281	CIP-006-6	R1; Part 1.10	[REDACTED] (the entity)	[REDACTED]	July 1, 2016	October 7, 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 [REDACTED], SERC sent [REDACTED] (the entity) an audit detail letter (ADL) notifying it of a compliance audit scheduled for [REDACTED] through [REDACTED], with the on-site week being the week of [REDACTED].</p> <p>On [REDACTED], the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R1, Part 1.10. the entity did not restrict physical access to cabling used between Cyber Assets within the same Electronic Security Perimeter (ESP) when such cabling was located outside of a Physical Security Perimeter (PSP).</p> <p>When transitioning to CIP Version 5, the entity completed five PSP site assessments with inaccurate information. The individuals assessing the PSP sites misread the internal survey question regarding any cabling or wiring that was within a singular ESP but outside of a PSP. The assessors interpreted the following question literally as of the time of the assessment, "...is there access to the cabling..." and documented a response of "No, the cabling was not accessible". However, the assessors should have interpreted the question to include any cabling or wiring within a singular ESP but outside of a PSP and should have answered "Yes" in five instances and the entity should have documented the other established protections. The entity performed the survey for the purpose of identifying the sites where the cabling was outside of the PSP and then documenting what security measures it had implemented to provide equally effective logical protection. The entity did not document the alternative security measures in these five instances.</p> <p>On [REDACTED], while preparing for the upcoming SERC Compliance Audit, the entity reviewed and assessed all [REDACTED] of its PSPs containing High Impact Bulk Electric System Cyber Systems. During this review, the entity discovered the five sites without the properly documented alternative security measures for cabling that extended outside of the PSP. In total, the entity had [REDACTED] sites where cabling within an ESP extended outside of the established PSP. This review also served as the extent-of-condition assessment for this issue.</p> <p>The entity determined that the root-cause of this noncompliance was human error. Specifically, there was a lack of communication between those who initiated the survey to obtain compliance information, and those who completed the survey.</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable, and ended on October 7, 2016, when the entity documented the alternative security measures taken for cabling outside of the PSP at the five sites.</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 entity's failure to document the alternative protections for cabling outside of the PSP could have caused modifications or additions to these sites to go unrecognized, and permitted the existing security measures deployed to be eliminated or altered, providing an opportunity for the cabling to become a point of weakness or possible attack vector to the BPS. However, the noncompliance was in documentation only, and the entity had already deployed alternative security measures at all five sites (specifically, armored fiber or twisted pair conduit). The entity had previously deployed alternative security measures and created an inventory of sites where it deployed alternative security measures, but the entity had not reassessed the documentation since 2012. No harm is known to have occurred.</p> <p>SERC considered the compliance history of [REDACTED] and determined that there were no relevant instances of noncompliance because the prior versions of the Standard and Requirement did not require restricting access to cabling used between Cyber Assets within the same ESP when such cabling is located outside of a PSP nor documenting alternative security measures.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> utilized network and/or PSP drawings to provide updated corrections to the five site assessments and diagrams identified in this report to adequately demonstrate compliance with the CIP requirements; and scheduled a training session between physical security operations team and the energy management system team to discuss communication process and training on identifying and documenting the requirements for CIP-006-6 R1 (Part 1.10) and to also determine the communication process if any future needs occur regarding the R1 (Part 1.10) 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
SERC2017017231	CIP-004-6	R5; Part 5.3	██████████ (the entity)	██████████	January 9, 2017	January 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 March 14, 2017, the entity submitted a Self-Report to SERC stating that, as a ██████████, it was in noncompliance with CIP-004-6 R5, Part 5.3. the entity did not revoke one individual's electronic access to the designated storage location for Bulk Electric System (BES) Cyber Security Information (BCSI) by the end of the next calendar day following the effective date of the termination action.</p> <p>On January 7, 2017, the entity employee retired, but the entity did not revoke the employee's electronic access to a BCSI storage location until January 13, 2017, which was six days after the termination. The accessible BCSI included information about the entity transmission substations, including ██████████ medium impact BES Cyber Systems also classified as ██████████ BES Cyber Assets (BCAs).</p> <p>Pursuant to the access revocation program, the employee's manager should have submitted an employment status change on or before January 7, 2017.</p> <p>On January 13, 2017, during an ad hoc periodic review by ██████████ operations compliance of its access management application access revocations, ██████████ discovered this access discrepancy. ██████████ The manager then realized the oversight and immediately entered an employment status change into the access management application, which initiated additional processes resulting in the revocation of the former employee's access to the BCSI storage location. The manager also contacted the Information Technology service center that day to revoke access to the corporate network where the BCSI resided.</p> <p>On January 24, 2017, ██████████ operations compliance concluded an extent-of-condition assessment. Specifically, ██████████ reviewed access revocation details for all terminated employees and contractors to ensure timely revocation of all CIP-related access across the ██████████ enterprise and found no additional instances of noncompliance.</p> <p>The root cause of this noncompliance was a training deficiency and ineffective internal controls.</p> <p>This noncompliance started on January 9, 2017, the day after when the entity should have revoked the former employee's BCSI access, and ended on January 13, 2017, when the entity revoked access to the BCSI.</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 revoking BCSI access within 24 hours, malicious actors could have used related information to gain control of cyber assets or make configuration changes via shared user accounts, affect BES facilities and Cyber Systems, and cause grid instability or disturbances. However, the employee retired voluntarily and was in good standing with a current personnel risk assessment and cyber security training. After retiring, the employee only retained access to BCSI and could not access substation BCAs because physical access permissions or Interactive Remote Access would have also been required. No harm is known to have occurred.</p> <p>SERC considered the compliance history of ██████████ and determined that there were no relevant instances of noncompliance because prior versions of the Standard and Requirement did not require entities to revoke access to BCSI repositories by the end of the next calendar day following termination.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) confirmed that the network ID of the entity employee, which could allow for local electronic access to the company network and potentially the BCSI repository, was disabled; 2) conducted a reconciliation review of all terminated employees and contractors that had CIP access to determine if CIP access was revoked within the required timeframe (which confirmed no additional instances); 3) developed and disseminated a CIP access revocation training reinforcement message provided to all managers that have employees reporting to them that are authorized for access to CIP designated areas, systems, and information repositories at the entity; 4) provided the CIP access revocation training from step 3 above to the transmission compliance managers and their personnel at each of the other affiliated companies; and 5) updated the quarterly CIP Awareness Training with a reinforcement message addressing CIP access revocation responsibilities for management. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018403	CIP-004-6	R5; Part 5.2	██████████ (the entity)	██████████	August 16, 2017	August 18, 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 September 27, 2017, the entity submitted a Self-Report to SERC stating that, as a ██████████, it was in noncompliance with CIP-004-6 R5, Part 5.2. the entity did not revoke an individual's authorized electronic access to an individual account by the end of the next calendar day following the date that the entity determined that the individual no longer required retention of that access.</p> <p>On August 12, 2017, the entity employee transferred to a new role. On August 14, 2017, a delegate of an account administrator determined that the transferred employee no longer required retention of electronic access to an Electronic Access Control or Monitoring System (EACMS) and revoked authorization for the access in the access management application. The system then automatically sent emails to all account administrators and delegates notifying them of the access revocation and the need to revoke the transferee's actual access to the EACMS by the end of the next calendar day. However, the account administrators overlooked the need to remove the employee's electronic access and did not complete the task.</p> <p>On August 17, 2017, ██████████ discovered the access discrepancy using a reconciliation tool that compares and reports inconsistencies between actual account access privileges on transmission substation CIP systems and authorized access records in the access management application. ██████████ ██████████ The entity runs this report each Monday morning as an internal control to ensure access revocation consistency. In this case, ██████████ discovered the issue on a Thursday by running the reconciliation tool while verifying access in the process of provisioning access for another user, unrelated to the instant access discrepancy.</p> <p>On August 18, 2017, the entity revoked the transferred employee's electronic access to the EACMS. Afterward, an analyst ran the reconciliation tool to verify proper revocation of all access.</p> <p>In order to verify the extent-of-condition, each ██████████ performed an ad hoc run of the reconciliation tool on all transmission substation CIP systems to ensure no similar issues existed in their systems. ██████████ discovered no additional instances.</p> <p>The root cause of this noncompliance was insufficient training related to access revocation procedures.</p> <p>This noncompliance started on August 16, 2017, the day after when the entity should have revoked access, and ended on August 18, 2017, when the entity revoked electronic 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. By not timely revoking a transferee's authorized electronic access by the end of the next calendar day, an enhanced opportunity existed to tamper with or impair the function of an EACMS. However, the erroneous access only lasted three days. The individual had read-only, non-interactive access, permitting only the viewing of EACMS-related functions applicable to cyber assets in transmission substations. No harm is known to have occurred.</p> <p>SERC determined that ██████████ compliance history should not serve as a basis for applying a penalty because ██████████ underlying conduct was different in the prior. In the prior noncompliance, the entity failed to update a list of personnel with access to Critical Cyber Assets (CCAs) after it had appropriately removed an individual's ability to physically access the CCAs, while in the instant noncompliance, the entity failed to revoke electronic access for a transfer.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the removal of the entity employee's authorized read-only access to the EACMS; 2) reviewed the entity employee's individual account to determine if any electronic access to the EACMS was attempted in the time between the revocation action and access removal; 3) conducted an extent of condition review of transmission substation CIP systems to determine if there are any other instances of authorized electronic access not removed within the required timeframes; and 4) conducted retraining sessions with applicable transmission substation CIP system application administrators on processes and procedures for revoking and removing/disabling access within the required timeframes. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018549	CIP-010-2	R4	██████████ (the entity)	██████████	June 27, 2017	June 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 October 30, 2017, the entity submitted a Self-Report to SERC stating that, as a ██████████, it was in noncompliance with CIP-010-2 R4. The entity had one instance where it did not implement one or more documented plan(s) for Transient Cyber Assets (TCAs) and Removable Media that included the sections in Attachment 1.</p> <p>On June 27, 2017, a field employee plugged a standard corporate laptop into a Bulk Electric System (BES) Cyber Asset (BCA) at an entity substation. The corporate laptop was not on the list of authorized TCAs. The entity substation contained ██████ medium impact BES Cyber Systems and BCAs, and one Protected Cyber Asset. The circumstances surrounding the use of a standard corporate laptop did not involve a CIP Exceptional Circumstance.</p> <p>On June 28, 2017, the entity discovered this noncompliance through a supervisor's inquiry during a maintenance work review. The entity conducted an extent-of-condition assessment by polling field services managers and personnel from the entity and all affiliates and did not discover any additional instances.</p> <p>As CIP-010-2 R4 became effective shortly before the incident, on April 1, 2017, the root cause of this noncompliance was the absence of adequate training on the new procedures and related situational awareness.</p> <p>This noncompliance started on June 27, 2017 at approximately 9:50 a.m., when the entity employee plugged a non-TCA into a BCA, and ended on June 27, 2017 at approximately 10:00 a.m., when the entity employee disconnected the non-TCA from the BCA.</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). By allowing a Cyber Asset that was not designated as a TCA to connect to a BCA, there was a potential risk for the introduction of malicious code or configuration changes, potentially allowing intruders to gain operational control of BPS facilities and cause grid instability. However, the Control Center was aware that there were issues with the BCA requiring replacement. The entity had hardened the BCA against the introduction of malicious code and alteration of the operating system. The non-TCA laptop received the latest available patches and malware prevention updates and had TCA-required security controls in place, making it functionally similar to a TCA. Finally, the entity ensured protection of the BCA by utilizing CIP defense-in-depth provisions, including placement behind a firewall in an Electronic Security Perimeter and Physical Security Perimeter with monitoring at all times. No harm is known to have occurred.</p> <p>SERC considered the compliance history of ██████████ and determined there were no relevant instances of noncompliance because CIP-010-2 R4 was not applicable under prior Versions of the Standard and Requirement.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) had the manager conduct retraining on the CIP-010-2 R4 requirements and the TCA and Removable Media management procedure addressing TCA protocols with offending employee; 2) had ██████████ security operations center conduct an analysis on the non-authorized TCA laptop to verify patches and anti-malware, review the system configuration, and conduct a virus scan of the laptop; 3) the entity transmission compliance sent a compliance communication to relevant transmission personnel reinforcing the requirements around TCAs and Removable Media; 4) the entity transmission compliance conducted TCA and Removable Media awareness training, aligned with the Compliance Communication to further reinforce TCA and Removable Media requirements with the relevant transmission personnel; and 5) the entity transmission compliance installed signage within the PSPs and device stickers on applicable BCAs within the PSP indicating those devices where the dedicated substation TCA must be used for connecting to the devices. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019232	CIP-004-6	R5; Part 5.2	[REDACTED] (the entity)	[REDACTED]	January 20, 2018	January 22, 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 20, 2018, the entity submitted a Self-Report to SERC stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R5, Part 5.2. For reassignments, the entity did not revoke two individuals' authorized unescorted physical access by the end of the next calendar day following the date that the entity determined that the individuals no longer required retention of that access.</p> <p>On January 19, 2018, the entity initiated revocation of authorized unescorted physical access for two reassigned [REDACTED] employees. The first employee planned to retire soon from [REDACTED] and the second employee directly reported to the first employee. The entity reassigned both employees to roles that did not require previously held unescorted physical access to one Physical Access Control System (PACS) badge clearance level that facilitated access to [REDACTED] Energy Management System (EMS) Physical Security Perimeters (PSPs). These [REDACTED] PSPs contained High Impact Bulk Electric System (BES) Cyber Systems owned and maintained by the EMS group, including [REDACTED] BES Cyber Assets, [REDACTED] Electronic Access Control or Monitoring Systems, and [REDACTED] Physical Access Control System Cyber Assets. Pursuant to the entity's documented access revocation program, the manager for the two employees initiated the revocation of physical access via entries in the access management application. However, the entity did not actually revoke access by the end of the next calendar day.</p> <p>On January 22, 2018, the [REDACTED] discovered the access discrepancies when it ran an internal control access comparison program, comparing actual provisioned physical access in the PACS to the intended access entered by the employees' manager in the access management system. The entity implemented this internal control comparison daily, Monday through Friday. Upon discovery, the entity began an investigation of the cause. On January 19, 2018, the [REDACTED] operator responsible for revoking access, revoked the first employee's [REDACTED] substation physical access in the PACS, instead of revoking the intended EMS physical access. Also on January 19, 2018, the [REDACTED] operator attempted to revoke the second employee's correct physical access in the PACS, but did not complete the process, likely due to closing out the PACS record without saving the change. On January 22, 2018 (two days late), the entity completed revoking access for these two employees.</p> <p>The entity did not find any other access discrepancies after running the access comparison program that compares actual access in PACS with intended access in the access management system across the [REDACTED] footprint.</p> <p>The root cause of this noncompliance was the absence of sufficient training in physical access revocation procedures.</p> <p>This noncompliance started on January 20, 2018, the day after when the entity should have revoked the employees' physical access and ended January 22, 2018, when the entity revoked the employees' physical 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. By not timely revoking unescorted physical access for two employees, there was a potential for malicious actors to gain operational control of high impact Bulk Electric System Cyber Assets or Systems and cause a degradation in situational awareness or operate BES Elements and Facilities, causing grid instability. However, because the entity executed its daily, Monday through Friday, internal control, the noncompliance period was only 44 hours. The two employees did not have electronic access to any BES Cyber Assets. The employees had current personnel risk assessments and cyber security training. Additionally, the entity protected the systems at issue with other CIP defense-in-depth measures, including monitoring and alerting, application whitelisting and video surveillance, and security staff on duty at all times. No harm is known to have occurred.</p> <p>SERC determined that the entity's compliance history should not serve as a basis for applying a penalty because the entity's underlying conduct was different in the prior noncompliance. In the prior noncompliance, the entity failed to update a list of personnel with access to Critical Cyber Assets (CCAs) after it had appropriately removed an individual's ability to access the CCAs, while in the instant noncompliance, the entity failed to revoke physical access for transfers.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the badge clearances associated with the access management application revocation in the PACS system and will perform a review of PSP access logs of the two personnel to ensure neither attempted unauthorized access following revocation of approval; 2) made improvements to the process steps of the relevant [REDACTED] work practice to add a requirement to specifically go back and verify clearance removal in a personnel profile after completing the access removal steps when preparing the summary notification to [REDACTED] management of the action completed; and 3) reviewed the updated [REDACTED] work practice with all of the [REDACTED] operators to ensure understanding of the procedure and to provide reinforcement of the access revocation 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
SERC2016016174	CIP-004-6	R5; Parts 5.1, 5.3, and 5.4	[REDACTED] (the entity)	[REDACTED]	July 2, 2016	September 6, 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 [REDACTED], SERC sent [REDACTED] an audit detail letter (ADL) notifying it of a Compliance Audit scheduled for [REDACTED] through [REDACTED], with the on-site week being the week of [REDACTED].</p> <p>On [REDACTED], the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5, Part 5.1. the entity failed to remove an individual's ability for unescorted physical access within 24 hours of the termination action.</p> <p>On [REDACTED], the entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5, Part 5.4. SERC later determined the entity was also in noncompliance with Parts 5.1 and 5.3. SERC also later determined that these issues were related to the initial September 21, 2016 Self-Report and decided to treat the subsequent Self-Report as an expansion of scope [REDACTED] was consolidated into SERC2016016174).</p> <p>In the first instance, on July 1, 2016, a [REDACTED] employee retired, but the entity did not remove the employee's unescorted physical access to the data center until July 5, 2016. The employee's manager failed to initiate the required revocation actions in the appropriate system prior to or on July 1, 2016. Instead, on July 5, 2016, the manager contacted Human Resources to initiate the termination process, resulting in revoking the employee's physical access four days late due to the backdated request. [REDACTED] did not implement the documented overarching the entity access revocation program that dictated specifically when and what actions were required to revoke unescorted physical access and interactive remote access.</p> <p>[REDACTED], while preparing for the upcoming Compliance Audit, the entity reviewed and assessed all 46 individual terminations conducted across all applicable facilities between [REDACTED] and only discovered this single instance of late access removal. the entity has [REDACTED] individuals with unescorted physical access or interactive remote access to Bulk Electric System (BES) Cyber Systems (BCSs).</p> <p>On [REDACTED], the entity discovered a second instance of access oversight while reviewing a list of employees requiring operational training. In this second instance, on August 4, 2016, a college intern completed his or her scheduled summer internship working in the [REDACTED] Control Center and returned to school, resulting in a voluntary termination event. Upon departure, the supervisor collected the intern's physical ID badge, but did not remove physical access authorization to certain CIP Physical Security Perimeters (PSPs) or access to Bulk Electric System (BES) Cyber Security Information (BCSI). In addition, the supervisor did not revoke the intern's non-shared user accounts (electronic access).</p> <p>Although the entity initiated removal of the intern's physical access by collecting the intern's ID badge upon departure, the entity did not disable the badge to fully remove the intern's physical access to three [REDACTED] Energy Management System (EMS) Physical Security Perimeters (PSPs) within 24 hours of the termination, which the entity's documented access revocation program required (Part 5.1). The entity did not revoke the intern's electronic access to two BCSI repositories by the end of the next calendar day following the termination (Part 5.3). Further, the entity did not revoke the intern's electronic access, via non-shared user accounts, to two High Impact EMS Bulk Electric System Cyber Systems (BCSs), within 30 calendar days of the termination (Part 5.4).</p> <p>On [REDACTED], the same day as discovery, the entity removed the intern's unescorted physical access and access to BCSI, as well as revoked the intern's non-shared user account(s) and unescorted physical access to PSPs. the entity never granted the intern Interactive Remote Access. The intern's supervisor managing the removal of access did not change the intern's employment status in the access management application from active to terminated, following the intern's departure.</p> <p>The entity conducted an extent-of-condition assessment, whereby it reviewed interns and co-op students across the [REDACTED] enterprise with electronic and physical access to CIP applicable systems, to ensure active employment and appropriate access. The entity found no additional instances of access discrepancies.</p> <p>The root cause of this noncompliance was human error due to insufficient training because the managers failed to follow the entity access revocation program.</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
SERC2016016174	CIP-004-6	R5; Parts 5.1, 5.3, and 5.4	[REDACTED] (the entity)	[REDACTED]	July 2, 2016	September 6, 2016	Self-Report	Completed
			<p>The first instance started on July 2, 2016, when the entity failed to remove access due to a termination within 24 hours, and ended on July 5, 2016, when the entity removed all access rights for the individual who retired. The second instance started on August 5, 2016, when the entity should have completed removing the intern's physical access to High Impact BCSs, and ended on September 6, 2016, when the entity removed and revoked all 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 (BPS). The entity's failure to timely remove terminated employees' access could provide the individuals the opportunity to access the BCS or the associated Cyber Assets and degrade or damage them in order to negatively impact local operations or create disturbances on the BES. However, the individuals at issue were in good standing and both terminations were voluntary. The individuals had current required cyber security training and had current personnel risk assessments. The individual involved in the first instance only had physical access to one single Physical Security Perimeter (PSP) and had no interactive remote access to any BCS or associated Cyber Assets. Further, this individual did not attempt to access any PSP after the retirement officially occurred on July 1, 2016. For the second instance, the entity collected the interns badge upon departure, making any attempts at physical access more difficult, and the intern never had Interactive Remote Access. No harm is known to have occurred.</p> <p>SERC determined that the entity's compliance history should not serve as a basis for applying a penalty because the entity's underlying conduct was different in the prior noncompliance. In the prior noncompliance, the entity failed to update a list of personnel with access to CCAs after it appropriately removed an individual's ability to access the CCAs. In the instant noncompliance, the entity failed to remove one individual's physical access ability within 24 hours of termination and failed to disable another individual's badge and revoke the individual's electronic access after termination within the required timeframes.</p>					
Mitigation			<p>To mitigate the first noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) [REDACTED] completed the removal of the [REDACTED] employee's physical access to the [REDACTED]; 2) [REDACTED] reviewed PACS logs to determine if the [REDACTED] employee physically accessed the [REDACTED] between July 1, 2016 and July 5, 2016; 3) [REDACTED] compliance team conducted retraining with the manager of the retired employee on the access management program and their responsibilities as a manager; and 4) [REDACTED] compliance team disseminated an awareness message to managers of personnel with CIP access instructing them in the ramifications of backdating terminations and transfers with human resources, which included the reiteration of training in the "[REDACTED]" that managers are responsible for revoking access on or before the effective date of termination or transfer. <p>To mitigate the second noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reviewed the list of current active interns and COOP students across [REDACTED] with access to CIP areas or systems and ensure they are still actively employed and their CIP access is still appropriate; and 2) conducted retraining for managers and supervisors across [REDACTED] that have active interns and COOP students reporting to them on the CIP access management program requirements and their responsibilities. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017711	CIP-004-6	R5; Part 5.2	[REDACTED] (the entity)	[REDACTED]	May 8, 2017	May 8, 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 8, 2017, the entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5, Part 5.2. the entity did not revoke one individual's authorized unescorted physical access by the end of the next calendar day following the date the entity determined the individual no longer required access due to a resignation or transfer.</p> <p>On May 6, 2017, an entity employee transferred to another department within the company where the employee no longer required unescorted physical access to two Physical Security Perimeters (PSPs). However, the entity did not revoke the employee's access until May 8, 2017.</p> <p>Prior to the transfer, the individual was an Energy Management System (EMS) employee with access to [REDACTED] PSPs. The transfer out of the EMS department to the operations compliance department involved retaining unescorted physical access to [REDACTED] of the PSPs and discontinuing access to two. Specifically, the entity should have disabled access to the EMS computer center that housed [REDACTED] High Impact Bulk Electric System (BES) Cyber Systems (BCSs) also classified as BES Cyber Assets, and to the EMS storage room, which was empty during this noncompliance. When the entity changed the employee's department code in the access management application, the system issued an access revocation notification email to the [REDACTED] to effect PSP access revocation as expected, but a technical issue delayed the email. On May 8, 2017, the [REDACTED] received the email and promptly revoked access to the two PSPs, approximately 8.5 hours late.</p> <p>On May 8, 2017, while performing a daily reconciliation of CIP physical access, the [REDACTED] discovered that it had not revoked the employee's physical access to the two PSPs by the end of the next calendar day following the employee's transfer. The daily reconciliation process covers the entire [REDACTED] enterprise and therefore was an extent-of-condition assessment. the entity did not find any additional access discrepancies.</p> <p>The root cause of this noncompliance was a technical issue that delayed the email prompt.</p> <p>This noncompliance started on May 8, 2017 at midnight, a day after unescorted physical access was determined to no longer be necessary, and ended on May 8, 2017 at 8:25 a.m., when the entity revoked 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. By not timely revoking physical access, there was a potential for a malicious actor to gain operational control of High Impact BCSs and cause grid instability. However, the noncompliance only lasted about 8.5 hours. Further, the individual involved was a long-term employee in good standing, familiar with procedures, and retained authorized access to several other PSPs. The transferring employee's personnel risk assessment and cyber security training were up-to-date. In addition, one of the PSPs was empty and the employee did not have electronic access to the BCS housed in the other PSP. Finally, security staff was on duty at all times. No harm is known to have occurred.</p> <p>SERC determined that the entity's compliance history should not serve as a basis for applying a penalty because there was a different underlying cause for the prior noncompliance. In the prior noncompliance, the entity failed to update a list of personnel with access to CCAs after it had appropriately removed an individual's ability to access the CCAs, while in the instant noncompliance, the entity failed to revoke an individual's electronic access for a transfer.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the removal of the employee's physical access to the [REDACTED] and [REDACTED]; 2) reviewed PACS logs to determine if the employee attempted to physically access the [REDACTED] and/or [REDACTED] after 5/6/2017; 3) reviewed the configuration / process and make updates to allow Security Operators the ability to remove physical access clearances in the CIP PACS upon revocation in the company's access management application; and 4) conducted retraining on the updates to the procedure and process for revoking and disabling access during weekend shifts. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017712	CIP-004-6	R5; Part 5.5	██████████ (the entity)	██████████	May 8, 2017	May 11, 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 8, 2017 the entity submitted a Self-Report to SERC stating that, as a ██████████, it was in noncompliance with CIP-004-6 R5, Part 5.5. For a termination action, the entity did not change passwords for shared account(s) known to the user within 30 calendar days of the termination action.</p> <p>On April 7, 2017, the entity terminated a contract employee, not for-cause. The terminated contractor had access to a local administrator shared account that was used to log into the password vault, which provided access to the Energy Management System (EMS) Domain password. The entity did not change the shared account password within 30 calendar days of the termination. On May 11, 2017, the entity changed the shared account password, four days late.</p> <p>On the day of termination, the employee's manager submitted the appropriate information to the Human Resources information and payroll system. Further, on the day of termination, the entity collected the contract employee's physical identification badge and revoked authorizations for physical and Interactive Remote Access to Bulk Electric System (BES) Cyber Assets and BES Cyber Systems (BCSs) in the access management application. The entity had appropriately revoked access to all assets and systems except the one associated with the EMS local administrator shared user account. The retained account provided access to ██████████ High Impact BCS also classified as a BES Cyber Asset.</p> <p>On May 11, 2017, an EMS analyst discovered this noncompliance while conducting on-the-job training between EMS staff responsible for user account management.</p> <p>On May 31, 2017, the entity completed an extent-of-condition assessment by reviewing all EMS personnel terminations and transfers since January 1, 2017, to ensure the entity changed passwords with 30 calendar days of termination for all shared account passwords known to the individuals terminated. The entity found no additional instances where it failed to change passwords to shared accounts within 30 days following a termination.</p> <p>The root cause of this noncompliance was management oversight during a workflow transition. The entity was in the process of transitioning the responsibility of changing the local administrator shared account password to another group within EMS, but had not fully completed the transition yet. This resulted in a miscommunication regarding which group within EMS was responsible for making the required shared password change during the transition period.</p> <p>This noncompliance started on May 8, 2017, the day after when the entity should have changed the shared account password, and ended on May 11, 2017, when the entity changed the shared account password.</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). By not changing a shared account password within 30 calendar days of termination, there was a potential for malicious actors to access and gain control of the EMS system and harm the BPS. However, the entity was only four days late in changing the password. The entity did not terminate the individual for cause. The individual had a current personnel risk assessment and cyber security training. The entity revoked Interactive Remote Access and physical access immediately upon termination. Physical proximity to the affected BCS was required to gain access using the shared account password. Because the password vault at issue used Active Directory authentication to control and manage privileged passwords, the individual could not retrieve the passwords once the entity removed the individual's Active Directory access. In addition, the passwords for the local administrator account are unique per device and complex, making it difficult for someone to memorize the passwords and gain access to a specific device. No harm is known to have occurred.</p> <p>SERC considered the compliance history of ██████████ and determined that there were no relevant instances of noncompliance because prior versions of the Standard and Requirement did not require entities to change passwords on shared accounts within 30 days of a termination action.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reviewed all individuals in EMS that have been terminated or transferred since January 1, 2017 to ensure all shared passwords known to a terminated or transferred individual were changed within 30 days of the effective date; 2) reviewed EMS process for EMS Domain Local Admin entity and ensure individuals are trained on roles and responsibilities; 3) reviewed EMS processes for managing shared account password changes as a result of a termination and make updates to prevent future recurrence; and 4) trained applicable EMS personnel on the new technical or procedural controls. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018140	CIP-006-6	R1; Part 1.2	██████████ (the entity)	██████████	July 5, 2017	July 8, 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 August 8, 2017, the entity submitted a Self-Report stating that, as a ██████████, it was in noncompliance with CIP-006-6 R1, Part 1.2 because the entity did not utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter (PSP) to only those individuals who have authorized unescorted physical access.</p> <p>At approximately 7:15 a.m. on July 8, 2017, security operators received a forced door alarm and an intrusion zone alarm in the Physical Access Control System (PACS) for a PSP at an entity medium impact substation containing ██████████ Bulk Electric System (BES) Cyber Assets (BCAs) and BES Cyber Systems (BCSs). An entity employee working at the substation opened the back door without badging in and caused the forced door alarm. The ██████████ security operators received the forced door alarm when the door opened. Further, the employee entering the switch house initiated an intrusion zone alarm causing a local audible alarm. The employee immediately exited the switch house and contacted the ██████████ to report the alarms. The entity's ██████████ used investigative camera footage of the area to confirm that the employee was in the switch house for less than one minute. On July 8, 2017, at approximately 7:19 a.m., the employee secured the back door and then left the premises.</p> <p>On July 10, 2017, the entity investigated the problem with the back door and determined that the top of the back door was rubbing the doorframe and did not fully secure the latch when shutting on its own. The door closed enough to engage the PACS system alarm contacts, but the door latch did not completely secure within the strike plate. The following day, the entity repaired the door.</p> <p>As part of the extent of condition and as required by the ██████████ procedures, the entity investigated all alarms received through the PACS PSP access control, logging, and monitoring system. Through the investigation, the entity determined the personnel involved, their access authorization status, their purpose in entering the PSP, and if the alarms were caused by any malfunction of the physical access controls in place at PSPs, which was the case in this instance. The entity did not discover any other instances of a PSP access point malfunction.</p> <p>The root cause was the door was out of alignment with the door frame. The door closed enough to engage the PACS alarm contacts, but not enough to latch the door, which allowed someone to pull the door open without using a badge.</p> <p>This noncompliance started on July 5, 2017, when the Standard became mandatory and enforceable on the entity, and ended on July 8, 2017, when the entity employee secured the door prior to leaving the switch house.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk to the reliability of the bulk power system (BPS). The ability to access the entity's medium impact substation switch house without using card access could allow a malicious individual to access and use it in order to disrupt the entity's operations or create a negative impact to the BPS. However, the risk was reduced by the fact that the door was monitored by the entity because it was closing enough to engage the PACS alarm contacts. This alerted ██████████ members to investigate, including the use of camera footage, and also resulted in audible alarms at the PSP. No harm is known to have occurred.</p> <p>SERC considered the compliance history of ██████████ and determined there were no relevant instances of noncompliance because prior versions of the Standard and Requirement did not apply to the substations involved in the instant noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) had the ██████████ issue a reinforcement communication to individuals conducting PSP physical site assessments to check entry and exit doors to ensure the doors are closing/securing properly; 2) had ██████████ conduct a PSP site assessment at the substation switch house and verified that after the repairs were completed, the front and back doors operated as required; and 3) had ██████████ send an email communication reminding individuals to check to ensure doors are secure at the time of departure from a PSP, and reinforcing the process to immediately report any PSP access control malfunction to the ██████████ 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016095	CIP-004-6	R5; Part 5.3	[REDACTED] (the entity)	[REDACTED]	July 1, 2016	July 6, 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 [REDACTED], SERC sent [REDACTED] an audit detail letter (ADL) notifying it of a Compliance Audit scheduled for [REDACTED] through [REDACTED], with the on-site week being the week of [REDACTED].</p> <p>On [REDACTED], the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5, Part 5.3. The entity failed to revoke access to a Bulk Electric System (BES) Cyber System Information (BCSI) repository by the end of the next calendar day following the effective date of the termination action.</p> <p>On June 25, 2016, an entity corporate security employee voluntarily terminated employment with the entity, but the entity did not revoke the individual's electronic access to one BCSI repository until July 6, 2016. The employee's manager submitted employment status change documentation to Human Resources (HR) for July 6, 2016, rather than June 25, 2016. The manager failed to submit the proper forms to off-board the employee in a timely fashion, as required in the entity's access revocation procedure. The manager completed the revocation of the employee's access on July 6, 2016, by removing the employee's corporate network ID and eliminating the ability for electronic access to the BCSI repository.</p> <p>[REDACTED], while preparing for the upcoming CIP compliance audit, the entity discovered this instance. Annually, in July, the entity conducted a review process, which initiated automatically to the managers with personnel who had any CIP accesses. During this annual review, the entity corporate security staff noted this individual was no longer with the company, but still had authorized access to the BCSI repository. This annual review had been in place since 2011 as an internal control. The entity performed this annual review for all individuals with CIP access as the extent-of-condition and confirmed that this instance was the only identified failure.</p> <p>The root cause of this noncompliance was a lack of training. The entity corporate security manager failed to submit the proper work orders as required due to a lack of understanding of the off-boarding processes.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable on the entity because prior versions of the Standard did not have a requirement for access revocation for BCSI, and ended on July 6, 2016, when the entity removed the employee's ability to electronically access the BCSI repository.</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). The entity's failure to revoke a voluntarily terminated employee's electronic access to a single BCSI repository could allow a malicious individual to access and use it to disrupt the entity's operations or create adverse impacts to the BPS. However, the entity reduced the risk for a malicious act because it removed the terminated employee's ability to physically access any the entity facilities by collecting the individual's badge on the last day of employment. The employee's last day of employment was June 25, 2016, at which time the individual had no ability for physical or Interactive Remote Access into any CIP Electronic Security Perimeters (ESPs) or the corporate network. No harm is known to have occurred.</p> <p>SERC considered the compliance history of [REDACTED] and determined that there were no relevant instances of noncompliance because prior versions of the Standard and Requirement did not require entities to revoke access to BCSI repositories by the end of the next calendar day following termination.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) had [REDACTED] IT confirm the [REDACTED] of the entity employee, which could allow for local electronic access to the company network and potentially the BCSI repository, has been disabled; 2) had the [REDACTED] Compliance department confirm the removal of the entity employee's access to the BCSI repository; 3) had the [REDACTED] Compliance department review electronic access logs to the BCSI repository to determine if the entity employee electronically accessed the BCSI repository during the noncompliance; and 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016095	CIP-004-6	R5; Part 5.3	██████████ (the entity)	██████████	July 1, 2016	July 6, 2016	Self-Report	Completed
			4) had the ██████████ Compliance disseminate an awareness message to managers of personnel with CIP access instructing them in the ramifications of backdating terminations and transfers with HR. Evidence will include the reiteration of training in the ██████████ which state managers are responsible for revoking access in the access management system and initiating the access removal processes on or before the effective termination or transfer.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016015989	CIP-006-3c	R2	[REDACTED]	[REDACTED]	7/1/2009	4/18/2018	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] through [REDACTED], the SERC Audit team determined that the Entity, as a [REDACTED], was in violation of CIP-006-3c R2, R2.2. the Entity did not identify all Cyber Assets that authorize and/or log access to the Physical Security Perimeters (PSPs), and did not afford all of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.</p> <p>The SERC Audit team determined that the Entity did not identify the control panels for the PSP access as part of the Physical Access Control System (PACS), resulting in the omission of the required protections from CIP-006-3c R2.2. Audit also noted that the Entity maintained the door controllers within the secured PSP and within an established Electronic Security Perimeter.</p> <p>Because the Entity's vendor asserted it would not provide security updates via firmware updates for these specific devices, the Entity classified the door controllers as non-intelligent locally mounted hardware, and not programmable Cyber Assets. However, SERC determined the door controllers are Cyber Assets and do control PSP access and maintain the data necessary to approve or decline access upon access badge presentation, which is defined by the Standard and Requirement language as the qualifiers for inclusion as a part of the PACS. Although the door controllers do not have security patches, and no security patch source exists for these Cyber Assets, as confirmed by the manufacturer of the PACS, the vendor can and does post operational updates for the firmware as needed. SERC has determined that the door controllers are Cyber Assets because they are programmable electronic devices, and should have been identified and included for appropriate protections as prescribed in CIP-006-3c R2.2.</p> <p>This issue affected two Critical Assets which contained Critical Cyber Assets. The primary headquarters contained [REDACTED] PSPs with [REDACTED] door controllers and the back-up control center contained [REDACTED] PSPs with [REDACTED] door controllers. These are the only PSP access points that utilize this specific type of door controller, so no additional instances could exist and no extent-of-conditions was required.</p> <p>This noncompliance started on July 1, 2009, when the Standard became mandatory and enforceable, and ended on April 18, 2018, when the Entity replaced the existing controller with a new PACS.</p> <p>The root cause of this noncompliance was a misinterpretation of the requirement language. The Entity believed that only the servers were considered PACS.</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 identify PACS Cyber Assets could result in the Entity overlooking or omitting the required protections, resulting the opportunity for manipulation or reconfiguration of PSP access permissions and potentially allowing unauthorized access into existing PSPs. However, although the Entity did not identify these door controllers as a part of the PACS, it did provide the required protections in all but three Requirements (CIP-007 R2, CIP-007 R3, and CIP-007 R4), two of which were not technically feasible for firmware based Cyber Assets (CIP-007 R2 and CIP-007 R4). For CIP-007 R3, although firmware based, the door controllers could be updated via firmware releases or chip set changes. The consultant working for the Entity also reviewed all support and download site of the vendor to determine that no security releases had occurred. No harm is known to have occurred.</p> <p>SERC considered [REDACTED] 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) replaced the entire PACS system; and 2) documented all cyber assets associated with the PACS as PACS Cyber Assets. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019392	CIP-006-6	R1: P1.4	[REDACTED]	[REDACTED]	7/1/2016	9/27/2017	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] to [REDACTED], SERC determined that the Entity, as a [REDACTED], was in noncompliance with CIP-006-6 R1; P1.4. The Entity did not implement a documented physical security plan that included monitoring for unauthorized access through physical access points into a Physical Security Perimeter (PSP).</p> <p>During a physical tour of the Entity's primary and backup control centers, the SERC Audit Team sampled and tested certain PSP doors to verify compliance under various PSP door alarm conditions. After the tour, the Entity presented the Audit Team with the PSP access and alarm logs generated during the tour. The Audit Team then analyzed notes taken and the logs generated during the tour and discovered one primary control center exit-only door not monitored for unauthorized access. Subsequent research revealed the cause was a faulty door contact switch. Because the Entity's documented physical security plan and CIP-006-6 R1; P1.4 require monitoring for unauthorized access through PSP access points, the Entity was in noncompliance.</p> <p>The Entity retained no Physical Access Control System access records prior to approximately 90 days prior to the audit. Due to the absence of records to support a last know working compliant state, SERC has determined that the violation start date was July 1, 2016 when the standard became mandatory and enforceable.</p> <p>On September 29, 2017, the extent-of-condition assessment for this issue concluded. The Entity conducted testing and verified proper monitoring and alerting for all PSP doors.</p> <p>The scope of affected Facilities included the Primary Control Center and a faulty door contact switch.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on September 27, 2017, when the Entity began monitoring PSP unauthorized access at the faulty door.</p> <p>The root cause of this noncompliance was determined to be lack of training to ensure consistent successful completion of configuration and verification steps on PSP access doors.</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 monitoring and alerting all PSP doors, there is a possibility that unauthorized intruders could gain physical access to Bulk Electric System Cyber Assets and Systems and potentially damage or degrade equipment that may affect operational performance or data integrity. However, in this instance, the affected PSP door was an emergency exit-only door with no external badge reader or access hardware. It was always in the line-of-sight of operating personnel who staffed the facility at all times. Security personnel monitored the door at issue real-time via video camera feeds into the security console. The affected PSP was located within a corporate campus behind a perimeter fence and gated entrance with a guard on duty 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) repaired the contact for the door in question, re-executed PACS testing for all physical access points at the primary and backup control centers, and verified that all alarms and door contacts are working as expected; 2) updated the existing Testing and Maintenance process and checklist to include: the addition of [REDACTED] operator(s) on the phone during testing; 3) developed and delivered training for the Field Testers performing the Testing and Maintenance process; and 4) performed testing of all PSP doors using the revised testing and maintenance 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
SERC2018020087	CIP-007-6	R2: P2.3	[REDACTED]	[REDACTED]	5/17/2018	6/25/2018	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 July 24, 2018, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2, P2.3. The Entity had three instances in which it did not implement evaluated security patches that were deemed applicable patches within 35 calendar days of the evaluation completion or create a mitigation plan to mitigate the vulnerabilities addressed by the patches.</p> <p>On June 20, 2018, while conducting routine monthly patch management processes, an Entity employee noted discrepancies in the user dashboard of its patch management tool. Upon investigation, the Entity discovered that three security patches that had previously been evaluated and determined to be applicable, had not been applied within 35 calendar days of evaluation.</p> <p>Specifically, on April 11, 2018, the Entity completed its evaluation of two of the three patches, determined they were applicable and intended application on [REDACTED] Bulk Electric System (BES) Cyber Assets, attempted to apply them but did not successfully apply them until 75 days later on June 25, 2018. A month later, on May 11, 2018, the Entity completed its evaluation of the third patch, determined it was applicable and in need of application on seven BES Cyber Assets, attempted to apply them but did not successfully apply them until 40 days later on June 20, 2018.</p> <p>The Entity used an automated patch deployment tool, but the installation process failed in these three instances. The three patches were queued for deployment; however, when the automated tool attempted to install the patches, the [REDACTED] BCAs disconnected from the patch repository while running the package installation manager, resulting in the tool no longer having an identified patch source to pull from, and resulting in the tool determining no patches existed. This resulted in an execution error and the three patches were not applied. Discovery was delayed due to the random samples chosen for verification scrutiny did not include the instances at issue in this Self-Report.</p> <p>To determine the extent of condition, the Entity reviewed and confirmed the proper patch inventory on in-scope cyber assets via an analysis of patch management tool reports. No additional instance found.</p> <p>The scope of affected Facilities included two control centers containing medium impact BES Cyber Systems. Affected Cyber Assets included two medium impact BES Cyber Systems and [REDACTED] total BES Cyber Assets. No Protected Cyber Assets, Electronic Access Control or Monitoring Systems, or Physical Access Control Systems were involved.</p> <p>This noncompliance started on May 17, 2018, when the first patch was required to have been applied, and ended on June 25, 2018, when the last late patch was applied.</p> <p>The root cause of this noncompliance was lack of internal controls. The Entity did not identify the patching failure after the deployment tool failed due to a lack of insight and awareness.</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 installing security patches within 35-days of assessment, the Entity created an opportunity for bad actors to potentially exploit known vulnerabilities and gain operational control of cyber assets and bulk power system facilities. Actions could then be taken to maliciously cause grid instability and lead to data mining or the introduction of malicious code. However, the unpatched condition lasted only 37 days past what was permitted by the requirement. The seven BES Cyber Assets were protected with access controls such that one could not have gained control of them and operated bulk power system facilities. Additionally, the BES Cyber Assets were protected by firewall/ESP with full-time monitoring and logging and the primary control center PSP was staffed at all times. All involved BES Cyber Assets were protected with malware protection, logging, alerting, ESP monitoring, whitelisting and electronic/physical access controls. The affected BES Cyber Assets had no access to public internet. 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) installed missing patches; 2) created manual patch script to check that the patch source is available to the Cyber Assets; 3) created an automated patch script from the automated patching tool, to be ran to find any missing patches; and 4) provided training for script use. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016015942	CIP-005-3a	R1, R1.4	[REDACTED]	[REDACTED]	3/17/2016	3/18/2016	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 July 22, 2016, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in noncompliance with CIP-002-3 R3. However, SERC determined that this issue is more appropriately addressed under CIP-005-3a R1.4. The Entity did not identify and protect a non-critical Cyber Asset within a defined Electronic Security Perimeter (ESP) pursuant to the requirements of Standard CIP-005-3a.</p> <p>On March 17, 2016, the Entity completed a software and hardware update on an Energy Management System (EMS) in a non-production environment. The Entity then placed the EMS into production. On March 18, 2016, while responding to a non-functioning display issue, the Entity employees realized there had been a miscommunication between the supervisory control and data acquisition (SCADA) department and the [REDACTED] regarding the connection of a Remote Terminal Unit (RTU). The SCADA department had previously asked the [REDACTED] to connect the RTU to the EMS non-production network believing that the [REDACTED] knew to remove it prior to placing the EMS into production. However, the [REDACTED] Network team that connected the RTU to the EMS network believed it was a permanent addition and part of the EMS update. Therefore, the [REDACTED] placed the EMS into production without first disconnecting the RTU. The oversight meant the Entity had inadvertently connected the RTU to the production EMS network and secured it within an ESP, but had not identified it as a Critical Cyber Asset (CCA). Realizing the compliance issue, the Entity then immediately disconnected the RTU from the EMS network.</p> <p>SERC determined that the RTU was not a CCA because it was not essential to the operation of the Critical Asset (the control center) as the Entity intended it for use exclusively during the non-production phase of the system upgrade to support noncritical displays in the control room. Because the RTU was not a CCA, the Entity was not in noncompliance with CIP-002-3 R3 as initially Self-Reported. Rather, the Entity was in noncompliance with CIP-005-3a R1.4 because the RTU was a non-critical Cyber Asset within a defined ESP, and the Entity had not identified and protected it pursuant to the requirements of CIP-005-3.</p> <p>The scope of affected facilities includes the primary and backup Control Centers. Affected Cyber Assets include [REDACTED] high impact bulk electric system (BES) Cyber System, [REDACTED] BES Cyber Assets, [REDACTED] Protected Cyber Assets, no Electronic Access Control or Monitoring Systems and no Physical Access Control Systems.</p> <p>The extent-of-condition assessment consisted of EMS network scans at the primary and backup Control Centers to ensure no additional connections of unidentified Cyber Assets.</p> <p>This noncompliance started on March 17, 2016, when the EMS was placed in production and an unidentified non-critical Cyber Asset (RTU) was within the ESP, and ended on March 18, 2016, when the RTU was disconnected from within the ESP.</p> <p>The root causes of this noncompliance were deficient procedures and training related to configuration change management. Specifically, the Entity lacked procedures that detailed the responsibilities of each of the business units with regards to the RTU.</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 Entity's failure to identify and protect non-critical Cyber Assets within an ESP could lead to a heightened risk that malicious intruders could capitalize on reduced security, affording them the opportunity to change and control CCAs and affect Bulk Electric System facilities. However, in this instance, the connection lasted for less than 24-hours. The Entity electronically protected the RTU within an ESP with firmware and up-to-date security patches. Further, remote access to it was not possible and the Entity physically secured it within a Physical Security Perimeter requiring two-factor authentication. The RTU also came from the same vendor as CIP-applicable RTUs, and the Entity had changed the default password. No harm is known to have occurred.</p> <p>SERC considered the Entity 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) disabled and moved the RTU outside of the ESP; 2) conducted a [REDACTED] scan for anything else that may have gotten connected to the EMS network; 3) implemented a new electronic change control; 4) labelled all CIP Cyber Assets; 5) implemented new weekly change control meetings; and 6) provided training. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016675	CIP-010-2	R2: P2.1	[REDACTED]	[REDACTED]	8/5/2016	11/15/2016	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 December 20, 2016, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED] it was in violation of CIP-010-2 R2, P2.1. the Entity had one instance where it did not implement one or more documented process that includes monitoring, at least once every 35 calendar days for changes to the baseline configuration.</p> <p>On August 2, 2016, the Entity performed monitoring of firmware on devices for changes as compared to the documented baseline configuration on two Energy Management System-connected storage devices classified as Protected Cyber Assets. On September 6, 2016, 35 days had elapsed since the August 2, 2016 review and monitoring of firmware for changes to the baseline configuration was due. However, the Entity did not conduct the required review.</p> <p>On October 31, 2016, during an ad hoc compliance review, the Entity employees discovered it had not performed the firmware monitoring review that was due September 6, 2016. On November 3, 2016, the Entity performed monitoring of firmware for changes to the baseline configuration on the two storage devices and determined there were no changes to the baseline since the last review that it conducted on August 2, 2016.</p> <p>The scope of affected facilities includes the primary and backup control centers, which contain a high impact Bulk Electric System (BES) Cyber System comprised of [REDACTED] BES Cyber Assets.</p> <p>The Entity concluded its extent-of-condition assessment across its enterprise in April 2017 through its mitigation efforts and discovered 9 additional instances where monitoring of baselines had not met the 35-day timeline. Specifically, one instance was 18 days late, one instance was 10 days late; one instance was seven days late, and 6 instances where monitoring for baseline changed did not occur.</p> <p>This noncompliance started on August 5, 2016, when monitoring of baseline changes was due but not conducted, and ended on November 15, 2016, when the Entity performed monitoring for all baselines.</p> <p>The root cause of this violation was an inadequate process. The manual process lacked proper oversight and internal controls to ensure it was conducted every 35-days.</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 Entity's failure to monitor firmware for changes to the baseline configuration, could allow for a degradation in situational awareness whereby intruders could potentially introduce malicious changes to BPS Cyber Assets undetected. However, in this instance, the Entity afforded all the other requisite CIP protections to the affected storage devices as Protected Cyber Assets. Also, although the assets involved were storage arrays associated with the Energy Management System, they did not perform a critical function in the monitoring or operation of the BES. Finally, when the Entity performed the monitoring of firmware for changes to the baseline configuration on the two storage devices, no changes were required. 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) the firmware version was reviewed and determined to be the same version as documented on August 2, 2016; 2) incorporated the review of the [REDACTED] firmware in an automated daily review process like the other components of the baseline; 3) automated the manual firmware review process; 4) had [REDACTED] personnel working with [REDACTED] Server Administrators to create a script that polls the [REDACTED] devices and returns the version information in [REDACTED] file integrity monitoring tool, which is reviewed daily by [REDACTED] professionals. Any unauthorized changes in firmware versions will be detected and remedied. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017016977	CIP-007-6	R2: P2.2, P2.3	[REDACTED]	[REDACTED]	8/5/2016	10/25/2016	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 February 10, 2017, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in violation of CIP-007-6 R2, P2.2 and P2.3. In one instance, the Entity did not evaluate security patches for applicability within 35 days (P2.2), and in another instance, the Entity evaluated a patch within the 35 days, but did not apply the security patch or create a mitigation plan to mitigate vulnerabilities addressed by the patch (P2.3).</p> <p>In the first instance, on September 20, 2016, the Entity [REDACTED] employees discovered its [REDACTED] used to monitor and manage two energy management system (EMS) servers, had security patches that were released, but were not evaluated for applicability within a 35-calendar day period since the last evaluation (P2.2).</p> <p>This instance of noncompliance started on August 5, 2016, when the Entity was required to evaluate the security patches, and ended on November 23, 2016, when the Entity evaluated and applied the patches.</p> <p>In the second instance, on July 5, 2016, the vendor issued a bulletin announcing a security patch release. On July 29, 2016, the Entity conducted an evaluation of the security patch and determined it was applicable. However, on September 3, 2016, 35 calendar days had elapsed since the Entity evaluated the patch, and the Entity had not yet applied the security patch or created a mitigation plan (P2.3).</p> <p>This instance of noncompliance started on September 3, 2016, when the Entity was required to have applied the security patch, and ended on October 25, when the Entity applied the security.</p> <p>The scope of affected facilities for these two instances was the high impact EMS and involved two Protected Cyber Assets (PCA). One PCA was located at the primary control center and the second was located at the back-up control center.</p> <p>The Entity determined that the root cause for instances one and two was an insufficient patch evaluation process. The responsible the Entity employee mistakenly thought the vendor was supposed to evaluate and install [REDACTED] patches. The Entity's process lacked the detail for responsibilities for different EMS components, which led to the failure.</p> <p>On October 4, 2016, a the Entity [REDACTED] employee reviewed a May 2016 Security Information and Event Manager (SIEM) patch assessment and discovered a security patch released prior to July 1, 2016 that was still in the pre-implementation stage. Upon investigation, the Entity determined that the security patch evaluation was due by September 5, 2016, but was completed on September 9, 2016, four days past the 35-day assessment window (P2.2). On October 25, 2016, the Entity installed the security patch on 21 Cyber Assets affected by this issue.</p> <p>This third instance affected [REDACTED] Electronic Access control and Monitoring Systems associated with [REDACTED] high impact and [REDACTED] medium impact Bulk Electric System Cyber Systems.</p> <p>For its extent-of-condition, the Entity reviewed all security patches for the EMS and determined that all other security patches were managed properly. No additional instances found.</p> <p>This instance of noncompliance started on September 5, 2016, when the Entity was required to evaluate the security patch, and ended on September 9, 2016, when the Entity evaluated and applied the patch.</p> <p>The root cause for the third instance was a lack of training for newer and less experienced staff who had responsibility for patching assistance and insufficient patch evaluation process. The patching process lacked the detail required to ensure the Entity properly evaluated and applied patches.</p>					
<p>Risk Assessment</p>			<p>This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to assess and deploy security patches within the prescribed time frame could allow known vulnerabilities to remain available for exploit allowing bad actors to gain operational control of cyber assets and bulk power system facilities and maliciously cause grid instability. However, the Entity deployed layered security controls such as network segmentation that utilized two-factor authentication and used an intrusion detection system with real-time alerting and response. Also, the Cyber Assets at issue were protected within an established electronic Security Perimeter such that an adversary could not have gained control of them and operated bulk power system facilities. The facilities containing the Cyber Assets were staffed full-time with on-site monitoring. Specifically for issue one, [REDACTED] uses a proprietary version of an operating system within a restricted shell that limits terminal commands to navigate [REDACTED] directories. No harm is known to have occurred.</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
SERC2017016977	CIP-007-6	R2: P2.2, P2.3	[REDACTED]	[REDACTED]	8/5/2016	10/25/2016	Self-Report	Completed
			SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) evaluated and applied all patches; 2) update the patch process to require patch reviewers to include a change request reference number on the patch evaluation form to ensure the applicable security patch has been scheduled for implementation; and 3) conducted training for all affected personnel on CIP-007-6 R2 and patching procedures. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017797	CIP-006-6	R1: P1.8	[REDACTED]	[REDACTED]	3/28/2017	6/1/2017	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 June 23, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in violation of CIP-006-6 R1, P1.8. The Entity had five instances where it did not implement one or more documented physical security plan that includes logging entry of each individual with authorized unescorted physical access into each Physical Security Perimeter (PSP), with information to identify the individual and date and time of entry.</p> <p>Sometime before May 1, 2017, the Entity began an initiative to implement and bolster internal controls associated with employees' security-related responsibilities. As part of this initiative, the Entity conducted a random sampling of access logs encompassing a two-month period. On May 1, 2017, the Entity discovered five instances where logs were not generated when individuals authorized for unescorted physical access entered PSPs. In each instance, individuals with authorized access followed other individuals with authorized access into the PSP without swiping their badges and thus were not being logged.</p> <p>These five instances occurred at [REDACTED] substations containing medium impact Bulk Electric System (BES) Cyber Systems. The scope of affected facilities includes [REDACTED] substations containing medium impact BES Cyber Systems. This violation could have impacted [REDACTED] medium impact BES Cyber Systems, [REDACTED] BES Cyber Assets, [REDACTED] Protected Cyber Assets, [REDACTED] Electronic Access Control or Monitoring Systems, and [REDACTED] Physical Access Control Systems Cyber Assets</p> <p>The extent-of-condition assessment consisted of a two-month random sampling of access logs from all [REDACTED] the Entity substations containing medium impact BES Cyber Systems. The Entity sampled 22% of all accesses to all substations, resulting in the identification of five additional instances of incomplete log entries.</p> <p>This noncompliance started on March 28, 2017, the earliest instance where the individual entered the PSP without swiping his/her access badge, and ended on June 1, 2017, the last instance where the individual entered the PSP without swiping his/her badge</p> <p>The root cause of this noncompliance was inadequate training. The training did not ensure that the Entity employees were aware that logging into the PSP was required via badging.</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 Entity's failure to log all PSP visits of authorized personnel, could lead to a loss of situational awareness in the case of insider threats and the ability to investigate malicious acts. However, in this case, the Entity employed security cameras that would facilitate recognition of employees, and all employees with PSP access were authorized to access the PSPs and underwent personnel risk assessments and required cyber security training. The affected BES Cyber Systems all required access credentials and employed security monitoring.</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) disabled card reader access to the CIP [REDACTED] for all employees; employees needing to enter the facilities were required to contact the [REDACTED] to gain access; 2) during the time access was disabled, required its [REDACTED] Compliance group to hold a CIP Compliance stand down with the affected management team. During this stand down, the issues were reviewed along with the specific CIP requirements and the means through which the Entity complies with the requirements. Management was directed to take the information back to their groups and review it with their staffs. Access was reestablished approximately 1 week after it was disabled; and 3) developed additional detailed training for all personnel that access the CIP [REDACTED] 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018381	CIP-004-6	R5: P5.3	[REDACTED]	[REDACTED]	8/1/2016	8/1/2016	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 September 22, 2017, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5, P5.3. The Entity did not adequately implement its process to complete the removal of unescorted physical access within 24 hours of a termination action.</p> <p>During an annual CIP-004 review, a consultant recommended an in-depth review of access revocations beginning July 1, 2016. On July 11, 2017, the Entity discovered one instance of a revocation of an employee's electronic access to designated storage locations for Bulk Electric System (BES) Cyber System Information that occurred two days after termination. On July 30, 2016, the termination occurred and the Entity should have revoked the employee's access by the end of the day on July 31, 2016. However, the Entity did not revoke the access until August 1, 2016, two days after the termination.</p> <p>The extent-of-condition process consisted of a review of records from July 1, 2016 through July 16, 2017 of terminated personnel with access to BES Cyber System Information to ensure timely revocation of access. The Entity did not find any additional issues.</p> <p>The scope of potentially affected facilities includes BES Cyber System Information related to the primary and backup Control Centers and [REDACTED] substations. Affected Cyber Assets include [REDACTED] high impact BES Cyber Systems comprised of [REDACTED] BES Cyber Assets, [REDACTED] medium impact BES Cyber Systems comprised of [REDACTED] BES Cyber Assets, [REDACTED] Protected Cyber Assets, [REDACTED] Electronic Access Control or Monitoring Systems and [REDACTED] Physical Access Control Systems.</p> <p>This noncompliance started on August 1, 2016 at 12:00:01 a., 24 hours after the employee terminated employment, and ended on August 1, 2016 at 08:54 a.m., when the Entity revoked the former employee's access to BES Cyber System Information.</p> <p>The root cause of this noncompliance was a deficient procedure and lack of training.</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 Entity's failure to revoke terminated employee's access to BCSI by the end of the next calendar day, could allow the terminated employee to gain operational control of cyber assets and bulk power system facilities. However, in this instance the issue was brief in that the Entity revoked access only nine hours beyond the deadline. In addition, the termination was voluntary and the terminated employee left on good terms with a then-current personnel risk assessment and cyber security training. This individual at issue never had electronic or physical access to BES Cyber Systems or their associated Cyber Assets. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, SERC determined that the Entity's compliance history should not serve as a basis for applying a penalty because of the different causes of the prior noncompliance and the current noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) removed the individual's BES Cyber System Information access; 2) Revised the internal documentation on account de-provisioning; and 3) revised training and documentation to address access revocation. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018018993	CIP-010-2	R1: P1.2	[REDACTED]	[REDACTED]	10/24/2017	11/09/2017	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 16, 2018, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1, P1.2. The Entity had two instances where it did not implement a documented process that includes authorizing and documenting changes that deviate from the existing baseline configuration.</p> <p>In the first instance, on October 24, 2017, the Entity's [REDACTED] department provided a system control and data acquisition engineer with a temporary workstation while it updated engineer's production workstation. The production workstation had a software suite installed that was not installed on the temporary workstation but needed to be in order to facilitate normal workflow related to support of the production workstation. The engineer noticed the temporary workstation was missing the software suite, and installed it without authorizing and documenting the baseline change deviation in conformance with the documented configuration change management process. The Entity classified this workstation as a Protected Cyber Asset, and it was located within the primary control center.</p> <p>On October 25, 2017, the Entity's CIP monitoring administrator received an automated notification regarding the installation of the software on the temporary workstation, then forwarded the notification details to the [REDACTED] department. [REDACTED] promptly realized and corrected the oversight by authorizing and documenting the baseline deviation change. This report was an internal control that the Entity implemented to identify such instances on a nightly basis.</p> <p>In the second instance, on October 24, 2017, the Entity created a draft baseline configuration change request related to the installation of a security patch on the [REDACTED] used to manage EMS servers. However, the Entity did not submit the draft as required by its change request process. On October 27, 2017, during a post-job review, the Entity discovered that previously in the day, a the Entity employee had installed a security patch on the [REDACTED] without authorizing and documenting the baseline deviation change, a noncompliance with CIP-010-2 R1, P1.2. On November 9, 2017, the Entity obtained authorization and documented the baseline deviation change.</p> <p>The Entity classified this [REDACTED] as a Protected Cyber Asset, located within the primary control center. The scope of affected facilities for both issues included the primary and backup control centers. Affected Cyber Assets included [REDACTED] high impact Bulk Electric System (BES) Cyber System, [REDACTED] BES Cyber Assets, [REDACTED] Protected Cyber Assets, [REDACTED] Electronic Access Control or Monitoring System, and [REDACTED] Physical Access Control Systems.</p> <p>The Entity completed the extent-of-condition assessment by reviewing the daily report that reports out on baseline discrepancies. The Entity identified no additional instances.</p> <p>This noncompliance started on October 24, 2017, when software was first installed without authorizing and documenting the baseline change, and ended on November 9, 2017, when the Entity obtained authorization and documented the baseline deviation change after applying a security patch.</p> <p>The root cause of this noncompliance was a training deficiency to ensure that changes that deviate from the existing baseline configuration are authorized and documented.</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 Entity's failure to authorize and document changes that deviate from the existing baseline could have led to a degradation in organized control and situational awareness of applied configurations. Malicious actors could potentially exploit these vulnerabilities to cause grid instability. However, in the first instance, the Entity previously tested, authorized and approved the software in the production environment and unintentionally left it off the temporary environment after an operating system upgrade. In the second instance, the [REDACTED] was solely for console access to EMS servers and was hardened to increase security and did not allow user-installed software or access to a command-level interface. Further, the Entity discovered both instances using established internal controls. 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, [REDACTED]</p> <ol style="list-style-type: none"> 1) Added the configuration of the workstation to the baseline; 2) Developed a new training module that covers internal change management tool and process, and 3) Trained all affected 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
SERC2017017233	CIP-007-6	R2: P2.2	[REDACTED]	[REDACTED]	10/5/2016	02/2/2017	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 14, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2P2.2. The Entity did not evaluate security patches for applicability at least every 35 days.</p> <p>On January 17, 2017, an Entity SCADA support personnel ran an unfiltered report on its energy management system (EMS) vendor's patch certification portal and discovered security updates that were listed with a status of "Certified – Use Caution" that did not show up on its standard reports after using the filter, "Certified."</p> <p>On August 30, 2016, the EMS vendor released one patch with a variant disclaimer wording "Certified-Use Caution." This language difference caused the assessor to miss the patch. Upon discovering the missed patch, the Entity evaluated and installed the patch on January 17, 2017.</p> <p>On November 30, 2016, the EMS vendor released three patches with a variant disclaimer wording "Certified-Use Caution." This language difference again caused the assessor to miss the patches. On January 20, 2017, the Entity evaluated the patches and determined that one of the patches was applicable, which was applied on February 2, 2017.</p> <p>This noncompliance started on October 5, 2016, when the Entity was required to evaluate the first patch, and ended on February 2, 2017, when the Entity applied the last missed patch.</p> <p>The root cause was determined to be lack of training on the EMS Patch Certification Portal. The SCADA support personnel misunderstood the filtering criteria on the EMS Patch Certification Portal, which caused the inaccurate available patch list.</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 Entity's failure to evaluate security patches for applicability at least every 35-days could have led to the Entity supporting vulnerable software, which could have opened attack vectors allowing possible unauthorized access into the Bulk Electric System (BES) Cyber System, potentially affecting the reliable operation of the BPS. However, the Entity BES Cyber Assets are inside an Electronic Security Perimeter (ESP), protected by a firewall, and the Entity does not permit email or instant messaging inside of the ESP. The Entity monitors its ESP network to alert its system administrators of escalated user privilege. In addition, the Entity discovered the missed patches within 60 days of required assessment. 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) determined that the selection criteria for all selections should be "all" to ensure it does not miss any items that are certified by the EMS vendor or certified with any exceptions. This will yield a report with all platforms, statuses, and manufacturers; 2) revised its process to include a step to verify that the installed patch list matches the list of installed patches that resulted from the patch evaluation; 3) instituted an internal control that the Entity SCADA support personnel will meet on the first week of every month to discuss new patch evaluations for the month and confirm "all" evaluated patches and updates from the previous month to be installed into production. The team reviews the recently applied patches for completion, the current approved patches for application deployment to the production system and the newly certified patches for evaluation; and 4) sent an email notification to all system administrators informing them of the changes to the Entity's CIP system security management 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
SERC2017017234	CIP-007-6	R2: P2.3	[REDACTED]	[REDACTED]	01/07/2017	01/24/2017	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 14, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2.3. The Entity did not install or mitigate applicable patches released by the identified patching source within 35 calendar days of the completed evaluation.</p> <p>On October 31, 2016, the Entity's energy management system (EMS) patch certification portal released a patch for a third-party software. On December 2, 2016, the Entity evaluated the software patch within the required 35-day assessment window. On January 17, 2017, the Entity discovered the noncompliance during an extent-of condition review following an earlier noncompliance ([REDACTED]) regarding missing patch evaluations. On January 24, 2017, the Entity applied software patch, which was 17 days outside of the required 35-day patch window.</p> <p>This noncompliance started on January 7, 2017, when the Entity was required to have installed the patch, and ended on January 24, 2017, when the Entity installed the patch.</p> <p>The root cause of this noncompliance was a lack of detailed process for comparing patch installation results to patch evaluation results.</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 Entity's failure to patch or mitigate security patches at least every 35-days after evaluation could have led to the Entity supporting vulnerable software, which could have opened attack vectors allowing possible unauthorized access into the Bulk Electric System (BES) Cyber System, potentially affecting the reliable operation of the BPS. However, the Entity BES Cyber Assets are inside an Electronic Security Perimeter (ESP), protected by a firewall, and the Entity does not permit email or instant messaging inside of the ESP. The Entity monitors its ESP network to alert its system administrators of escalated user privilege. In addition, the Entity patched the vulnerability within 17 days after the required patch timeframe. Moreover, the [REDACTED] hack addressed in the late patch is a specific vulnerability identified in [REDACTED], which the Entity does not utilize inside the ESP. 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) reviewed every patch back to the date of the system build to ensure that the Entity installed all patches that were available; 2) revised its process to include a step to verify that the installed patch list matches the list of installed patches that resulted from the patch evaluation; 3) instituted an internal control that the Entity SCADA support personnel will meet on the first week of every month to discuss new patch evaluations for the month and confirm "all" evaluated patches and updates from the previous month to be installed into production. The team reviews the recently applied patches for completion, the current approved patches for application deployment to the production system and the newly certified patches for evaluation; and 4) sent an email notification to all system administrators informing them of the changes to the Entity's CIP system security management 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
SERC2018019099	CIP-007-6	R4: P4.3	[REDACTED]	[REDACTED]	10/06/2017	03/08/2018	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 January 31, 2018, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R4, P4.3. The Entity did not retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days.</p> <p>On October 6, 2017, the Entity performed its annual shared account password changes per CIP-007-6 R5, P5.6. After the password changes, the Entity failed to reconfigure [REDACTED] of the updated passwords in the central logging and alerting software, thereby inadvertently disabling the logging for two Electronic Access Control or Monitoring Systems (EACMSs) located in its demilitarized zone (DMZ).</p> <p>On December 27, 2017, during a review of the Entity's logging and alerting software, an Entity employee discovered that it could not access event logs for the two EACMSs. The local event logging on the [REDACTED] EACMSs were logging correctly, but because the local windows were set to "overwrite" instead of "archive", and because the large volume of data, each had only 19 days of event logs available, instead of the required 90 days. On that same date, the same the Entity employee performed the configuration change, which restored log retrieval, correlation and alerting.</p> <p>As an extent-of-condition review, the Entity stated that it performed a complete analysis of the two central logging systems deployed by the Entity for its [REDACTED] Medium Impact Cyber Assets, and confirmed that the loss in connectivity had only occurred for the [REDACTED] EACMSs.</p> <p>This noncompliance started on October 6, 2017, when the Entity failed to retain applicable event logs when it reconfigured two of the updated passwords in the central logging and alerting software, and ended on March 8, 2018, 90 days after the Entity's earliest evidence of local log files.</p> <p>The root cause of this noncompliance was a procedural deficiency. The Entity had an insufficiently detailed procedure for ensuring that the Entity captured logs after password changes and for configuring log settings.</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 Entity's failure to retain applicable event logs for at least the last 90 consecutive calendar days could have inhibited potential investigation into a compromise of the operation of Bulk Electric System (BES) Cyber Systems because the missing data, in this instance, would not have been available for review. However, the Entity had 19 days of the latest logs available locally, remote access into the DMZ to access these servers still required VPN authentication at the intermediate system, and the servers themselves, required additional authentication. Also, the servers were located inside a Physical Security Perimeter (PSP), which is restricted to authorized personnel who are current on NERC CIP training and an up-to-date personnel risk assessment on file. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, SERC determined that the Entity's compliance history should not serve as a basis for applying a penalty because of the different causes of the prior noncompliance and the current noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) corrected the configuration on the [REDACTED] cyber assets so that affected logs are being forwarded properly; 2) assigned personnel to actively monitor [REDACTED] software for logging at least once per week; 3) contacted vendor for assistance on additional configuration measures to ensure alerting on event log failures or forwarding failures; 4) changed local event log settings on cyber assets which log to [REDACTED] software to archive logs locally as well when file size reaches certain size; 5) configured [REDACTED] to automatically send status of logging report for all assets monitored by the [REDACTED] software and discontinued active personnel monitoring once this report was tested and operational; 6) updated and formalized the SCADA administrators' checklist to follow when implementing annual shared account password change to ensure that event log forwarding and alerting is functional; 7) trained SCADA System Administrators on any procedural changes; and 8) applied and tested vendor-recommended changes for [REDACTED] software to effectively detect and alert on failures of event logging. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019267	CIP-010-2	R1: P1.4	[REDACTED]	[REDACTED]	3/28/2017	10/16/2017	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 February 26, 2018, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1, P1.4. the Entity did not implement one or more documented processes that, for a change that deviated from the existing baseline configuration, prior to the change, determined required cyber security controls in CIP-005 and CIP-007 that could have been impacted by the change, verified that required cyber security controls determined in 1.4.1 were not adversely affected, and documented the results of the verification.</p> <p>On March 28, 2017, the Entity installed a new Physical Access Control System (PACS) server, replacing an existing PACS server. The Entity repurposed the old server as a data repository, and disconnected it from all control panels, but did not disconnect it from the Electronic Security Perimeter (ESP) network. The Entity removed the old server from the ESP network drawings and its Bulk Electric System (BES) Cyber System Asset list, but did not reclassify the old server as a Protected Cyber Asset (PCA) or remove the server from the ESP network. The data repository remained connected to the ESP network, but the Entity did not list it on any documentation.</p> <p>On October 5, 2017, during its annual Cyber Vulnerability Assessment, the Entity discovered the data repository server still on the ESP network. On October 16, 2017, the Entity disconnected the server from the ESP network.</p> <p>The Entity performed an extent-of-condition and determined the issue was limited to that one cyber asset.</p> <p>This noncompliance started on March 28, 2017, when the Entity installed a new PACS server, but did not disconnect the old PACS server from the ESP network and instead used it as a repository, and ended on October 16, 2017, when the Entity disconnected the repository from the ESP network.</p> <p>The root cause of this noncompliance was the Entity's insufficient change management process. The Entity did not have a clearly-defined process for reclassifying Cyber Assets in or associated with BES Cyber Systems.</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's failure to reclassify a replaced Cyber Asset or remove it from the ESP network could have afforded an opportunity for potential malicious actors to access and modify or compromise the operation of BES Cyber Systems because the Cyber Asset, in this instance would not have been trackable because the Entity took it off of the ESP Diagram and Cyber Asset list. However, in this instance, remote access into the ESP to access this server still required VPN authentication at the intermediate system and additional authentication into the server. Also, the server was located inside a Physical Security Perimeter, which is restricted to authorized personnel who are current on NERC CIP training and an up-to-date personnel risk assessment on file. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, SERC determined that the Entity's compliance history should not serve as a basis for applying a penalty because of the different causes of the prior noncompliance and the current noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) disconnected the old PACS server from the network; 2) start the process of decommission/reuse of a cyber asset; 3) converted Cyber Asset to a repository; 4) finalized process changes for decommission/reuse of cyber assets to include the conversion of a cyber asset to a repository. Review and update, as appropriate, the change review process and security controls check list for process improvements; 5) trained personnel on process changes. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017037	CIP-006-6	R1: P1.4	[REDACTED]	[REDACTED]	12/22/2016	12/23/2016	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 February 17, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R1, P1.4. The Entity did not monitor for unauthorized access through one physical access point into a Physical Security Perimeter (PSP).</p> <p>On December 22, 2016, the Entity installed a secondary doorway in a PSP containing a Medium Impact Bulk Electric System (BES) Cyber System. The Entity installed a temporary security device to prevent any access to the PSP through the new doorway until installation of standard electronic door monitoring and alarming equipment was completed. The primary doorway to the PSP was still monitored, logged, and alarmed. During the door construction, the Entity designated a CIP-authorized employee as a full-time escort so that the contractor could perform work on the new doorway.</p> <p>At approximately 3:00 p.m. on December 22, 2016, the contractor completed work for the day. The contract personnel properly signed in and out of the NERC CIP access log for visitors, but the escort failed to secure the new PSP door with the temporary security device. At approximately 6:30 a.m. on December 23, 2016, the Control Room Supervisor found the newly constructed PSP door unsecured and missing the temporary security device. The Entity immediately reinstalled the temporary security device.</p> <p>The Entity found that the extent-of-condition of this noncompliance was limited to the one-time construction activity on a single door.</p> <p>This noncompliance started on December 22, 2016 at approximately 3:00 p.m., when the escort left the PSP with installing the temporary security device, and ended on December 23, 2016 at approximately 6:30 a.m., when the Entity reinstalled the temporary security device.</p> <p>The root cause of this noncompliance was a procedural deficiency, e.g., the specific steps to provide security during construction.</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 Entity's failure to monitor for unauthorized access through a physical access point into a PSP could have led to unauthorized access by a malicious actor who could have affected real-time operation of the BPS. However, the Entity staffs the control center 24/7 and the new PSP door is visible to the system operators and the shift supervisor. The PSP sits within a secure office space with three layers of security before a person could have reached the unsecured PSP door. The Entity discovered this noncompliance using an internal control and secured the PSP door within 15.5 hours after it was left unlocked. The Entity personnel observed no unauthorized access to the PSP in question during the noncompliance. 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) updated the NERC CIP Physical Security Plan to include instructions for maintaining the PSP at required security levels during periods of time that the PSP is temporarily impacted due to work affecting normal monitoring and alarming capabilities; 2) created a new "Construction CIP" procedure to define the proper implementation steps to take during periods when the Entity suspends the electronic monitoring and alarming of the PSP; 3) provided training on the "Construction CIP" procedure; 4) installed and commissioned an electronic locking, monitoring and alarming system on the new door; and 5) created procedures to stress the importance of securing and monitoring PSP access points during times when electronic means are unavailable (e.g. construction). 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018100	CIP-004-6	R5: P5.1	[REDACTED]	[REDACTED]	07/08/2017	07/10/2017	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 August 3, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5, P5.1. The Entity did not implement a process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action.</p> <p>On July 7, 2017, the Entity scheduled a retiring employee with authorized unescorted physical access to a PSP in a control center to return his work-related items. The manager of the control center responsible for implementing the procedure for Physical Security Perimeter (PSP) access termination was on vacation. The assistant manager was not familiar with the procedure and therefore did not terminate the retiring employee's physical access to the PSP as called for by the original retirement plan. The employee had physical access to the PSP but did not have Interactive Remote Access.</p> <p>On July 10, 2017, during an internal control termination review, the manager learned of the uncompleted termination process and immediately executed the access termination procedure. The manager initiated an extent-of-condition review and discovered no other relevant instances of related noncompliance.</p> <p>This noncompliance started on July 8, 2017, when the Entity was required to remove the former employee's unescorted physical access to the PSP, and ended on July 10, 2017, when the Entity removed the former employee's unescorted physical access to the PSP.</p> <p>The root cause of this noncompliance was inadequate training on its CIP access termination procedure for the assistant manager who was covering for the vacationing manager.</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 Entity's failure to remove the retiring employee's ability for unescorted physical access within 24 hours of the termination action could have led to unauthorized access by a malicious actor who could have affected real-time operation of the BPS. However, the retiring individual had been a long-term employee that had proper CIP clearance in place. The Entity staffs the control center 24/7, making it difficult for unauthorized access to go unnoticed. In addition, the Entity removed the retired employee's access two days after the noncompliance started, which was the following business day. The Entity determined that the retired employee did not attempt to physically access the PSP after his July 7, 2017 retirement. 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) permanently terminated the unescorted physical access formerly granted to the retired system operator; and 2) implemented formal training to control center management, including the assistant manager, on the PSP access removal procedure. The Entity implemented this formal training as an annual training requirement. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016170	CIP-006-6	R1, P1.4, P1.8			07/06/2016	08/01/2016	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 violation.)			<p>On September 19, 2016, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R1, P1.4 and P1.8. The Entity had 10 instances where it did not monitor access through a physical access point into a Physical Security Perimeter (PSP) (P1.4) and log entry and exit of each individual who accessed a PSP (P1.8).</p> <p>Before CIP-006-6 became enforceable on July 1, 2016, it was company practice for field personnel to call the [REDACTED] to have them remotely unlock substation relay house doors to facilitate entry to cyber assets for field work. After July 1, 2016, such doors became PSP access points into PSPs and the prior practice became obsolete. On August 1, 2016, while investigating an open gate issue at a substation, staff discovered that personnel at the [REDACTED] had remotely unlocked the substation PSP access door, and that it was a potential noncompliance. This led to an extent-of-condition assessment whereby the Entity researched all [REDACTED] remote unlocks that occurred in the month of July 2016 to determine if any additional instances occurred. The Entity discovered nine additional instances where the [REDACTED] remotely unlocked relay control house doors for authorized personnel at three substations housing medium impact Bulk Electric System (BES) Cyber Systems (BCSs) with External Routable Connectivity on nine different days, thus resulting in violations of CIP-006-6 R1 P1.4, P1.8. The 10 instances involved 23 employees who had authorized access to the PSPs but did not swipe their badges when entering or existing the PSPs.</p> <p>The scope of affected Facilities included three transmission substations. Affected Cyber Assets included [REDACTED] medium impact Bulk Electric System (BES) Cyber Systems, [REDACTED] BES Cyber Assets, and [REDACTED] Protected Cyber Assets.</p> <p>This noncompliance started on July 6, 2016, when the [REDACTED] remotely unlocked a substation relay house PSP door for the first employee, and ended on August 1, 2016, when the [REDACTED] was informed to no longer permit remote provision access.</p> <p>The root cause of this noncompliance was inadequate training during the transition to CIP-006-6.</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 logging PSP entry of each authorized individual, a degradation in situational awareness occurred with respect to the identities and times of personnel entry. Thus, if a cyber security incident or other adverse event had occurred, it may not have been possible to determine the responsible individual(s). However, in all instances, the Entity authorized personnel for unescorted physical access. In all but one instance, recorded video surveillance was available and reviewed to identify individuals. In each instance, the [REDACTED] was aware that field personnel were inside PSPs. The Entity monitored and protected BES Cyber Assets within the ESPs, and controlled electronic access to them in order to thwart misuse. Finally, the Entity reduced the possibility of entry by unauthorized persons by either locking perimeter gates or placing them under human supervision. 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) notified [REDACTED] of the human error and the [REDACTED] employees were directed to discontinue unlocking doors remotely; 2) performed a gap analysis to identify and resolve any gaps in its CIP-006-6 physical security plan and procedures for monitoring and logging access to PSPs; 3) created a formal face-to-face training for [REDACTED] to ensure they understand the monitoring and logging access procedures and their roles and responsibilities; 4) created a face-to-face targeted training emphasizing unescorted physical access responsibilities for personnel and service contractors working in substations to ensure they understand their responsibilities; and 5) completed training for [REDACTED] and personnel and service contractors working in substations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016508	CIP-004-6	R5, P5.1, P5.2	[REDACTED]	[REDACTED]	07/01/2016	08/23/2016	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 violation.)			<p>On November 15, 2016, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5, P5.1 and P5.2. The Entity reported one instance where it did not timely revoke a terminated employee's unescorted physical access to a Physical Security Perimeter (PSP) (P5.1) and two instances where it did not timely revoke unescorted physical access to a PSP of two employees who were transferred to different positions that do not require such access rights (P5.2).</p> <p>The reported instances involved three workers from an interconnected unaffiliated [REDACTED] generation facility with authorized unescorted physical access to one Entity's PSP located at the Entity-owned switchyard control house located at the unaffiliated generation facility.</p> <p>In the first instance, on August 23, 2016, the Entity received notice from the unaffiliated generation facility that one of its employees with unescorted physical access to one Entity-owned switchyard PSP was terminated, effective July 1, 2016. However, the Entity did not revoke the former employee's unescorted physical access until On August 23, 2016, the date the Entity received notice that the employee had been terminated (P5.1).</p> <p>This instance of noncompliance started on July 1, 2016, when the Entity was required to revoke the terminated employee's unescorted physical access to the PSP, and ended on August 23, 2016, when the Entity revoked such access.</p> <p>In the second and third instances, on August 23, 2016, the Entity received notice from the unaffiliated generation facility that two of its employees with unescorted physical access to one Entity-owned switchyard PSP had been transferred to different positions, which did not require such access. The first individual was transferred on June 20, 2016, and the second individual was transferred on July 4, 2016; however, the Entity did not revoke the employees' unescorted physical access until August 23, 2016, the date the Entity received notice of the transferred employees who no longer needed such access (P5.2).</p> <p>The second instance of noncompliance started on June 21, 2016, when the Entity was required to revoke the transferred employee's physical access to the PSP, and ended on August 23, 2016, when the Entity revoked such access. The third instance started on July 5, 2016, when the Entity was required to revoke the transferred employee's physical access to the PSP, and ended on August 23, 2016, when the Entity revoked such access.</p> <p>The scope of affected Facilities included one transmission switchyard. Affected Cyber Assets included [REDACTED] medium impact BES Cyber Systems (BCS) in the control house with [REDACTED] Electronic Access Control and/or Monitoring Cyber Assets, [REDACTED] BES Cyber Assets, [REDACTED] Protected Cyber Assets, and [REDACTED] Physical Access Control System Cyber Asset.</p> <p>The Entity conducted an extent-of-condition by reviewing lists of individuals with unescorted physical access to its unaffiliated generation facilities and confirmed no additional instances of noncompliance.</p> <p>The root cause of these instances of noncompliance was a deficient process that did not clearly define the roles and responsibilities of the Entity and unaffiliated generation facility. Consequently, there was confusion as to the ownership of certain tasks, which resulted in inconsistent application of the revocation process.</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 timely revoking unescorted physical access, three individuals had the ability to access the BCS and potentially make configuration changes to protection equipment or damage or manipulate facilities interconnecting a generating facility. This could have resulted in misoperations or other grid instability. However, in these instances, the unaffiliated generation facility transferred two of the three individuals to different positions, and the third individual was not terminated for cause. None of the three individuals had electronic access to the BCS. In addition, entering the PSP would have triggered an alarm at the Security Operations Center, prompting an immediate investigation. The PSP had video surveillance, which would have been available to review had an investigation been necessary. Finally, the BCS contained in the substation control house was protected within an Electronic Security Perimeter, and CIP-007 electronic monitoring was in place 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>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016508	CIP-004-6	R5, P5.1, P5.2	[REDACTED]	[REDACTED]	07/01/2016	08/23/2016	Self-Report	Completed
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked access of the three individuals; 2) coordinated a face-to-face meeting and conference call with the non-Entity company to discuss requirements of the Entity's procedure and NERC requirements; and 3) completed and executed an Memorandum of Understanding (MOU) with the non-Entity utility; the MOU established processes and procedures to be followed, and clearly defined the roles and responsibilities of both the Entity and the non-Entity utility to ensure compliance with NERC requirements. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017016786	CIP-002-5.1	R1, P1.3	[REDACTED]	[REDACTED]	07/01/2016	02/17/2017	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 violation.)			<p>On January 14, 2017, the Entity submitted a Self-Report to SERC stating that, as a [REDACTED], it was in noncompliance with CIP-002-5.1 R, P1.3. The Entity did not identify each asset that contained a low impact Bulk Electric System (BES) Cyber System (BCS).</p> <p>On November 4, 2016, while performing a comprehensive review of a BES asset list, the Entity discovered that its list of assets containing low impact BCSs was inaccurate when signed off by the [REDACTED] prior to the July 1, 2016 effective date of CIP Version 5.</p> <p>The inaccuracies included the following: (1) in-service dates for some of the substations containing low impact BCAs were expedited and placed in-service before July 1, 2016 and not communicated to the personnel compiling the list; (2) failure to identify all low impact BCAs, primarily BES Transmission Elements, that can be remotely operated through the RTU, such as motor operated disconnect switches; (3) failure to identify low impact BES Cyber Assets located in BES facilities not owned by the Entity, but that contain low impact BCAs owned by the Entity; and (4) lack of proper subject matter review prior to finalizing the list to ensure it contained the correct low impact BCSs.</p> <p>There were [REDACTED] affected facilities where low impact BCSs were not correctly identified.</p> <p>The extent-of-condition consisted of a comprehensive review of all BES assets, and a review of asset in-service dates to ensure identification of all BCSs (not just low impact BCSs).</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on February 17, 2017, when the Entity included all BES assets containing low impact BCSs in its BES asset list.</p> <p>The root cause of this noncompliance was a procedural deficiency. The procedures did not provide for proper assessment, communication, reviews, and approvals necessary to determine BES assets that contain low impact 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. By not identifying each asset containing a low impact BCS, the Entity could have missed providing required security measures and controls. However, this oversight was a documentation error due to the signing of a list that was incomplete, and not an operational failure where sites were left unsecured. The duration of the noncompliance was approximately seven-and-a-half months, meaning that the noncompliance was discovered well in advance of the annual 15-month required review period. Additionally, the misclassified facilities were commissioned between the date of the original list of facilities containing low impact BCS and the date of discovery; thus, the facilities were not misclassified when they were commissioned. The Entity maintains that all personnel knew the affected facilities contained only low impact BCSs, so the required awareness and actions were in place. 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) completed an extent of condition analysis to verify all BES assets containing low-impact BES Cyber Assets have been included in the Entity's BES asset list; and 2) updated the current procedures to ensure that (i) the revised procedures provide for proper assessment, communication, reviews, and approvals necessary to determine BES assets that contain low impact BCAs; (ii) the BES asset list is updated to include new BES assets prior to their being placed in service; and (iii) the BES asset list is properly maintained to reflect changes to the BES. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017017014	CIP-010-2	R2, Part 2.1	██████████	██████████	08/05/2016	04/01/2017	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 ██████████, prior to a Compliance Audit, ██████████ submitted a Self-Report stating that as a ██████████, it was in noncompliance with CIP-010-2 R2, Part 2.1. On ██████████, following the completion of the Compliance Audit, ██████████ additional information stating that, as a ██████████, it was in noncompliance with CIP-010-2, Part 2.1 for the same reasons stated in the Self-Report. Specifically, ██████████ failed to monitor at least every 35 calendar days for changes to the baseline configuration.</p> <p>During the transition to NERC CIP Version 5 Reliability Standards, ██████████ was using two separate methods for compliance with CIP-010-2 R2. One method was successful in meeting compliance with the Standard for the majority of ██████████ Cyber Assets. The second method was used for a subset of Cyber Assets ██████████ and was successful in developing baselines and authorizing changes; however, it created voluminous reports that were hundreds of pages long. As a result, ██████████ was unable to monitor at least every 35 calendar days for changes to the baseline configuration for applicable Cyber Assets.</p> <p>The root cause of this noncompliance was an insufficient process to ensure compliance with CIP-010-2 R2 Part 2.1. During the transition to the NERC CIP Version 5 Reliability Standards, ██████████ ██████████.</p> <p>This noncompliance started on August 5, 2016, which is 36 calendar days following July 1, 2016 when CIP-010-2 R2 became mandatory and enforceable. The noncompliance ended on April 1, 2017 when ██████████.</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 upon the following factors. First, during the Compliance Audit, ██████████ demonstrated that it has processes in place to comprehensively address all of the requirements of CIP-010-2 R2. Second, during the Compliance Audit it was confirmed that ██████████ ██████████ as required by CIP-010-2 R1, Part 1.2. Third, the noncompliance was discovered within one month of the enforcement date of the Standard, and ██████████ quickly took steps to investigate and resolve the issue. Fourth, ██████████.</p> <p>No harm is known to have occurred.</p> <p>Texas RE considered ██████████ compliance history and determined there were no relevant instances of noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, ██████████:</p> <ol style="list-style-type: none"> 1) implemented a new configuration management tool for compliance with CIP-010-2 R2; 2) trained affected personnel on the new configuration management tool; and 3) conducted testing and validation of the new configuration management tool. <p>Texas RE 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
TRE2017017015	CIP-010-2	R1, Parts 1.3 and 1.4	██████████	██████████	07/01/2016	05/31/2017	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 ██████████, prior to a Compliance Audit, ██████████ submitted a Self-Report stating that, as a ██████████, it was in noncompliance with CIP-010-2 R1. On ██████████, following the Compliance Audit, ██████████ submitted additional information stating that, as a ██████████, it was in noncompliance with CIP-010-2 R1 for the same issue identified in the Self-Report. Specifically, ██████████ failed to update existing baseline configurations within 30 calendar days as required by CIP-010-2 R1, Part 1.3. During the subsequent Compliance Audit, Texas RE determined that ██████████, as a ██████████, was in noncompliance with CIP-010-2 R1, Part 1.4. Specifically, ██████████ failed to determine and verify that required cyber security controls were not adversely impacted for changes that deviated from the baseline configuration.</p> <p>For the Part 1.3 Issue, during the transition to the NERC CIP Version 5 Reliability Standards, ██████████ was using two separate methods for compliance with CIP-010-2. One method was successful in meeting compliance with the Standard for the majority of ██████████ Cyber Assets. The second method was used for a subset of Cyber Assets ██████████ and was successful in developing baselines and authorizing changes; however, it created voluminous reports that were hundreds of pages long for each Cyber Asset. As a result, baseline configurations were updated but ██████████ was unable to determine whether baseline configurations were updated within 30 days following a change as required by CIP-010-2 R1, Part 1.3. For the CIP-010-2 R1, Part 1.4 issue, ██████████ personnel were conducting the required reviews to determine the required cyber security controls that could be impacted by a change that deviates from an existing baseline configuration and verifying the controls are not adversely affected. However, personnel did not consistently document the verification results, resulting in noncompliance for ██████████.</p> <p>The root cause of this noncompliance was insufficient processes and controls to ensure compliance with CIP-010-2 R1, Parts 1.3 and 1.4. During the transition to the NERC CIP Version 5 Reliability Standards, ██████████ ██████████ as required by CIP-010-2 R1, Part 1.3. Additionally, ██████████ implemented a process to verify security controls for authorized changes as required by CIP-010-2 R1, Part 1.4; however, ██████████ lacked a control to ensure documentation of the verification.</p> <p>This noncompliance started on July 1, 2016, when CIP-010-2 R1 became enforceable, and the noncompliance ended on May 31, 2017, when ██████████ ██████████.</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, during the Compliance Audit, ██████████ demonstrated that it has documented processes in place to address all of the requirements of CIP-010-2 R1. Second, during the Compliance Audit, it was confirmed that ██████████ ██████████ as required by CIP-010-2 R1, Part 1.2. Third, the noncompliance related to failing to timely update baseline configurations was discovered within six weeks of the enforcement date of the Standard. This demonstrates that ██████████ had sufficient detective controls in place to monitor compliance. Further, after identifying the noncompliance, ██████████ quickly took steps to investigate and resolve the issue. Lastly, ██████████ ██████████.</p> <p>No harm is known to have occurred.</p> <p>Texas RE considered ██████████ compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, ██████████:</p> <ol style="list-style-type: none"> 1) implemented a new configuration management tool; 2) trained affected personnel on the new configuration management tool; 3) conducted testing and validation of the new configuration management tool; and 4) revised its security controls checklist, implemented a new process to ensure change tickets are not closed until the complete checklist is attached, and updated the relevant procedure and distributed it to affected personnel. <p>Texas RE 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
TRE2017017016	CIP-007-6	R5, Part 5.4	[REDACTED]	[REDACTED]	07/01/2016	09/15/2016	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 [REDACTED], prior to a Compliance Audit, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5, Part 5.4. Specifically, [REDACTED] failed to change known default passwords, per Cyber Asset capability.</p> <p>Prior to the July 1, 2016 enforcement date for CIP-007-6, [REDACTED] identified and documented the third account level as a default and shared account; however, [REDACTED]. On September 13, 2016, during a conversation between personnel, [REDACTED] discovered that documentation had been found stating that the default passwords at issue could be changed. [REDACTED] immediately took steps to change the default password at issue, and completed the change within two days.</p> <p>The root cause of this noncompliance was an [REDACTED]. To prevent recurrence of this noncompliance, [REDACTED]</p> <p>This noncompliance started on July 1, 2016, when CIP-007-6 became enforceable, and ended on September 15 2016, when [REDACTED]</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 duration of the noncompliance was relatively short, less than three months, and once discovered [REDACTED] acted immediately to end the noncompliance within two days. Second, for the [REDACTED] Third, the [REDACTED] Lastly, the [REDACTED]</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) changed the default password for all impacted Cyber Assets; 2) revised its procedures to ensure that the [REDACTED] and personnel are instructed to change the default password; and 3) [REDACTED] <p>Texas RE 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
TRE2017017019	CIP-007-6	R3, Part 3.3	[REDACTED]	[REDACTED]	07/05/2016	11/17/2016	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>[REDACTED], prior to a Compliance Audit, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-007-6 R3. Specifically, [REDACTED], as required by CIP-007-6 R3, Part 3.3.</p> <p>Prior to CIP-007-6 becoming enforceable on July 1, 2016, [REDACTED]. Also prior to July 1, 2016, [REDACTED] determined that after updating signatures and patterns, system reliability was impacted so the antivirus software was disabled pending reconfiguration. The employee responsible for implementing the antivirus software was reassigned and the reconfiguration and re-enabling of the antivirus software was overlooked prior to the enforcement date of CIP-007-6 on July 1, 2016. On August 10, 2016, [REDACTED] discovered this issue when the employee re-assigned to manage the antivirus software conducted a review. Following discovery of the issue, [REDACTED]. Once everything was properly configured in the non-production environment, the appropriate changes were applied to the production environment on November 17, 2016. [REDACTED]</p> <p>The root cause of this noncompliance was the lack of a control to ensure signature reports are initiated weekly, as required by [REDACTED] documented process. [REDACTED]. For this noncompliance, [REDACTED], and [REDACTED] to comply with its written process.</p> <p>This noncompliance started on July 5, 2016, when the first weekly antivirus report was due to be issued, and ended on November 17, 2016, when the missing signatures were tested and installed.</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 noncompliance was relatively short – less than five months. Second, during the Compliance Audit Texas RE determined that [REDACTED] implemented a process to update signatures, including the testing and installation of signatures and found no additional instances of noncompliance with CIP-007-6 R3, Part 3.3. Third, [REDACTED]. 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) reconfigured the servers so that issuance of the weekly signature report resumed, and missed signatures were tested and installed; 2) implemented a reporting system that monitors signatures and will report within 24 hours when a signature is out of date; 3) created service requests to monitor and track definitions to ensure there were no additional instances of noncompliance; and 4) conducted a periodic check of signature updates. <p>Texas RE 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
TRE2017017023	CIP-007-3a	R6, Parts 6.1, 6.2, and 6.5	██████████	██████████	03/09/2016	05/17/2016	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>██████████, prior to a Compliance Audit, ██████████ submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-007-3a R6.1 and R6.5. Specifically, ██████████. Additionally, Texas RE determined that ██████████ was in noncompliance with CIP-007-3a R6.2 for its security monitoring controls failing to issue automated or manual alerts for detected Cyber Security Incidents.</p> <p>Prior to the transition to NERC Reliability CIP Version 5 Standards, ██████████. During this time, the new security event monitoring system was in limited use and administrators were learning to install and configure the system. The issue was discovered on April 20, 2016, when a contractor employed by ██████████ identified the issue following a review of logs. ██████████. Although logs were maintained locally, they were not reviewed before being deleted following the 90-day retention period required by CIP-007-3a R6.4. Additionally, ██████████, as required by CIP-007-3a R6.2.</p> <p>The root cause of this noncompliance was that ██████████. During the transition to NERC Reliability Version 5 Standards, ██████████. Although ██████████ had a process in place for monitoring system events related to cyber security, ██████████.</p> <p>This noncompliance started on March 9, 2016, ██████████, and ended on May 17, 2016, ██████████.</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 duration was short – approximately two months. Second, the issue impacted ██████████ that would not adversely affect the BES within 15 minutes of being rendered unavailable, degraded, or misused. Third, ██████████. Fourth, there were no Reportable Cyber Security incidents during the time period at issue. Lastly, ██████████ employs defense in depth measures.</p> <p>No harm is known to have occurred.</p> <p>Texas RE considered ██████████ compliance history and determined there were no relevant instances of noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, ██████████:</p> <ol style="list-style-type: none"> 1) ██████████; 2) ██████████. <p>Texas RE has verified completion of 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
TRE2017017707	CIP-003-3	R4; R4.1	[REDACTED]	[REDACTED]	11/17/2015	01/12/2016	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 06, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] ([REDACTED] it was in noncompliance with CIP-003-3 R4. Specifically, [REDACTED] failed to implement its documented program to protect information associated with Critical Cyber Assets, in particular Critical Cyber Asset lists, as required by CIP-003-3 R4.1.</p> <p>[REDACTED] had a documented information protection program ("program") that detailed the process to identify, classify, and protect information associated with Critical Cyber Assets. According to [REDACTED] program, information associated with Critical Cyber Assets was [REDACTED]. Further, [REDACTED].</p> <p>On 11/17/2015, as part of [REDACTED] CIP Version 5 transition project, a project team member sent an email with a spreadsheet attached that contained Critical Cyber Asset information to the entire project team. The project team was working on [REDACTED] [REDACTED] and the spreadsheet contained a list of BES Assets, BES Cyber Systems, and BES Cyber Assets, including classifications and other pertinent information. On 01/12/2016, during a team training and discussion regarding information protection, an IT Manager was made aware that personnel had been sent information associated with Critical Cyber Assets via email. It was determined that [REDACTED] individuals that received the email did not have authorized access for [REDACTED] [REDACTED] information. After being made aware of the issue on 01/12/2016, the IT Manager instructed personnel to delete the email.</p> <p>The root cause of this noncompliance was insufficient awareness and training to comply with requirements to protect information associated with Critical Cyber Assets.</p> <p>The noncompliance started on 11/17/2015 when the email containing information associated with Critical Cyber Assets was sent to unauthorized personnel. The noncompliance ended on 01/12/2016 when personnel were instructed to delete the email. The duration of the 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. The risk of this issue is minimal based on the following factors. First, while the Critical Cyber Asset information was shared with individuals without authorized access, the information was only sent to internal [REDACTED] email addresses and was not shared externally. This reduces the likelihood that the information would be used to compromise [REDACTED] systems. Second, [REDACTED] has [REDACTED]. Lastly, the duration of the issue was short, lasting approximately two (2) months.</p> <p>No harm is known to have occurred.</p> <p>Texas RE determined that [REDACTED] compliance history should not serve as a basis for aggravating the risk.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) instructed all project team members to delete the email; 2) sent an email reminder enforcing [REDACTED] guidelines for how to handle protected information, including guidelines on sharing protected information via email; 3) updated information protection training content; and 4) released updated information protection training. <p>Texas RE 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
TRE2017018092	CIP-004-6	R4; Parts 4.1 and 4.4	[REDACTED]	[REDACTED]	07/01/2016	03/09/2018	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 August 01, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] [REDACTED] it had an instance of noncompliance with CIP-004-6 R4. [REDACTED] subsequently reported three additional instances of noncompliance with CIP-004-6 R4 for a total of four instances of noncompliance. Upon further investigation, Texas RE determined that [REDACTED] was in noncompliance with CIP-004-6 R4 in only three instances.</p> <p>In the first instance, on June 08, 2017, an administrator working on a break/fix issue created a test account and provisioned it access [REDACTED] without first submitting an access request and obtaining approval, as required by [REDACTED] documented process for CIP-004-6 R1, Part 4.1. [REDACTED]. On June 09, 2017, [REDACTED] discovered the issue. The administrator removed the test account [REDACTED] group that same day.</p> <p>For the first instance, the noncompliance started on June 08, 2017 when the test account was provisioned access [REDACTED]. The noncompliance ended on June 09, 2017 when test account was removed [REDACTED]. The duration of the noncompliance was one day.</p> <p>In the second instance, on September 07, 2016, an employee was reviewing system permissions and discovered that [REDACTED] employees did not have authorization records for access privileges to a [REDACTED] classified as an EACMS, as required by CIP-004-6 R4, Part 4.1. The [REDACTED] had been classified as an EACMS as part of [REDACTED] transition to CIP Version 5. The [REDACTED] employees had been granted access [REDACTED] prior to CIP Version 5 and [REDACTED] being onboarded into [REDACTED] access management system. After the [REDACTED] was onboarded into the access management system, access was configured to be provisioned [REDACTED] and access was requested for existing users so there were authorization records on file. For the [REDACTED] employees who had [REDACTED] access, [REDACTED] did not have authorization records. After discovery of the issue, access requests were entered in the access management system for the [REDACTED] employees. Access was approved for [REDACTED] employees, with the last approval obtained on September 22, 2016. Access was rejected and removed for [REDACTED] employees, with the last removal completing on September 26, 2016.</p> <p>For the second instance, the noncompliance started on July 01, 2016 when CIP-004-6 R4 became mandatory and enforceable. The noncompliance ended on September 26, 2016 when access was rejected and removed for the last impacted employee. The duration of the noncompliance was less than three months.</p> <p>In the third instance, on October 13, 2016, [REDACTED] discovered that it had not included its [REDACTED] application as a designated storage location of BES Cyber System Information in its access management system as part of its CIP Version 5 transition. As a result, [REDACTED] did not implement a process to authorize access based on need for the application, as required by CIP-004-6 R4, Part 4.1. Further, [REDACTED] failed to timely perform a verification that access privileges are correct and are those that [REDACTED] determined are necessary for performing assigned work functions, as required by CIP-004-6 R4, Part 4.4. On December 06, 2017, [REDACTED] onboarded the application into its access management system as designated storage location of BES Cyber System Information, thereby implementing a process to authorize access based on need. On March 09, 2018, [REDACTED] completed a review to verify access privileges are correct and are those that [REDACTED] determined are necessary for performing assigned work functions.</p> <p>For the third instance, the noncompliance started on July 01, 2016 when CIP-004-6 R4 became mandatory and enforceable. The noncompliance ended on March 09, 2018 when [REDACTED] completed a review to verify access privileges are correct and are those that [REDACTED] determined are necessary for performing assigned work functions. The duration of the noncompliance was approximately 20 months.</p> <p>The root cause of the noncompliance is insufficient processes and controls to ensure that access is properly managed. In regards to the first incident, administrators need the ability to simulate test accounts with lower access privileges in order to diagnose and fix issues and [REDACTED] process did not account for this. In regards to the second instance, [REDACTED] lacked a consistent method to provision access. In regards to the second and third instances, gaps existed in the process of implementing access management controls for systems that were being brought into CIP scope as part of the transition to CIP Version 5. The impacted business unit's change management process and associated forms and templates did not include a review and consideration of impacts to access when a Cyber Asset or BES Cyber System Information repository is added, changed, or removed. As a result, during the CIP Version 5 transition, access was not appropriately onboarded in the access management system and included in the required access management processes and controls.</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 was minimized by the following factors. In all instances, employees with access to the impacted systems had completed cyber security training and had a Personnel Risk Assessment (PRA) on file. For the first instance, the duration was short, lasting one day. Further, for the first instance, two-factor authentication was required to access any systems to which membership in the [REDACTED] provided access and the test account was not</p>					

	<p>provided the second factor. Therefore, the test account was not able to access any critical systems. For the second instance, the duration was also short, lasting less than three months. For the third instance, the noncompliance was limited to the application-level as access to the system at the Cyber Asset-level was being appropriately controlled for EACMS Cyber Assets. Further, for the third instance, the only users permitted to access the system for the duration of the noncompliance were employees who required access to support the [REDACTED] process.</p> <p>No harm is known to have occurred.</p> <p>Texas RE considered [REDACTED] compliance history and determined there were relevant instances of noncompliance. However, [REDACTED] compliance history should not serve as a basis for aggravating the risk as the prior noncompliance involved different facts and root cause.</p>
<p>Mitigation</p>	<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) corrected the first instance; 2) corrected the second instance; 3) corrected the third instance; 4) performed an extent of condition review; 5) updated the [REDACTED]; 6) implemented a process to ensure consistent provisioning of access [REDACTED]; 7) implemented a [REDACTED] and 8) implemented a [REDACTED]. <p>Texas RE has verified 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																
WECC2017018482	CIP-004-6	R5: P5.5	[REDACTED]	[REDACTED]	10/2/2016	7/3/2017	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 October 10, 2017, the entity submitted a Self-Report stating, as a [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED], it was in noncompliance with CIP-004-6 R5. Specifically, on June 12, 2017, while completing a compliance review, the entity discovered three instances in which it did not change passwords for shared accounts within 30 calendar days of the termination action. These instances included three employees who had administrative access to shared accounts on an RSA SecureID and an Intrusion Detection System, both classified as Electronic Access Control or Monitoring Systems (EACMS), associated with the High Impact Bulk Electric (BES) Cyber System (HIBCS). The entity utilized an automated process which changed the shared account passwords on these EACMS every few months. However, terminations required the shared account passwords be changed manually and while the entity had a checklist in place for employee terminations, it did not have a section for changing shared account passwords manually. The employees responsible for doing so were not aware of this and therefore, assumed the automated process would change the passwords.</p> <p>After reviewing all relevant information, WECC determined the entity failed, in three separate instances, to change passwords for shared accounts known to the user within 30 calendar days of the termination action, on two EACMS associated with the HIBCS, as required by CIP-004-6 R5 Part 5.5.</p> <p>The root cause of the issue was a less than adequate process for changing passwords for shared accounts timely after a termination action. Specifically, the entity had a checklist for employee terminations, but that checklist did not have a touchpoint for the compliance requirement of CIP-004-6 R5 Part 5.5. Additionally, the roles and responsibilities of employees charged with changing passwords was not clearly defined and understood.</p> <p>This noncompliance started when the shared account passwords were not changed as required by CIP-004-6 R5 Part 5.5, and ended when the shared account passwords were changed. The start and end dates of each instance are as described below:</p> <table border="1" data-bbox="969 1003 1759 1185"> <thead> <tr> <th>Instance</th> <th>Start Date</th> <th>End Date</th> <th>Duration (days)</th> </tr> </thead> <tbody> <tr> <td>One</td> <td>10/2/2016</td> <td>1/3/2017</td> <td>94</td> </tr> <tr> <td>Two</td> <td>3/26/2017</td> <td>4/6/2017</td> <td>12</td> </tr> <tr> <td>Three</td> <td>5/7/2017</td> <td>7/3/2017</td> <td>58</td> </tr> </tbody> </table>						Instance	Start Date	End Date	Duration (days)	One	10/2/2016	1/3/2017	94	Two	3/26/2017	4/6/2017	12	Three	5/7/2017	7/3/2017	58
Instance	Start Date	End Date	Duration (days)																					
One	10/2/2016	1/3/2017	94																					
Two	3/26/2017	4/6/2017	12																					
Three	5/7/2017	7/3/2017	58																					
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 entity failed, on three separate instances, to change passwords for shared accounts known to the user within 30 calendar days of the termination action on two EACMS associated with the HIBCS, as required by CIP-004-6 R5 Part 5.5. However, the entity implemented strong compensating controls. Specifically, for each terminated employee, unescorted physical access, Interactive Remote Access, and access to BES Cyber System Information was removed the day of termination; thereby removing their ability to access the HIBCS and any associated Cyber Assets or its information. Additionally, the entity disabled all of their corporate Active Directory (AD) user account access. No harm is known to have occurred.</p> <p>The entity does not have any relevant CIP-004-6 R5 compliance history.</p>																					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> changed the shared account passwords on both EACMS; and updated its process to include an off-boarding checklist which includes a list of various accesses that must be removed when an employee ends their employment through resignation, retirement, termination, or transfer. This checklist also includes steps for changing passwords on shared accounts. The individuals who created the checklist are also the individuals who perform the actions, so no formal training was performed. <p>WECC 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
WECC2017018877	CIP-002-5.1	R2: P2.1; P2.2	[REDACTED]	[REDACTED]	7/1/2016	12/27/2017	Self-Report	Completed 6/1/2018
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 December 21, 2017, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-002-5.1 R2. Specifically, the entity reported that it conducted a compliance review and discovered that although it had implemented and performed the initial process required by CIP-002-5.1 R1 to review its candidate Bulk Electric System (BES) Assets and identify the assets that contained its Low Impact BES Cyber System (LIBCS) by the mandatory and enforceable date of July 1, 2016, it did not have evidence that its CIP Senior Manager reviewed and approved the initial identifications of its assets that contained LIBCS by July 1, 2016, as required by CIP-002-5.1 P2.2. At the time of this Self-Report, the entity had not yet performed any subsequent reviews of its candidate BES Assets or its list of assets that contained LIBCS as the CIP Senior Manager was out of the office.</p> <p>After reviewing all relevant information, WECC determined that the entity failed to have its CIP Senior Manager approve the initial identifications required by R1, as required by CIP-002-5.1 R2 Part 2.2 by the mandatory and enforceable date of July 1, 2016. In addition, the entity also failed to review the identifications in R1 and its parts (and update them if there were changes identified) at least once every 15 calendar months, even if it had no identified items in R1 and have its CIP Senior Manager approve the identifications required by R1 at least once every 15 calendar months, even if it had no identified items in R1, as required by CIP-002.5.1 R2 Part 2.1 and Part 2.2.</p> <p>The root cause of the violation was a lack of management follow up or monitoring of activities not identifying problems. Specifically, the entity's management follow-up and monitoring of compliance activities did not identify that there were no processes in place to ensure that CIP-002-5.1 compliance obligations are met.</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable for the entity, and ended on December 27, 2017, when the entity met the requirements of R2, for a total of 545 days.</p>					
Risk Assessment			<p>This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to have its CIP Senior Manager approve the initial identifications required by R1, as required by CIP-002-5.1 R2 Part 2.2. In addition, the entity also failed to review the identifications in R1 and its parts (and update them if there were changes identified) at least once every 15 calendar months, even if it had no identified items in R1 and have its CIP Senior Manager approve the identifications required by R1 at least once every 15 calendar months, even if it had no identified items in R1, as required by CIP-002.5.1 R2 Part 2.1 and Part 2.2.</p> <p>The two [REDACTED] inside the control house were [REDACTED]. These devices are also isolated from the generation network. In addition, the assets identified in R1 were correctly identified as containing only LIBCS. However, no other controls were identified that could have effectively prevented or detected this noncompliance. No harm is known to have occurred.</p> <p>WECC notes that the entity does not have any relevant previous violations of this or similar Standards and Requirements.</p>					
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none"> 1) conducted a review of its candidate BES Assets and list of assets containing LIBCS and obtained the approval of the CIP Senior Manager; 2) included CIP-002 BES Cyber System approval status and next date for review in its monthly compliance report; and 3) scheduled the periodic review for 12 calendar months rather than 15 calendar months. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020556	CIP-004-6	R4: P4.1; P4.1.2	[REDACTED]	[REDACTED]	6/6/2018	9/18/18	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 violation.)			<p>On October 19, 2018, the entity submitted a [REDACTED] stating that, as a [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED], it was in noncompliance with CIP-004-6 R4. Specifically, the entity moved into new corporate headquarters in November of 2017, which led to a significant increase in the number of keys to consider for hard-key management. On September 18, 2018, the entity completed a quarterly audit of physical hard keys and discovered that on June 6, 2018, one contractor was given a hard-key to access the entire key inventory cabinet without going through the correct authorization process. This contractor was given the hard-key to assist with the significant key management duties. The cabinet included keys to the Physical Security Perimeters (PSPs) access points containing Cyber Assets associated with [REDACTED] High Impact Bulk Electric System (BES) Cyber Systems (HIBCS) and [REDACTED] Medium Impact BES Cyber System with External Routable Connectivity (ERC). The root cause of the issue was the process not being followed correctly. Specifically, the employee responsible for granting hard-key access assumed that the contractor had authorization for the hard-key to the cabinet because they had authorized unescorted physical access via electronic card key to [REDACTED] HIBCS PSPs for janitorial purposes.</p> <p>After reviewing all relevant information, WECC determined the entity failed to appropriately implement its documented access management process for unescorted physical access to a PSP, as required by CIP-004-6 R4 Part 4.1 Sub-Part 4.1.2.</p> <p>This noncompliance started on June 6, 2018, when a contractor was given unauthorized unescorted physical access to [REDACTED] HIBCS PSP and [REDACTED] MIBCS PSPs, and ended on September 18, 2018, when the key was taken from the contractor and the unauthorized unescorted physical access to the [REDACTED] PSPs was thereby removed, for a total of 105 days.</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. In this instance, the entity failed to appropriately implement its documented access management process for unescorted physical access to a PSP, as required by CIP-004-6 R4 Part 4.1 Sub-Part 4.1.2. The entity had weak preventive controls but good detective controls which caught the issue very timely. As further compensation, the contractor was already authorized for unescorted physical access with an electronic card key to [REDACTED] of the HIBCS PSPs, had completed CIP training and had a valid Personnel Risk Assessment. Additionally, there were no reports of any PSPs sounding a forced door alarm as a result of a hard key being used to gain entry, therefore it was concluded that the hard-key was not used while in the contractor's possession. No harm is known to have occurred.</p> <p>WECC considered the entity's compliance history in its designation of this remediated issue as a CE. The entity's prior compliance history with CIP-004 R4 includes NERC Violation IDs [REDACTED], [REDACTED], and [REDACTED].</p> <p>Regarding [REDACTED], the entity failed to review its electronic access list for supervisory control and data acquisition. Regarding [REDACTED], the entity failed to update its access list within seven days of a personnel change. Therefore, WECC determined that these violations were distinct, separate, and not relevant to the issue in this CE.</p> <p>WECC determined NERC Violation ID [REDACTED] to be relevant because the root cause of that issue was similar to the root cause of this CE however, it 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) removed the unauthorized access to the [REDACTED] PSPs by collecting the hard-key from the contractor; and 2) provided additional training on the access request and authorization process to the all employees responsible for granting said access. <p>WECC has verified the completion of all mitigation activity.</p>					

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC)

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
WECC2018019943	CIP-004-6	R5 P5.1			3/18/2018	3/21/2018	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 violation.)			<p>On June 28, 2018 the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. Specifically, an employee retired with an effective date of March 17, 2018. The entity initiated the removal of the employee's ability for unescorted physical access to a Medium Impact BES Cyber Systems (MIBCS) on March 16, 2018 by collecting their badge card key and substation access keys; however, it did not complete the removal of the individuals' ability to physically access the MIBCS until March 21, 2018 which was not within 24 hours of the termination action.</p> <p>The root cause of this issue was based on reduced staffing, working off a backlog of work tickets resulting in the completion of access removals falling outside of the required 24-hour timeframe.</p> <p>After reviewing all relevant information, WECC determined the entity failed to complete the removal of an employee's ability for unescorted physical access within 24-hours of a termination action as required by CIP-004-6 R5 Part 5.1.</p> <p>This issue began on March 18, 2018 when the removal of the employee's ability for unescorted physical access should have been completed and ended on March 21, 2018 when it completed the individuals' ability to physically access a MIBCS, for a total of four days.</p>					
Risk Assessment			<p>WECC determined 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, the entity failed to complete the removal of an employee's ability for unescorted physical access within 24-hours of a termination action as required by CIP-004-6 R5 Part 5.1.</p> <p>The entity had implemented strong preventive controls in the form of documented processes for initiating the removal of unescorted physical access; however, due to staffing issues it was not able to complete the removals timely. Additionally, its detective controls included a weekly report review which is how this issue was discovered. The employee whose access removal was in process did not attempt to physically gain access. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty as the root cause and fact patterns of this issue are separate and distinct from the entity's prior CIP-004-6 R5 noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed removal of unescorted physical access for the employee in scope; 2) implemented the use of alarm monitoring system (AMS) personnel for weekend and holiday coverage of access revocation; 3) hired one additional personnel to provide 75 percent of their time to support the access revocation program; 4) allocated an existing resource to assist with access revocation; and 5) updated three access revocation documents to include the new processes and personnel responsibilities and distributed to applicable personnel. 					

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC)

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
WECC2018020224	CIP-004-6	R5 P5.1			6/12/2018	3/21/2018	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 violation.)			<p>On August 17, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], and [REDACTED] it was in noncompliance with CIP-004-6 R5. Specifically, an employee resigned with an effective date of June 11, 2018. The entity initiated the removal of the employee's ability for unescorted physical access to a Medium Impact BES Cyber System (MIBCS) on June 8, 2018; however, it did not complete the removal of the employee's ability to physically access the MIBCS until June 18, 2018 which was not within 24-hours of the termination action. The root cause of this issue was based on reduced staffing, working off a backlog of work tickets resulting in the completion of access removals falling outside of the required 24-hour timeframe. After reviewing all relevant information, WECC determined the entity failed to complete the removal of an employee's ability for unescorted physical access within 24-hours of a termination action as required by CIP-004-6 R5 Part 5.1. This issue began on June 12, 2018 when the removal of the employee's ability for unescorted physical access should have been completed and ended on June 18, 2018 when it completed the employee's ability to physically access a MIBCS, for a total of four days.</p>					
Risk Assessment			<p>WECC determined 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, the entity failed to complete the removal of an employee's ability for unescorted physical access within 24-hours of a termination action as required by CIP-004-6 R5 Part 5.1.</p> <p>The entity had implemented strong preventive controls in the form of documented processes for initiating the removal of unescorted physical access; however, due to staffing issues it was not able to complete the removals timely. Additionally, its detective controls included a weekly report review which is how this issue was discovered. The employee whose access removal was in process did not attempt to physically gain access. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty as the root cause and fact patterns of this issue are separate and distinct from the entity's prior CIP-004-6 R5 noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed removal of unescorted physical access for the employee in scope; 2) implemented the use of alarm monitoring system (AMS) personnel for weekend and holiday coverage of access revocation; 3) hired one additional personnel to provide 75 percent of their time to support the access revocation program; 4) allocated an existing resource to assist with access revocation; and 5) updated three access revocation documents to include the new processes and personnel responsibilities and distributed to applicable personnel. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020715	CIP-004-6	R5 P5.1	[REDACTED]	[REDACTED]	7/28/2018	8/1/2018	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 violation.)			<p>On November 16, 2018 the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. Specifically, an employee retired with an effective date of July 27, 2018. The entity initiated the removal of the employee's ability for unescorted physical access and Interactive Remote Access (IRA) on July 27, 2018 by collecting the badge which was a [REDACTED] High Impact BES Cyber Systems (HIBCS); however, did not complete the removal of the employee's ability for unescorted physical access to its HIBCS and Medium Impact BES Cyber Systems (MIBCS) until August 1, 2018 which was not within 24-hours of the termination action.</p> <p>The root cause of this issue was based on reduced staffing, working off a backlog of work tickets resulting in the completion of access removals falling outside of the required 24-hour timeframe.</p> <p>After reviewing all relevant information, WECC determined the entity failed to complete the removal of the employee's ability for unescorted physical access within 24-hours of a termination action as required by CIP-004-6 R5 Part 5.1.</p> <p>This issue began on July 28, 2018 when the removal of the employee's ability for unescorted physical access should have been completed and ended on August 1, 2018 when it completed the employee's ability to physically access its HIBCS and MIBCS, for a total of five days.</p>					
Risk Assessment			<p>WECC determined 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, the entity failed to complete the removal of the employee's ability for unescorted physical access within 24-hours of a termination action as required by CIP-004-6 R5 Part 5.1.</p> <p>The entity had implemented strong preventive controls in the form of documented processes for initiating the removal of unescorted physical and IRA access; however, due to staffing issues it was not able to complete the removals timely. In this instance, the employee whose access removal was in process did not attempt to physically or electronically gain access. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty as the root cause and fact patterns of this issue are separate and distinct from the entity's prior CIP-004-6 R5 noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed removal of unescorted physical access for the employee in scope; 2) implemented the use of alarm monitoring system (AMS) personnel for weekend and holiday coverage of access revocation; 3) hired one additional personnel to provide 75 percent of their time to support the access revocation program; 4) allocated an existing resource to assist with access revocation; and 5) updated three access revocation documents to include the new processes and personnel responsibilities and distributed to applicable personnel. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019243	CIP-002-5.1	R2	[REDACTED]	[REDACTED]	9/29/2016	1/8/2018	Self-Report	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>On February 22, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-002-5.1 R2. Specifically, the entity completed the initial performance of CIP-002-5.1 R2 Parts 2.1 and 2.2 [REDACTED]. The entity should have performed the initial review and obtained CIP Senior Manager approval by its applicable registration date. The entity had [REDACTED] identified and subject to the review and approval.</p> <p>After reviewing all relevant information, WECC determined the entity failed to perform the initial review and obtain CIP Senior Manager approval of the initial identifications in Requirement R1 and its parts, as required by CIP-002-5.1 R2 Part 2.1 and Part 2.2, by the date of its registration.</p> <p>The root cause of the issue was based on a reassignment of the required tasks and a misunderstanding of the Standard and Requirement. Specifically, the entity had reassigned the CIP Senior Manager role to an individual who believed they had 15 calendar months from the date of its registration as a [REDACTED] to complete CIP-002-5.1a R2 Parts 2.1 and 2.2 and did not interpret the initial performance of the review and approval as being required prior to or by its registration as a [REDACTED].</p> <p>This issue began on September 29, 2016, when the initial performance should have been completed, and ended on January 8, 2018, when the entity completed Parts 2.1 and 2.1, for a total of 467 days.</p>					
<p>Risk Assessment</p>			<p>WECC determined 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, the entity failed to perform the initial review and obtain CIP Senior Manager approval of the initial identifications in Requirement R1 and its parts, as required by CIP-002-5.1 R2 Part 2.1 and Part 2.2, by the date of its registration.</p> <p>The entity had no controls in place to detect or prevent this issue; however, the entity had only [REDACTED] in scope of this issue. No harm is known to have occurred.</p> <p>The entity has no compliance history with this Standard and Requirement.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> performed a review of the identifications in Requirement R1; obtained CIP Senior Manager approval of those identifications; educated the new CIP Senior Manager to the correct timeline expectations of the Requirements; and created a task as a reminder for the new CIP Senior Manager to conduct recurring CIP-002-5.1a R2 reviews and approval <p>WECC has verified the completion of all mitigation activity.</p>					

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 Exception 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	MRO2018019235	Yes		Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 years
2	MRO2018020298			Yes	Yes					Yes				Category 2 – 12: 2 years
3	MRO2018020840			Yes	Yes								Yes	Category 2 – 12: 2 years
4	SPP2018019319			Yes	Yes								Yes	Category 2 – 12: 2 years
5	MRO2018020850			Yes	Yes									Category 2 – 12: 2 years
6	MRO2018020839			Yes	Yes									Category 2 – 12: 2 years
7	MRO2018020836	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
8	MRO2018020795	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
9	MRO2018020801			Yes	Yes									Category 2 – 12: 2 years
10	MRO2018020292			Yes	Yes									Category 2 – 12: 2 years
11	NPCC2017016902			Yes	Yes									Categories 3 – 4: 2 year
12	NPCC2017016905	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
13	NPCC2017017113		Yes	Yes	Yes									Category 2 – 12: 2 years
14	NPCC2017018778	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
15	NPCC2018018910		Yes	Yes	Yes				Yes					Category 2 – 12: 2 years
16	NPCC2018019288		Yes	Yes	Yes									Category 2 – 12: 2 years
17	NPCC2018019726		Yes	Yes	Yes									Category 2 – 12: 2 years
18	NPCC2018019894		Yes	Yes	Yes									Category 2 – 12: 2 years
19	NPCC2018020279		Yes	Yes	Yes				Yes					Category 2 – 12: 2 years
20	RFC2018020608	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
21	RFC2018020430	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
22	RFC2018020431	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
23	RFC2018020253	Yes		Yes	Yes			Yes	Yes					Category 1: 3 years; Category 2-12: 2 years
24	RFC2018019898	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
25	RFC2018019878	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2-12: 2 years
26	RFC2018020255	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
27	RFC2018020029	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
28	RFC2018020208	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; 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)
29	RFC2018019903	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
30	RFC2018020741	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
31	TRE2017017809	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
32	TRE2017018030	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
33	TRE2017016876	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
34	WECC2017017871	Yes		Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 year
35	WECC2017018751			Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 year
36	WECC2017017876			Yes	Yes				Yes				Yes	Category 1: 3 years; Category 2 – 12: 2 year
37	WECC2017018583			Yes	Yes						Yes		Yes	Category 2 – 12: 2 years
38	WECC2017017878	Yes		Yes	Yes				Yes				Yes	Category 1: 3 years; Category 2 – 12: 2 year
39	WECC2018020339	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
40	WECC2017017301	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
41	WECC2017017302	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
42	WECC2017017305	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
43	WECC2017017294	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; 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
MRO2018019235	CIP-002-5.1	R1	[REDACTED]	[REDACTED]	07/01/2016	08/01/2017	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 January 10, 2018, [REDACTED], submitted a self-log to MRO stating that, [REDACTED], it was in noncompliance with CIP-002-5.1 R1. [REDACTED]. The self-log identified three instances of noncompliance. The noncompliance occurred [REDACTED].</p> <p>In the first instance of noncompliance, during an internal review of ESP diagrams, [REDACTED] discovered RTUs that were not classified as BES Cyber Assets in the BES Cyber Systems documentation. The RTUs were located in the [REDACTED]; the RTUs may have not been classified as Cyber Assets due to a lack of updatable traits. The noncompliance began on July 1, 2016 when the standard became enforceable, and ended on August 1, 2017 when the RTUs were classified as BES Cyber Assets.</p> <p>In the second instance of noncompliance, during the substation's annual cyber vulnerability assessment and inventory, [REDACTED] discovered a Cyber Asset (programmable logic controller) that was not classified as a BES Cyber Asset in the BES Cyber System documentation. The device was located in the [REDACTED]. The noncompliance began on July 1, 2016 when the standard became enforceable, and ended on June 1, 2017 when the device was classified as a BES Cyber Asset.</p> <p>In the third instance of noncompliance, during the substation's annual cyber vulnerability assessment and inventory, [REDACTED] discovered devices that were not classified as BES Cyber Assets in the BES Cyber System documentation. The substation was located in the [REDACTED] states that the devices were located in the substation's 115 kV control house. The noncompliance began on July 1, 2016 when the standard became enforceable, and ended on June 20, 2017 when the devices were classified as BES Cyber Assets.</p> <p>The cause of the noncompliance was [REDACTED] failure to follow its documented procedures regarding classification of certain substation equipment.</p> <p>The noncompliance began on July 1, 2016, when the standard became enforceable, and ended on August 1, 2017, when the BES Cyber System documentation was updated in the first 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. The first instance was minimal because per [REDACTED], the BES Cyber Assets did not have ERC or IRA, [REDACTED], the devices were compliant with the required CIP-007-6 cyber security controls; and could not be connected to via an Ethernet connection; additionally, the devices were in a functioning PSP. The second instance was minimal, because per [REDACTED], the BES Cyber Asset did not have ERC, was located in a functioning PSP, had an up-to-date CIP-10-2 baseline, and was in compliance with the required CIP-007-6 cyber security controls. The third instance was minimal, because per [REDACTED], the BES Cyber Assets were in a functioning PSP, had up-to-date CIP-10-2 baselines, and were mostly compliant with the required CIP-007-6 cyber security controls. [REDACTED] states that one device still had a default password ([REDACTED]). 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 required BES Cyber System documentation; and 2) held meetings and formal training sessions with the substation CIP program team members and impacted SMEs on BES Cyber Asset and ESP categorization and process 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
MRO2018020298	CIP-002-5.1	R1	[REDACTED]	[REDACTED]	7/1/2016	5/30/2018	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 to MRO stating that, [REDACTED], it was in noncompliance with CIP-002-5.1 R1. [REDACTED]. The self-log identified two instances of noncompliance. The noncompliance occurred [REDACTED].</p> <p>In the first instance of noncompliance, [REDACTED] states that its low impact asset list (P1.3) was incorrect. [REDACTED] discovered the noncompliance during the performance of an internal control, specifically, reviewing all shared access at low impact asset substations to support future NERC CIP compliance. [REDACTED] reports there was a jointly owned low impact asset (substation) that was not on the low impact asset list; the substation is located in the [REDACTED]. The cause of the noncompliance was that the design and construction project process did not have sufficient controls to identify new low impact substation assets. The noncompliance began on November 22, 2016, when the asset was placed into service, and ended on April 10, 2018, when the low impact asset list was updated.</p> <p>In the second instance of noncompliance, [REDACTED] states that it failed to identify each medium impact BES Cyber System as required by P1.2. [REDACTED] states that during a cyber vulnerability assessment, it discovered that a relay was not correctly identified during the CIP-002-5 inventorying that occurred during CIP v5 transition. The noncompliance was caused by [REDACTED] not correctly following its documented process. The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on May 30, 2018, when the BES Cyber System documentation was updated.</p> <p>The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on May 30, 2018, when the BES Cyber System documentation was updated in the second 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. The first instance was minimal because the substation was a low impact asset and because per [REDACTED], the noncompliance should not delay its compliance with the low impact requirements related to routable communication and physical security controls. The second instance was minimal, because per [REDACTED], the relay's firmware was up to date and was compliant with the required CIP-007-6 security controls. Additionally, there was no External Routable Connectivity (ERC) or Interactive Remote Access (IRA) to the relay. Finally, [REDACTED] states that the relay was located within a functioning PSP. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <p>To mitigate the first instance of noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) updated the low impact asset list; and 2) updated its process for projects of this type in 2017 to improve interdepartmental information sharing on projects of this type. <p>To mitigate the second instance of noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) updated the BES Cyber System documentation; 2) updated the ESP Diagram; and 3) discussed this incident at a cross-departmental meeting as a lesson learned. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020840	CIP-010-2	R1	[REDACTED]	[REDACTED]	07/11/2018	07/18/2018	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 violation.)			<p>On October 31, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. [REDACTED] states that it failed to perform a security control assessment before applying three patches to one BES Cyber Asset (server) as required by P1.4. [REDACTED] reports that the server was listed in a patching tool that was previously used only to manage non-SCADA assets; however the tool's responsibilities were expanded to manage this server. [REDACTED] states that on July 11, 2018, a patch administrator saw that the server had not been placed in a patching group, moved the server into a test group, and then applied the patches; a different administrator detected the noncompliance the next day.</p> <p>The cause of the noncompliance was weakness in implementing a new process for patching this specific server.</p> <p>This noncompliance started on July 11, 2018, when the patches were applied without the required testing and ended on July 18, 2018, when the patches were removed from the server.</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 only impacted a single BES Cyber Asset. No harm is known to have occurred.</p> <p>MRO reviewed [REDACTED] relevant CIP-010-2 R1 compliance history. [REDACTED] relevant compliance history includes a minimal risk noncompliance of CIP-007-3 R1 that was resolved as a Find, Fix, Track that was mitigated on [REDACTED] and a moderate risk violation of CIP-007-1 R1 that was mitigated on [REDACTED]. 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 there exists a substantial duration of time between the current and prior noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) removed the three applied patches; and 2) moved the server into a dedicated SCADA patching group; the SCADA patching group is configured so that patches are not automatically pushed to its 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
SPP2018019319	CIP-004-6	R3	[REDACTED]	[REDACTED]	01/03/2017	11/28/2017	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 violation.)			<p>On February 28, 2018, [REDACTED] submitted a Self-Certification stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R3. [REDACTED] states that during an internal review by the Security Officer, the Security Officer discovered that an employee had authorized physical access without having a fully complete personnel risk assessment (PRA). Specifically, the employee's PRA did not include a criminal history record check that included prior addresses as required by P3.2.2. [REDACTED] reports that the internal review uncovered a second employee with the same issue.</p> <p>The noncompliance was caused by weakness in [REDACTED] processes; specifically, the PRA review process did not include a step to confirm the residence history verification.</p> <p>This noncompliance started on January 3, 2017, when the first employee was granted physical access and ended on November 28, 2017, when [REDACTED] revoked the access for both employees.</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 employees had a fingerprint criminal background history check; these checks typically include a check against a national database which should capture the same information as performing a residence history verification. No harm is known to have occurred.</p> <p>MRO considered [REDACTED] relevant compliance history. [REDACTED] CIP-004-6 R3 compliance history includes a minimal risk violation of CIP-004-1 R3 ([REDACTED]) that was mitigated on [REDACTED], and a non-serious violation of CIP-004-1 R3 ([REDACTED]) that was mitigated on [REDACTED]. 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 instances of noncompliance and there is a substantial duration of time between the current noncompliance and the prior instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) revoked the access for both employees; and 2) added the Security Officer to the list of reviewers in the Access Request Process flow. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020850	CIP-003-6	R1	[REDACTED]	[REDACTED]	7/1/2018	8/13/2018	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 violation.)			<p>On August 30, 2018, [REDACTED] submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-003-6 R1. [REDACTED] states that it failed to review and obtain CIP Senior Manager approval for its cyber security policies at least once every 15 months for its low impact BES Cyber Systems as required by P1.2. The prior review was completed on March 1, 2017. [REDACTED] states that it had a compliance and document management tool that was configured to send reminder notifications associated with CIP Senior Manager review and approval, but those notifications were disabled as part of a compliance and document management tool project.</p> <p>The noncompliance was caused by [REDACTED] failing to follow its process to approve the cyber security policies.</p> <p>This noncompliance started on July 1, 2018, 15 months after its CIP Senior Manager last approved the cyber security policies and ended on August 13, 2018, when the CIP Senior Manager approved the cyber security 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] states that the CIP Senior Manager had already conducted reviews of multiple cyber security policies prior to July 1, 2018, but had not formally approved them. Further, [REDACTED] reports that there were no substantive changes made to the cyber security policies since the previous CIP Senior Manager approval. 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) had the CIP Senior Manager review and approve the cyber security policies; 2) re-enabled the notifications in its compliance and document management tool and added additional CIP-003-6 R1 related notifications; and 3) included CIP-003-6 R1 tasks in the task spreadsheet as an additional control. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020839	CIP-003-6	R1	[REDACTED]	[REDACTED]	06/03/2018	09/14/2018	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 violation.)			<p>On September 14, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-003-6 R1. Specifically, [REDACTED] states that it did not, at least every 15 months, have its CIP Senior Manager review and approve its documented cyber security policies for its assets that contain low impact BES Cyber Systems as required by P1.2.</p> <p>The cause of the noncompliance was that the review process lacked detail that resulted in an incorrect date of the prior review being recorded (i.e. the prior review occurred on March 3, 2017, but was incorrectly recorded as June 2017).</p> <p>This noncompliance started on June 3, 2018, when the existing cyber security policy was not reviewed and approved at least every 15 months and ended on September 14, 2018 when the CIP Senior Manager reviewed and approved its cyber security 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] reports that the cyber security policies did not require any updating since the last review and approval. 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) had its CIP Senior Manager review and approve the cyber security policy; and 2) will record the approval date in a calendar reminder which provides additional documentation for the compliance advisor. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020836	CIP-006-6	R1	[REDACTED]	[REDACTED]	07/01/2016	03/02/2018	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 violation.)			<p>On October 16, 2018, [REDACTED] submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-006-6 R1. [REDACTED]. The noncompliance occurred in the [REDACTED].</p> <p>[REDACTED] did not have any controls in place to monitor for unauthorized access when the rack doors were left open as required by P1.4. [REDACTED] states that during daily rounds, security personnel discovered that a rack door in the primary datacenter had an open front door. [REDACTED] states that the door was left open approximately 26 hours. [REDACTED].</p> <p>The cause of the noncompliance is that [REDACTED] failed to implement adequate controls during its CIP v5 transition.</p> <p>This noncompliance started on July 1, 2016, when the standard became enforceable and ended on March 2, 2018, [REDACTED].</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 entry to the data center is secured by badge access and door contacts. Additionally, [REDACTED] reports that the datacenter is protected by video monitoring and daily walkthroughs; a review of the video footage confirms there was no unauthorized access during the period that the rack door was left open. Finally, [REDACTED] states that the rack door badge readers log access and report access attempts to security personnel in real-time.</p> <p>BEPC has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) closed the rack door; 2) added an additional security camera; and 3) [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
MRO2018020795	CIP-007-6	R2	[REDACTED]	[REDACTED]	09/16/2017	09/13/2018	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 October 8, 2018, [REDACTED] submitted a self-log stating that, [REDACTED], it was in noncompliance with CIP-007-6 R2. [REDACTED] states that during the annual vulnerability assessment it discovered that a security patch was not installed on a single BES Cyber Asset (relay). [REDACTED] reports that it discovered that the patch was not applied because staff had interpreted the description of the patch as a feature enhancement as opposed to a cyber security patch. [REDACTED].</p> <p>The cause of the noncompliance was a deficient process that did not have any controls related to staff misinterpreting a patch description.</p> <p>This noncompliance started on September 16, 2017, 36 days after the patch was evaluated and ended on September 13, 2018, when the patch was installed.</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 only impacted a single relay. Additionally, [REDACTED] states that [REDACTED]. Additionally, [REDACTED] reports that the relay was located within a functioning PSP and ESP, and access to the relay was further limited by an intermediate system. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) installed the patch; 2) instructed the patch management group to reach out to the manufacturer regarding uncertainty about future security patches; 3) created a backup review plan for interpretation of patch releases; 4) contacted the manufacturer and asked for clearer language in the patch descriptions to differentiate between a feature enhancement and a vulnerability patch; and 5) updated the patch implementation procedure for medium impact BES Cyber Systems and their associated PCAs. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020801	CIP-004-6	R4	[REDACTED]	[REDACTED]	03/02/2018	05/16/2018	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 violation.)			<p>On October 18, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4. Specifically, on March 2, 2018, [REDACTED] improperly granted an employee who did not have the proper authorization access to a designated BES Cyber System Information storage location (P4.1.3).</p> <p>The cause of the noncompliance was that [REDACTED] failed to follow its process for granting access to BES Cyber System Information storage locations.</p> <p>The noncompliance began on March 2, 2018, when the access was granted, and ended on May 16, 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. [REDACTED] states that the employee had authorized access to other BES Cyber System Information storage locations and authorized access to BES Cyber Systems. The employee had received the required cyber security training and had a current personnel risk assessment. 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) revoked the employee's access to the BES Cyber System Information storage location; and 2) held a coaching session with the responsible team regarding the incident. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020292	CIP-009-6	R3	[REDACTED]	[REDACTED]	01/19/2018	01/30/2018	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 violation.)			<p>On August 7, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-009-6 R3. [REDACTED] reports that the annual test was scheduled for November 2017 and actually occurred on November 16, 2017. [REDACTED] states that on October 20, 2017, its recovery procedures were exercised through an actual recovery. After the test and after the recovery, [REDACTED] was required within 90 days to update the recovery plan and notify each person with a defined role of the updates as required by P3.1. [REDACTED] states that it performed the updates for the actual recovery and the test in tandem. [REDACTED] reports that it did not update the procedure until January 26, 2018 (8 days late as calculated from the October 20, 2017 recovery) and did not notify the named persons of the changes until January 30, 2018 (12 days late).</p> <p>The cause of the noncompliance was that [REDACTED] process for updating its recovery plan did not adequately address situations where an actual recovery occurred as opposed to a planned test.</p> <p>This noncompliance started on January 19, 2018, 91 days after the actual recovery, and ended on January 30, 2018, when [REDACTED] notified the named persons of the changes to the recovery 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. The noncompliance can accurately be regarded as a documentation only issue that was resolved by updating the recovery plan and sending the notifications. Further, per [REDACTED], prior to the recovery plan updates, [REDACTED] had demonstrated its ability to recover through the successful recovery on October 20, 2017. 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) updated the recovery plan and sent the required notifications; and 2) added a control where the requirement owner contacts the SME on a monthly basis to determine if a recovery has occurred, and if so tracks the recovery to ensure that timely updates and notifications occur. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017016902	CIP-007-6	R5.	[REDACTED]	[REDACTED]	07/01/2016	02/17/2017	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 violation.)			<p>On February 3, 2017, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED], it was in noncompliance in two instances with CIP-007-6 R5.2.</p> <p>For instance one, on November 17, 2016, the entity discovered that it was in noncompliance with CIP-007-6 R5. (5.2.) after preparing to execute a license upgrade for the entity's Physical Access Control System (PACS) and identified that it did not inventory a system account used for license management.</p> <p>This instance started on July 1, 2016 when the entity implemented a documented process for System Access Controls but did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type for one (1) account on one (1) applicable Cyber Asset. The instance ended on January 13, 2017 when the account in question was added to the account inventory.</p> <p>Specifically, the account in scope can only be used to access the license administration tool. The license administration tool is accessed via a web interface that is locally hosted, the account can only be used to manage the license and cannot be used to perform any operating tasks. The entity had not previously inventoried the license administration account pursuant to CIP-007-6, as the license account is noted in the PACS installation materials but is not otherwise listed in any vendor documentation.</p> <p>The root cause of this instance was failure to review PACS installation documentation to ensure that all required accounts have been inventoried.</p> <p>For instance two, on December 21, 2016, the entity discovered that it was in noncompliance with CIP-007-6 R5. (5.2.) due to an increased awareness of inventory accuracy following a previous self-report.</p> <p>This instance started on July 1, 2016 when the entity implemented a documented process for System Access Controls but did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type for one (1) account on one (1) applicable Cyber Asset. The instance ended on February 17, 2017 when the account in question was added to the account inventory.</p> <p>Specifically, when the entity transitioned to its CIP Version 5 program, a local database service account on a Smart Grid production server was not added to the account inventory because an employee relied on an alternate server, rather than a production server for generating the account inventory. The employee assumed that both the production and alternate server had identical accounts. However, due to license limitations, the accounts were different on these devices.</p> <p>The root cause of this instance was that an individual relied on a test server rather than a production server when performing an inventory of accounts.</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, by failing to inventory all system accounts, the system accounts may not be afforded all of the protections required by the CIP standards. Lack of account protections could lead to compromise of applicable Cyber Assets rendering the Cyber Asset unavailable, degraded, or misused.</p> <p>For instance one, the account in question only had access to the license administration tool for the PACS. If the PACS license was deactivated, the PACS would continue to maintain all access controls, access lists, and access logs.</p> <p>For instance two, the account in question is a service account used only for performance monitoring on smart grid servers. Every user with access to the account was provisioned for CIP access and had a business need to use the account.</p> <p>The risk related to account compromise was reduced. The accounts in question were not privileged accounts and were limited in terms of system functionality. Additionally, the ESP containing the Cyber Assets were afforded the protection required by the CIP standards, including malicious activity detection. Attempts to compromise the accounts would have likely been detected by the entity's intrusion detection systems.</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
NPCC2017016902	CIP-007-6	R5.	[REDACTED]	[REDACTED]	07/01/2016	02/17/2017	Self-Report	Completed
			No harm is known to have occurred as a result of this noncompliance.					
			NPCC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) Instance 1: On January 13, 2017, the account was added to the inventory of default accounts. 2) Instance 2: On February 17, 2017, the account was added to the inventory of default accounts. 3) The passwords were changed for the accounts. The entity reviewed all PACS and SQL documentation to confirm no additional default accounts were excluded from the inventory. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017016905	CIP-010-2	R1.	[REDACTED]	[REDACTED]	8/03/2016	12/08/2016	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 violation.)			<p>On February 3, 2017, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED], it was in noncompliance in two instances with CIP-010-2 R1. In both instances, the entity's baseline configuration monitoring tool alerted to a software change that prompted an internal investigation.</p> <p>The first instance started on December 2, 2016, when the entity failed to follow its Configuration Change Management process for one (1) High Impact BES Cyber Asset. Specifically, the entity failed to authorize and document the change, determine required cyber security controls that could be impacted by the change, and test in a test environment or in a production environment in a manner that minimizes adverse effects. The instance ended on December 6, 2016, when the entity removed the unauthorized software.</p> <p>Specifically, an employee installed a support tool on a workstation. The software is approved for use in the entity's corporate environment but had not been used in the CIP environment. The entity's baseline configuration monitoring tool alerted to the software change and an investigation was conducted. The investigation confirmed that the software changes were not part of any IT Request for Change or other approved IT work.</p> <p>The root cause was a failure of an employee to follow internal change management process and technical controls were not in place to prevent installation of software.</p> <p>The second instance started on August 3, 2016, when the entity failed to follow its Configuration Change Management process for one (1) High Impact BES Cyber Asset. Specifically the entity failed to authorize and document the change, determine required cyber security controls that could be impacted by the change, and test in a test environment or in a production environment in a manner that minimizes adverse effects. The noncompliance ended on December 8, 2016, when the entity removed the unauthorized software.</p> <p>Specifically, an employee installed software to a workstation. The software was a newer version of software approved for and in use on this workstation; however, the version of software installed was not reviewed and deployed through the entity's change management process. The entity's baseline configuration monitoring tool alerted to the software change and an investigation was conducted. The investigation revealed that the software deployed did not appear unusual for this device, however, the software changes did not appear to be part of any IT Request for Change or other approved IT work.</p> <p>The root cause was an employee did not follow internal change management process and technical controls were not in place to prevent installation of software.</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 exposed its ESP to potentially malicious software by not following the entity's change management procedures, installing unauthorized software on two workstations, and failing to ensure applicable CIP controls were not impacted by the changes.</p> <p>[REDACTED] The software in the first instance was approved for use in the entity's corporate environment, and the software in the second instance was obtained directly from the vendor, through secure means, and was a later version of the software already in use on the Cyber Asset in scope.</p> <p>The assets in scope are also scanned weekly for vulnerabilities and the vulnerability scan results did not flag any additional vulnerabilities due to the unauthorized software. The assets further have up to date antivirus software installed.</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) Removed software from the workstation (in both Instances) 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017016905	CIP-010-2	R1.	[REDACTED]	[REDACTED]	8/03/2016	12/08/2016	Self-Report	Completed
<p>To prevent recurrence:</p> <p>Instance 1:</p> <ol style="list-style-type: none"> 1. Removed admin rights from intermediate "jump" systems; 2. [REDACTED] 3. [REDACTED] 4. [REDACTED] 5. Worked with vendor to reevaluate the need to remove local administrator rights from workstations; 6. Expanded User Policy Enforcement Changes to Workstations within the ESP, to allow further control of what user activity is allowed on the Workstation within the ESP. <p>Instance 2:</p> <ol style="list-style-type: none"> 1. Sent email communication to all staff reinforcing the importance of following the approved change management process. 2. Removed admin rights from intermediate "jump" systems 3. [REDACTED] 4. [REDACTED] 5. [REDACTED] 6. Worked with vendor to re-evaluate the need to remove local administrator rights from certain workstations; 7. Expanded policy changes to control user activity on the workstations within the ESP 								

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017017113	CIP-004-6	R5.	[REDACTED]	[REDACTED]	09/21/2016	10/25/2016	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 violation.)			<p>On March 3, 2017, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it had discovered on October 21, 2016, it was in noncompliance with CIP-004-6 R5. (5.2.) after the entity conducted an access review following an employee transfer.</p> <p>This noncompliance started on September 21, 2016 when the entity failed to remove access from one (1) individual to one (1) EACMS associated with High Impact BES Cyber Systems following a transfer date of September 19, 2016. The noncompliance ended on October 25, 2016, when the entity disabled the employee's EACMS account. On December 7, 2016, the entity removed the account from the EACMS.</p> <p>Specifically, the entity failed to remove access to the entity's [REDACTED] application for one employee following a transfer date.</p> <p>The root cause of this noncompliance was a failure to manually update a CSV file at the time the employee was granted access to the [REDACTED] application. The employee's original approved access was not incorporated into [REDACTED]. The [REDACTED] system did not know to remove the employee's access when the individual was transferred.</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, by failing to revoke electronic access to a transferred employee, the employee may continue to access the monitoring systems that is associated with High Impact BES Cyber Systems without a valid business need and may use the information within the logs of the monitoring system to gain access to High Impact BES Cyber Systems and disrupt operations.</p> <p>The noncompliance's risk was reduced due to the employee internally transferring. The employee was approved at all times for CIP access and did not access the [REDACTED] following the transfer.</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) Disabled the [REDACTED] account 2) Removed the account from [REDACTED] 3) Automatically generates a task assigned to an [REDACTED] administrator to update the CSV file required for [REDACTED] when manually provisioning access to a CIP Cyber Asset 4) Added a verification step in [REDACTED] to confirm CSV file updates are made 5) Generated a discrepancy report that is reviewed weekly to assess inconsistencies between granted and documented access. 6) Automated the generation of CSV files in [REDACTED] when access is granted. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018778	CIP-007-3a	R3.	[REDACTED]	[REDACTED]	01/13/2016	09/19/2017	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 December 15, 2017, [REDACTED] (the entity) submitted a Self-Report stating that as [REDACTED] it had discovered on September 11, 2017 it was in noncompliance with CIP-007-3a R3. (R3.2.) after performing a routine security assessment.</p> <p>This noncompliance started on January 13, 2016 when the entity failed to implement its security patch management program for tracking and installing applicable cyber security software patches for two (2) Cyber Assets. The noncompliance ended on September 19, 2017 when the entity applied the applicable security patches.</p> <p>[REDACTED] Thus, the entity missed applying the patch to two (2) IT performance monitoring cyber assets identified as PCAs under version 3 and identified as EACMS under version 5.</p> <p>The root cause of this noncompliance was a process weakness with tracking the final application or mitigation of patches that are applicable to assets owned by multiple subject matter experts.</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 tracking and patching applicable cyber security patches the entity leaves systems susceptible to exploit. If an attacker were to have exploited the known vulnerability, they could have performed a denial of service attack to the devices in scope, in an attempt to disrupt monitoring services or BES Cyber Systems that were located on the same network.</p> <p>The entity reduced the risk of a known vulnerability being exploited by restricting external traffic with firewall access control polices. The entity restricts access to devices within its Electronic Security Perimeter and monitors cyber assets with malware detection software and network intrusion detection systems.</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) Deployed the applicable patches 2) Performed a one time full patch reconciliation, by asset, based upon the 2017 CIP Asset List 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018018910	CIP-007-6	R2.	[REDACTED]	[REDACTED]	05/24/2017	11/22/2017	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 December 28, 2017, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it had discovered on November 21, 2017 that it was in noncompliance with CIP-007-6 R2. (2.2.) after performing its annual Cyber Vulnerability Assessment.</p> <p>This noncompliance started on May 24, 2017 when the entity failed to evaluate one (1) security patch for applicability within 35 calendar days of the last evaluation for the source or sources identified. This noncompliance affected one (1) Electronic Access Control and Monitoring System. The noncompliance ended on November 22, 2017 when the applicable cyber security patch was assessed.</p> <p>Specifically, the electronic repository which tracks ownership of CIP Cyber Assets identified a prior owner of the [REDACTED] system as the appropriate SME. The patch was assigned for review to the incorrect SME for assessment with respect to the entity's [REDACTED] system and the SME closed the ticket without assessing the patch.</p> <p>The root cause of this noncompliance was failure to ensure the accuracy of information on applicable Cyber Assets stored in the entity's 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, not assessing cyber security patches within the required timeframe can leave applicable Cyber Assets exposed to compromise via vulnerability exploit for prolonged periods. System compromise can then be used to render a Cyber Asset unavailable, degraded, or misused due to the noncompliance. In this instance, the vulnerability could allow Remote Denial of Service if successfully exploited.</p> <p>The entity reduced the risk of system compromise via vulnerability exploit as it restricts external traffic to these cyber assets via firewalls, limiting the risk of remote exploitation. Access is restricted to authorized and authenticated users within the ESP. The assets are monitored by malware detection on hosts and network Intrusion Detection Systems (IDS). Further, if the vulnerability was exploited internally, it would provide no ability to affect core reliability or market systems.</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) Assessed the vulnerability and patch with respect to [REDACTED]. The entity deployed the patch to [REDACTED]. 2) Performed a review of asset owners in its electronic registry of CIP Cyber Assets to verify accuracy. 3) Presented issue as a "lessons learned" with IT SMEs to request that they investigate the reason a ticket may have been assigned to them in error prior to closing. 4) Enhanced an existing weekly patch and vulnerability reconciliation report reviewed by the [REDACTED] to verify that each asset owning team has all applicable patches for their respective teams tracked in the patch tracking system. This report will allow the [REDACTED] to identify patches which have not been entered into an RFC ticket and to escalate with asset owners when necessary. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019288	CIP-007-6	R5.	[REDACTED]	[REDACTED]	04/16/2017	10/31/2017	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 February 26, 2018, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it had discovered on April 16, 2017 that it was in noncompliance with CIP-007-6 R5. (5.6.) after performing its annual shared account review.</p> <p>This noncompliance started on April 16, 2017 when the entity failed to technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months. The noncompliance ended on October 31, 2017 when the entity changed the password for one (1) of the shared accounts, disabled the other two (2) shared accounts, and completed the required process modifications.</p> <p>Specifically, the noncompliance was for three (3) shared administrator accounts supporting the entity's [REDACTED] system. The passwords were last changed on January 15, 2016.</p> <p>The root cause of this noncompliance was failure to ensure that account review procedures were executed during the required timeframe.</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, not annually changing shared passwords can increase the probability of shared password disclosure and/or hacking/cracking. The shared password can be used to gain unauthorized access to an applicable Cyber Assets and render the asset unavailable, degraded, or misused due to the noncompliance.</p> <p>The entity reduced the risk of shared account compromise by protecting remote access to the cyber asset using multi-factor authentication via intermediate LAN (jump-hosts), firewall rules enforcing cyber access controls and physical access controls. The entity also verified that the passwords had been changed from the default.</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) changed the password on one admin account, and elected to disable the other two admin accounts. 2) updated its review process to use the entity's GRC tool to track completion of the shared account review on a 12 month cycle; 3) implemented escalations when attestations are not timely completed; 4) required a final reconciliation/signoff when all attestations have been completed. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019726	CIP-005-5	R2.	[REDACTED]	[REDACTED]	02/08/2018	02/08/2018	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 violation.)			<p>On May 22, 2018, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED], it had discovered on February 8, 2018 that it was in noncompliance with CIP-005-5 R2. (2.1., 2.2., 2.3.) after a user did not use an Intermediate System during an interactive remote access (IRA) session with an applicable Cyber Asset.</p> <p>This noncompliance started on February 8, 2018 when the entity failed to follow its IRA processes when establishing a logical connection to a High Impact BES Cyber Asset. As a result, the entity failed to utilize an intermediate system, encryption, and multi-factor authentication for an IRA session. The noncompliance ended on February 8, 2018, when the user closed the IRA session and reported the issue.</p> <p>Specifically, a Database Administrator (DBA) was investigating connectivity issues associated with a system-to-system configuration between a non-CIP server and a Protected Cyber Asset within the ESP, an [REDACTED] server. In the course of testing the system to system communication path, the DBA remotely logged-in to [REDACTED] through the enabled port used for system-to-system communication. The DBA took no further actions and immediately terminated the session.</p> <p>The root cause of this noncompliance was failure to comply with documented IRA procedures.</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, not following documented IRA procedures could lead to unintentional compromise of applicable Cyber Assets by connecting less hardened assets to protected cyber assets and performing unintended tasks. This access could potentially allow an unauthorized individual remote access to applicable Cyber Assets. The unauthorized access could be used to render Cyber Assets unavailable, degraded, or misused due to the noncompliance.</p> <p>The entity reduced the risk of unauthorized remote access by immediately terminating the IRA session. The user in question was also approved for IRA via the entity's Intermediate Systems.</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) updated its security policy to make clear that ports open for permissible system-to-system communication cannot be used for any other purpose; 2) communicated that message through an awareness communication. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019894	CIP-009-6	R3.	[REDACTED]	[REDACTED]	04/03/2018	05/04/2018	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 violation.)			<p>On June 19, 2018, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it had discovered on May 3, 2018 it was in noncompliance with CIP-009-6 R3. (3.1.2 and 3.1.3) after preparing for a mock CIP Audit.</p> <p>This noncompliance started on April 3, 2018 when the entity failed to update the recovery plan based on documented lessons learned and failed to notify each person or group with a defined role in the recovery plan of the updates within 90 calendar days after completion of a recovery plan test. This noncompliance was for one (1) EACMS associated with High Impact BES Cyber Systems. The noncompliance ended on May 4, 2018 when the entity updated the recovery plan and notified responsible individuals of the updates.</p> <p>Specifically, the entity performed the test of the recovery plan on January 3, 2018, the entity documented the lessons learned on January 28, 2018. The recovery plan was updated on April 23, 2018 (20 days late) and each person or group within a defined role in the recovery plan were notified on May 4, 2018 (31 days late). The noncompliance applied to the entity's [REDACTED] which is an EACMS. The SME who conducted the tabletop test was not aware of the time limits for updating recovery plans and notifying the affected individuals with a defined role in the plan.</p> <p>The root cause of this noncompliance was lack of training/awareness concerning the timeframe requirements for the update of recovery plans and notification of individuals/groups with defined roles.</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, not updating the recovery plan and notifying responsible individuals of the update in a timely fashion, could lead to the Cyber Asset being rendered unavailable or degraded due to incorrect or ineffective actions being taken during recovery plan execution.</p> <p>The risk of recovery plan updates and notifications not being performed in a timely fashion was reduced by the fact that the recovery plan updates were minor and would not have impacted the entity's ability to recovery the asset. Although members of the recovery team changed as part of the lesson's learned update, the employee with primary responsibility for this recovery plan had access to the updated plan.</p> <p>If the system in scope were to become unavailable, automated access request processing through the system would be unavailable. The entity in this instance would manually process access requests until the system could be restored. No other systems or processes would be interrupted.</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. Completed update of the recovery plan and notified the affected individuals of the updated recovery plan; 2. Used a GRC tool to track the performance of recovery plan tests, which will send automated reminders to SMEs to conduct and document recovery plan tests. The language in the automated reminders has been updated to include the time requirements for updating the plan and notifying affected individuals after the test is conducted. 3. Used a GRC tool to automatically track completion of recovery plan updates following tests, including escalations when deadlines approach. Notification of recovery plan updates will be automated through the GRC tool. 4. Conducted an awareness session with SMEs to review recovery plan test requirements. 5. Validated other recovery plans for any additional instances of the noncompliance. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018020279	CIP-004-6	R5.	[REDACTED]	[REDACTED]	07/11/2018	07/30/2018	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 violation.)			<p>On August 28, 2018, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED], it had discovered on July 10, 2018, it was in noncompliance with CIP-004-6 R5. (5.2.) after failing to manually revoke access when its automated process failed.</p> <p>This noncompliance started on July 11, 2018 when the entity failed to revoke access to one individual during an internal transfer. The noncompliance ended on July 30, 2018, when the entity manually revoked the individual's access.</p> <p>Specifically, an employee transferred from the entity's networking group to the [REDACTED] department. It was determined that the individual's need for electronic access would cease as of July 9, 2018, and therefore would be terminated as of July 10, 2018. Access terminations are managed on an automated basis through roles provisioned in the entity's [REDACTED] System. Five [REDACTED] roles for that employee were scheduled to end on July 10, 2018; the tasks to end four roles successfully completed, but the task for the fifth role did not successfully complete. As a secondary control, the entity's access management group monitors access revocations and determined that one role was not revoked. They attempted to troubleshoot the automated software issue but were unable to remove the [REDACTED] role on July 10, 2018.</p> <p>The root cause of this noncompliance was due to a vendor software defect, which was patched after consultation with the vendor. A secondary cause of the violation was the failure to take steps to manually remove access on July 10, 2018 when the software did not successfully end the [REDACTED] role.</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 employee was authorized as an administrator in his previous role and was also granted administrator access in his new role. The employee had a valid PRA and CIP Training. The employee did not attempt to access any electronic areas to which access should have been revoked after the start of the noncompliance.</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) Removed the transferred individual's access 2) Patched the software defect which prevented termination of the [REDACTED] role 3) Updated its internal process document to make clear that steps should be taken to remove access manually in the event of unresolvable technical failures 4) Communicated the update to [REDACTED] through email and lessons learned 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Mitigation Completion Date
RFC2018020608	CIP-007-6	R2	[REDACTED]	[REDACTED]	10/1/2016	10/15/2018	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 22, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2.</p> <p>The Basic Input Output System (BIOS) on the entity's computer workstations and servers associated with a Bulk Electric System (BES) Cyber System were not patched in accordance with CIP-007-6 R2. Both workstations and servers associated with the BES Cyber System did not include BIOS on the patch source list. Therefore, the entity did not evaluate BIOS for security patches per CIP-007-6 R2.</p> <p>The entity discovered this issue during a review of vulnerabilities when compliance staff identified the release of security patches, which suggested that the workstations and servers' BIOS should be updated to the latest version to address security vulnerabilities. The BIOS was not on the patch source list because the entity baselined the BES Supervisory Control and Data Acquisition system at the time using a baseline tool, but the baseline tool was not configured to pull the BIOS into the Software Baseline reports.</p> <p>This noncompliance involves the management practices of asset and configuration management and verification. The root cause of this noncompliance is that the baseline tool was not configured to pull the BIOS into the Software Baseline reports. This failure reveals ineffective asset and configuration management and ineffective verification.</p> <p>This noncompliance started on October 1, 2016, when the BIOS were first installed on computer workstations and servers and ended on October 15, 2018, when the entity applied the overdue patches to the BIOS on computer workstations and servers.</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 failing to patch BIOS on computer workstations and servers increases the opportunity for infiltration of unauthorized network traffic into the Electronic Security Perimeter. The risk is minimized because the workstations and servers impacted exist on an independent/isolated network with no external connections making them more difficult to compromise. The entity also has a low peak load of approximately [REDACTED]. Lastly, during the noncompliance, the entity confirmed that no unauthorized accounts were created and no unauthorized attempts to access the system were reported. 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 current noncompliance has a different root cause than the prior noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) evaluated BIOS patch releases; 2) developed a mitigation plan if applicable Security Patches were found; 3) included BIOS in system baselines where applicable. This will help prevent recurrence because the entity is now including BIOS when it is updating baselines; 4) included BIOS in the source evaluation process for patching. This will help prevent recurrence because the entity now includes BIOS when searching for and applying applicable patches; and 5) updated applicable documentation to ensure relevant staff continue to evaluate patches for BIOS. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020430	CIP-010-2	R1	[REDACTED]	[REDACTED]	8/14/2018	8/15/2018	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 September 13, 2018, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], they were in noncompliance with CIP-010-2 R1. [REDACTED]</p> <p>While troubleshooting a partial security-patch installation on a workstation (identified as Physical Access Control Systems (PACS)), the entity updated the [REDACTED] Update Agent to the latest version without determining the impacted cyber controls prior to the change.</p> <p>In early August 2018, an IT Application Consultant applied security patches to the workstations. While updating the configuration baselines, the [REDACTED] Consultant noted that one of the workstations did not have the entire set of patches applied. On August 8, 2018, the entity initiated an incident report to document the investigation into the discrepancy.</p> <p>The entity investigated the incident and determined that the [REDACTED] Update Agent installed on the workstation was not the latest version. On August 14, 2018, the [REDACTED] Update Agent was updated to the latest version and the security patches were installed successfully. On August 15, 2018, the entity's CIP Compliance team reviewed the [REDACTED] Update Agent and determined that the version change was made without the requisite assessment, verification, and documentation of their potential impact to CIP-005 and CIP-007 security controls. Following the investigation, the entity initiated a latent change request on August 15, 2018 to document the configuration change aspects of the incident.</p> <p>This noncompliance involves the management practices of workforce management and verification. Although the individuals involved in updating the configuration baselines have extensive experience with the entity's change-management processes, workforce management is involved because the individuals still made the mistake despite their understanding of the processes. A failure to verify is the root cause because entity personnel did not verify that they had determined the impacted security controls prior to making the change to the baselines.</p> <p>This noncompliance started on August 14, 2018, when the entity updated the baseline configurations without determining the impacted security controls prior to the change and ended on August 15, 2018, when the entity initiated a latent change request to document the configuration change aspects of the noncompliance.</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 updating the [REDACTED] Update Agent to the latest version without determining the impacted cyber controls prior to the change being implemented. That change could adversely affect system security. The risk is minimized because the entity had installed the same [REDACTED] Update Agent version on other similar workstations at the entity with no negative effects. Additionally, the duration is only one day. The entity quickly identified, assessed, 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 instant noncompliance was identified, assessed, and corrected within one day and has a different root cause than the prior noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) provided counseling about the importance of process adherence, and accurately assessing and documenting the details of changes. The entity documented completion of counseling; 2) created a targeted awareness reminder for all personnel with Cyber Admin Access rights about the importance of process adherence; and 3) instituted a practice within the NERC CIP Compliance Team to provide "just in time" awareness reminders about the potential need for additional change records when a support team is assigned an incident to investigate and resolve configuration anomalies. This was discussed in a team meeting and has been incorporated into the appropriate procedure. <p>ReliabilityFirst 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
RFC2018020431	CIP-010-2	R1	[REDACTED]	[REDACTED]	8/14/2018	8/15/2018	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 September 13, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>While troubleshooting a partial security-patch installation on a workstation (identified as Physical Access Control Systems (PACS)), the entity updated the [REDACTED] Update Agent to the latest version without determining the impacted cyber controls prior to the change.</p> <p>In early August 2018, an IT Application Consultant applied security patches to the workstations. While updating the configuration baselines, the [REDACTED] Consultant noted that one of the workstations did not have the entire set of patches applied. On August 8, 2018, the entity initiated an incident report to document the investigation into the discrepancy.</p> <p>A [REDACTED] and [REDACTED] Consultant investigated the incident and determined that the [REDACTED] Update Agent installed on the workstation was not the latest version. On August 14, 2018, the [REDACTED] Update Agent was updated to the latest version and the security patches were installed successfully. On August 15, 2018, the entity's CIP Compliance team reviewed the [REDACTED] Update Agent and determined that the version change was made without the requisite assessment, verification, and documentation of their potential impact to CIP-005 and CIP-007 security controls. Following the investigation, the entity initiated a latent change request on August 15, 2018 to document the configuration change aspects of the incident.</p> <p>This noncompliance involves the management practices of workforce management and verification. Although the individuals involved in updating the configuration baselines have extensive experience with the entity's change-management processes, workforce management is involved because the individuals still made the mistake despite their understanding of the processes. A failure to verify is the root cause because entity personnel did not verify that they had determined the impacted security controls prior to making the change to the baselines.</p> <p>This noncompliance started on August 14, 2018, when the entity updated the baseline configurations without determining the impacted security controls prior to the change and ended on August 15, 2018, when the entity initiated a latent change request to document the configuration change aspects of the noncompliance.</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 updating the [REDACTED] Update Agent to the latest version without determining the impacted cyber controls prior to the change being implemented. That change could adversely affect system security. The risk is minimized because the entity had installed the same [REDACTED] Update Agent version on other similar workstations at the entity with no negative effects. Additionally, the duration is only one day. The entity quickly identified, assessed, 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 instant noncompliance was identified, assessed, and corrected within one day and has a different root cause than the prior noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) provided counseling about the importance of process adherence, and accurately assessing and documenting the details of changes to the [REDACTED] Consultant. The entity documented completion of counseling; 2) created a targeted awareness reminder for all personnel with Cyber Admin Access rights about the importance of process adherence; and 3) instituted a practice within the NERC CIP Compliance Team to provide "just in time" awareness reminders about the potential need for additional change records when a support team is assigned an incident to investigate and resolve configuration anomalies. This was discussed in a team meeting and has been incorporated into the appropriate procedure. <p>ReliabilityFirst 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
RFC2018020253	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/26/2018	7/27/2018	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 August 21, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. The entity failed to complete baseline configurations for updates to [REDACTED] specific software devices within 30 calendar days of an authorized change. The specific [REDACTED] system had previously been included in the entity's manual process for establishing baselines. The specific software devices are designed to detect for and/or block [REDACTED] against a target application or a computer. [REDACTED].</p> <p>A [REDACTED] developer [REDACTED] notified the [REDACTED] lead [REDACTED] that the automation for the specific software devices had been completed, tested, and validated. The [REDACTED] employee did test that the scripts were running correctly on the data collection server and that accurate data was being captured in the collection database. The [REDACTED] employee failed to test/validate that the data was being transmitted from the collection database to the final repository [REDACTED]. The [REDACTED] employee told the senior employee that everything had been tested successful. The senior employee did not validate that all stages had been properly tested as instructed. The senior employee ignored reporting alerts that manual data collection had not been performed within the required timeline (believing that the automated data collection was working).</p> <p>During the entity's [REDACTED] baseline configuration review, the [REDACTED] department determined that a specific software upgrade had been completed, but that the baseline configurations had not been updated within the 30 calendar days required. The baseline configurations were updated on day 32. The investigation concluded that the [REDACTED] scripting process was completed, but the data feed [REDACTED] had not yet been activated.</p> <p>This noncompliance involves the management practices of workforce management, validation, and verification. The [REDACTED] employee [REDACTED] was ineffectively trained on how to test/validate that the data was being transmitted [REDACTED] to the final repository [REDACTED]. The senior employee assumed that the data for these [REDACTED] devices were now being collected [REDACTED], but they did not validate and verify that [REDACTED] collection [REDACTED] was working for these devices. That failure to validate and verify is a root cause of this noncompliance.</p> <p>This noncompliance started on July 26, 2018, when the entity was required to update baseline configurations for [REDACTED] software devices within 30 calendar days of an authorized change and ended on July 27, 2018, when the entity updated the baseline configurations for [REDACTED] 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 risk posed by a failure to update the baselines is providing an opportunity for unauthorized and undetected modifications to be made to applicable Cyber Assets, which could introduce system instability or affect the functionality of such assets, and the entity could rely on incorrect information when performing subsequent tasks. The risk is minimized because this noncompliance only affected [REDACTED] specific software devices [REDACTED] and the noncompliance occurred for just one day. The entity quickly identified and corrected this noncompliance, which reflects strong detective and corrective internal controls. Additionally, the entity had authorized the initial change that necessitated updating the baseline configurations. 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 different root causes, the potential harm to the BPS was highly unlikely, and the short time frame (one day) reduced the risk of potential harm. Additionally, the entity quickly identified, assessed, and corrected the instant noncompliance, which reveals strong detective and corrective controls.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) documented the baseline configuration items per the requirements; 2) documented a process for cutting over baseline configuration data collection [REDACTED] activities; and 3) trained personnel impacted by the new documented process. <p>The new process will help ensure that there are no gaps with baseline configuration data collection and review. The entity will continue to research and apply opportunities to improve compliance and security controls where they are found to improve the reliability of the BPS. The entity performed an extent of condition to determine if any other devices were affected in addition to the specific [REDACTED] devices. That extent of condition revealed that this issue did not occur on any other CIP production devices.</p> <p>ReliabilityFirst 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
RFC2018019898	CIP-003-6	R2	[REDACTED]	[REDACTED]	4/1/2017	8/31/2018	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 June 6, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-003-6 R2. On January 1, 2018, [REDACTED] took over control of plant operations and NERC compliance at the [REDACTED] facility. As part of this change, [REDACTED] performed a baseline review of NERC compliance in place at the time of the change. As part of this review, [REDACTED] discovered that, while [REDACTED] personnel stated that they performed Cyber Security Awareness training and an exercise of the Cyber Security Incident Response Plan in 2017, [REDACTED] could not locate documentation to verify this fact.</p> <p>The root cause of this noncompliance was the lack of effective internal controls to ensure the training and exercise was properly completed and documented each year. This root cause involves the management practice of reliability quality management, which includes maintaining a system for identifying and deploying internal controls.</p> <p>This noncompliance started on April 1, 2017, when the entity was required to comply with CIP-003-6 R2 and ended on February 8, 2018, when the entity delivered the training and performed the exercise for 2018.</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 harm associated with failing to deliver required Cyber Security Awareness training is that the operating staff may not have been fully aware of the cyber security practices that the entity employs. The potential risk associated with failing to perform the required Cyber Security Incident Response Plan exercise is that the entity would not have been able to discover any potential issues with the plan itself. These risks were mitigated in this case by the following factors. First, the entity stated that it had delivered the requisite training and performed the requisite exercise, but that it failed to retain documentation of these activities. Consequently, this noncompliance is primarily a documentation issue. Second, when the entity delivered the training and performed the exercise for 2018, no surprises occurred. Relevant staff also concluded that the Cyber Security Incident Response plan was adequate as written with no recommendations for changes coming out of the exercise. 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) completed the 2018 Cyber Security Awareness Training and Cyber Security Incident Response Plan exercise, ensuring that relevant evidence files are stored in appropriate [REDACTED] server; and 2) developed a preventative maintenance work order that will monitor the two activities described above to ensure they are performed on the correct frequency and the completion documentation is stored in the appropriate [REDACTED] location. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019878	CIP-011-2	R2	[REDACTED]	[REDACTED]	10/19/2016	4/7/2019	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 June 8, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-011-2 R2. The entity asset disposal program requires that each disposed device that contains Bulk Electric System Cyber System Information (BCSI) be sanitized by an approved method and documented properly per the NERC program procedure. [REDACTED] The entity failed to follow these proper procedures for three (3) devices (i.e., two Ethernet switches and the Remote Terminal Unit).</p> <p>During a quality review, the entity discovered that these three (3) devices did not have the disposal/reuse form completed per its documented asset disposal procedure. The three (3) devices were located at two (2) separate medium impact sites without External Routable Connectivity (ERC).</p> <p>Regarding the first two devices, the entity replaced the two Ethernet switches as part of a project and retired them in the [REDACTED] on October 19, 2016. The [REDACTED] retirement test prompted the testing engineer performing the retirement to follow the associated procedure, but the testing engineer failed to upload the form to [REDACTED] or send an email to the area planner to be attached in the work management database.</p> <p>Regarding the third device, the RTU failed, which caused the entity to replace it and retire it in the database on May 25, 2017. The database retirement was performed by a SCADA engineer, but a field engineer performed the actual work. The field engineer did not complete the form or record the method of sanitization. The engineer placed the RTU in the E-waste bin located in a secure location without destroying the [REDACTED].</p> <p>In all three instances, the devices were not redeployed on the system and have no recorded evidence of disposal in accordance with the policy.</p> <p>The root cause of this noncompliance was inadequate training and enforcement of the asset disposal procedure with respect to the field engineering team. This root cause involves the management practice of workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on October 19, 2016, when the entity retired the Ethernet switches and will end on April 7, 2019, when the entity committed to complete its Mitigation Plan including changing the passwords on all RTUs that had the same password as the one improperly disposed of.</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 associated with disposing of assets containing BCSI without taking proper precautions is that the BCSI could be obtained by an unauthorized individual. This risk was mitigated in this case by the following factors. First, with respect to the RTU at issue, the only BCSI at risk was the device IP address and password. The similar devices that could potentially be compromised by this information are on an isolated network which can only be accessed when someone is physically inside the respective substation. This means that the IP Address cannot be used to remotely access the device from the internet or within the business network. Furthermore, these devices are located within physically controlled zones [REDACTED]. Second, with respect to the Ethernet switches, those devices do not implement any security controls that are relied upon to protect devices on the local network. [REDACTED] 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) reviewed corrective actions from [REDACTED] to confirm actions cover reported CIP-011 issue. (The corrective actions in [REDACTED] include reinforcement training for relevant personnel on the entity's asset disposal procedure.); 2) initiated a project to issue password settings changes for all similar Remote Terminal Unit's (RTUs): [REDACTED]; and, created the work order tasks for the relevant group to implement the changes; 3) tracked completion of the password settings changes work orders and [REDACTED] results' 4) tracked completion of the password settings changes work orders and [REDACTED] results; and 5) tracked completion of the password settings changes work orders and [REDACTED] results. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020255	CIP-009-6	R2	[REDACTED]	[REDACTED]	2/10/2018	5/25/2018	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 August 17, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-009-6 R2. The entity's management platform consists of [REDACTED]. On May 22, 2018, during a review of the status of 2018 functionality testing, the entity discovered that the functionality recovery testing for the management platform had not yet been completed. The last [REDACTED] was completed on November 17, 2016, and the [REDACTED] was completed on December 22, 2016. Consequently, the next test for the [REDACTED] should have been completed by February 10, 2018, and the next test for the [REDACTED] should have been completed by March 17, 2018.</p> <p>The root cause of this noncompliance was a breakdown in the transition of CIP-009 functionality testing duties between the entity's support team and the centralized technical services team for the entity's parent company. During a reorganization in August 2017, support of the entity's management platform was transferred from the entity's support team to the centralized technical services team for the entity's parent company. However, the transition plan did not explicitly call out the functionality testing task. This omission caused confusion between the two teams and resulted in the missed testing. This root cause involves the management practice of integration because it involves the integration, or reorganization, of the processes applicable to two different business units.</p> <p>This noncompliance started on February 10, 2018, when the entity should have completed the [REDACTED], and ended on May 25, 2018, when the entity completed the requisite tests.</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 complete functionality recovery testing is that the relevant systems may not be able to timely recover from an adverse event. This risk was minimized in this case by the following factors. First, [REDACTED] was completed as expected during the time of noncompliance (i.e., February through May 2018), which increases the likelihood that the systems could have been restored after an adverse event. Second, the systems at issue do not directly control the BPS. Rather, they are [REDACTED], so a delay in recovery of these assets would not have a direct operational effect on the BPS. ReliabilityFirst also notes that during the time of the noncompliance, there was no need to actually implement the recovery plan. 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) completed the functionality testing on all management platforms; 2) reviewed the [REDACTED] inventory for confirmation of locations which store CIP-009 compliance requirement evidence; 3) submitted a ticket to create or modify the appropriate access management system role(s) for the CIP-009 compliance team to include access to the required [REDACTED] (if the team/team members do not already have access); 4) completed a review of the tracking information for confirmation of compliance activity due dates for CIP-009 R2.2; 5) developed standardized templates to be used for future functionality recovery testing evidence; 6) communicated the location of the templates to the teams responsible for the completion of functionality recovery testing; and 7) developed a job aid for new managers and individual contributors for CIP-009 compliance obligations. The job aid will include instructions for developing/updating recovery plans, overview of methods for conducting tabletop and operational drills and sign off obligations of managers for CIP 009 related documents. Relevant documents will be posted to the [REDACTED]. <p>ReliabilityFirst 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
RFC2018020029	CIP-011-2	R1	[REDACTED]	[REDACTED]	11/16/2017	7/19/2018	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 July 6, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-011-2 R1. On November 14, 2017, a CIP-qualified, entity-authorized contractor requested a group of substation and system protection drawings for a project at Substation A. In this group of drawings was a CIP protected diagram that contained Bulk Electric System (BES) Cyber System Information (BCSI), including [REDACTED] of BES Cyber Assets (BCAs) at Substation A.</p> <p>Two days later, a member of the [REDACTED] checked out the group of drawings to the contractor and placed all of the drawings on the corresponding [REDACTED] site. [REDACTED]</p> <p>Subsequently, on April 25, 2018, the [REDACTED] discovered that the CIP protected drawing was incorrectly placed on the [REDACTED] site without encryption. The drawing file was removed from the [REDACTED] site and the entity requested that the contractor run a scan to search for the drawing file on the contractor's servers and backups to ensure that the file was not present on any of their systems. The contractor determined that it had two copies of the drawing on its system, one on its [REDACTED] repository and one on its backup recovery tapes. The contractor removed both copies.</p> <p>The root cause of this noncompliance was the failure by the entity employee to realize the CIP protected nature of the drawing. The document management system that is used for checking out drawings to contractors did not properly display the entire drawing description, which would have included its CIP protected nature.</p> <p>This noncompliance started on November 16, 2017, when the entity placed the CIP protected drawing in the [REDACTED] folder without encryption and ended on July 19, 2018, when the entity ensured that the contractor had removed the drawing from its servers.</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 posed by failing to properly protect BCSI is that an unauthorized person could access the information and use it to adversely affect the BPS. This risk was mitigated in this case by the following factors. First, although the CIP protected drawing was not encrypted, it was contained in a [REDACTED] site that only CIP-qualified and entity-approved contractors could access due to password protection. Second, even if an unauthorized person had obtained the drawing, it only contained information for [REDACTED] to BCAs within Substation A. Therefore, that person would require physical access to Substation A or be able to bypass [REDACTED] to actually use the information. 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 noncompliances were the result of different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the folder containing the CIP Protected drawing from [REDACTED] site; 2) removed the drawing from the contractor servers; 3) [REDACTED] 4) [REDACTED] The entity communicated changes to impacted personnel. <p>ReliabilityFirst 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
RFC2018020208	CIP-010-2	R1			3/26/2018	4/12/2018	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 August 6, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. On April 10, 2018, during [REDACTED] review, the entity discovered certain software on a Supervisory Control and Data Acquisition (SCADA) workstation that was not reflected in the baseline review. Upon discovery, the entity's CIP compliance operations team contacted the entity's data maintenance group, who uses the device, and requested that the software be uninstalled.</p> <p>As background, the entity's [REDACTED] hired new contractors in January 2018 for SCADA projects. On March 6, 2018, one of the new contractors received a new console and logged on to perform job duties. The contractor navigated to the [REDACTED] menu and was presented with the [REDACTED] application available through [REDACTED] to a shared drive. The [REDACTED] tool is normally installed on consoles for the data maintenance team and this contractor had used this software on other data maintenance consoles in the past. So, when the contractor noticed that it was not installed on this console, he attempted to install it, but the installation failed.</p> <p>Subsequently, on March 26, 2018, this same contractor heard that data maintenance software had been loaded, tested, and approved on another system, he logged on to a production console and access the [REDACTED] tool from the Start menu. The application installed successfully, but was not operational because of some missing configuration settings. The entity [REDACTED] later discovered the software in the following baseline review.</p> <p>The root cause of this noncompliance was the contractor's incorrect assumption that the software available on the shared drive was approved for use on the device. Another contributing cause was the fact that the contractor had administrator rights to the console despite the fact that installing data maintenance software is the responsibility of the entity [REDACTED]. This root cause involves the management practices of external interdependencies, which includes managing the risk posed by external interdependencies, and asset and configuration management, which includes controlling changes to assets, configuration items, and baselines.</p> <p>This noncompliance started on March 26, 2018, when the contractor installed the software on the console and ended on April 12, 2018, when the entity removed the software from the console.</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 making unauthorized changes is that they could adversely impact the security or functionality of the impacted assets. This risk was mitigated in this case by the following factors. First, the entity quickly detected and corrected the issue through effective internal controls. Second, although the software was not authorized for the device it was inappropriately installed on, the software was prescreened and approved for use on other data maintenance consoles, which reduced the likelihood that it would have had an adverse impact on this console. 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 noncompliance posed a minimal risk to the reliability of the bulk power system, and ReliabilityFirst determined that the conduct at issue constitutes high frequency conduct for which the entity has shown the ability to quickly detect and correct through internal controls.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the original unauthorized software; 2) reviewed the incident during the weekly team stand down meeting; 3) relocated the [REDACTED] on the shared drive to a secured location only accessible by IT administrators; and 4) reviewed and adjusted Supervisory Control and Data Acquisition data maintenance roles in the access management system to limit their capabilities. <p>ReliabilityFirst 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
RFC2018019903	CIP-004-6	R5	[REDACTED]	[REDACTED]	2/11/2018	2/28/2018	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 June 8, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. On February 27, 2018, the entity discovered that it had terminated an intern, but failed to remove all of the intern's non-shared user accounts within 30 calendar days. The entity terminated the intern on January 12, 2018, but did not remove the intern's non-shared user accounts until February 28, 2018.</p> <p>Generally, the majority of entity interns, [REDACTED] are managed more collectively by HR with pre-established termination dates. [REDACTED]</p> <p>In this case, the intern's supervisor performed the off-boarding process on January 12, 2018, during which he removed the intern's unescorted physical access and electronic access by collecting the intern's badge and laptop. (The intern was never granted electronic remote access.) However, the supervisor mistakenly believed that this particular intern's termination would be managed by the termination tracker program [REDACTED].</p> <p>The root cause of this noncompliance was the supervisor's mistaken belief that he did not have to contact HR directly to inform them of the intern's termination. This major contributing factor involves the management practice of workforce management, which includes managing employee's access to assets.</p> <p>This noncompliance started on February 11, 2018, the date by which the entity was required to have removed the intern's non-shared user accounts and ended on February 28, 2018, when the entity completed this removal.</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 posed by failing to remove a terminated employee's non-shared user accounts within 30 calendar days is that the employee could utilize those accounts for an improper purpose after termination. This risk was mitigated in this case by the following factors. First, the supervisor removed the intern's unescorted physical access and electronic access by collecting the intern's badge and laptop. Therefore, the intern had no ability to utilize any remaining access rights in the system following termination because he no longer had physical or electronic access. Second, the intern was never granted electronic remote access rights and would not have had the ability to login remotely. Third, the intern was a trusted individual with current CIP training and a Personnel Risk Assessment, which reduces the likelihood that he would have done anything nefarious if he could have access these accounts. 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 noncompliances were the result of different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) provided evidence showing the responsible group fully disabled the intern's accounts access rights; 2) provided evidence showing human resource generalist met with the supervisor of the intern to discuss and report the intern termination for this intern; 3) [REDACTED]; 4) developed a template that will populate end dates for the intern resources. The entity downloaded these resources from [REDACTED] into the template. The entity entered a projected end date for the interns; 5) developed a template that will populate end dates for intern [REDACTED] resources. The entity downloaded these resources from [REDACTED] into the template; 6) developed a report that lists all interns (existing and new job codes) that have a NERC role and includes the end date and the assigned operating company. [REDACTED] 7) sent an email to HR providing reminders/instructions for off-boarding interns, focusing on end dates; 8) updated the manager toolkit for interns; 9) reviewed out processing guidelines for managers and updated, if/as needed, for inclusion of intern out processing steps; 10) provided "Train the Trainer" training to HR personnel regarding the updated process for tracking intern onboarding and off-boarding processes, keeping end dates current and to notify appropriate personnel if any end dates change; 11) provided training to entity managers of interns regarding the updated process for tracking intern onboarding and off-boarding processes, keeping end dates current and to notify appropriate personnel if any end dates change; 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019903	CIP-004-6	R5	[REDACTED]	[REDACTED]	2/11/2018	2/28/2018	Self-Report	Completed
			12) developed and implemented auto-terminate for all Interns; 13) automated notification to managers of upcoming terminations for all interns; and 14) performed a quality review of the automated process to ensure the recruiters and Sr. HR business partners are receiving weekly emails and report and confirmed recruiters and Sr. HR business partners are monitoring and populating the projected end dates for interns [REDACTED] with NERC roles. ReliabilityFirst has verified the completion of all mitigation activity.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020741	CIP-007-6	R4	[REDACTED]	[REDACTED]	7/30/2018	8/2/2018	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 November 21, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R4.</p> <p>On July 30, 2018, two Electronic Access Control or Monitoring Systems (EACMS) located at the entity backup control center restarted due to an unknown origin and became inaccessible. The administrator contacted the vendor and worked with the vendor. Through troubleshooting scripts, it was discovered that several services were found not to be "bound." These services were restored to a "bound" status and normal operations resumed. As part of the troubleshooting, one service, the syslog service, was not started. The syslog service provides local logging support, and because failed logins were neither being recorded nor retained, the ability to alert on failed logins was interrupted.</p> <p>This issue was discovered on August 2, 2018, during the administrator's weekly review of sampling the logs of the root account in accordance with CIP-007-6 R4 part 4.2.2. The administrator had knowledge that he logged in on July 30, 2018, but discovered that the successful logins he generated were not reflected in the log sampling report he was reviewing. Therefore, the logs were not retaining the required 90 consecutive calendar days logins.</p> <p>The root cause of this noncompliance was the failure to log the elements required for the root account login when the syslog service lost their "binding" to the syslog service when the systems restarted and became inaccessible.</p> <p>This noncompliance involves the management practices of external interdependencies and verification. External interdependencies management is involved because the entity coordinated with the [REDACTED] [REDACTED] to manage the recovery process which was ineffective and helped cause this instance of noncompliance. Verification management is involved because entity staff did not verify that all services, including the syslog service, were started following the "binding" process.</p> <p>This noncompliance started on July 30, 2018, when the syslog service was not started and logs were not recorded or retained, and ended on August 2, 2018, when the entity re-binded the syslog service and restored the logging functionality.</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 risk posed by the entity's failure to log the required elements for the root account login had the potential to affect the reliable operation of the BPS by impeding a Registered Entity's ability to identify and investigate Cyber Security Incidents. This risk was mitigated in this case by the following factors. First, the devices are monitored continuously. Second, the entity has the following protections in place: they reside in a Physical Security Perimeter, they are on an internally protected network with other EACMS, they are protected by multiple layers of firewalls, and they have antivirus and malware prevention tools. Third, the noncompliance lasted for a short duration of time of fewer than four days. 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 different root causes 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) started the syslog service which restored logging; 2) reviewed the available security logs to ensure logging is occurring; 3) upgraded to a new version; and 4) performed training on how to check syslog service if the Device Reboots. <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
TRE2017018030	CIP-007-6	R5; R5.2; R5.4	██████████	██████████	July 1, 2016	May 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 July 27, 2017, the entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-007-6 R5. According to the entity, it discovered a number of active generic accounts that were not properly documented in accordance with CIP-007-6 R5, Part 5.2. The entity stated that this issue likely occurred because it did not consider inventorying all application-layer identity stores to verify accounts were documented. Furthermore, the entity stated that it also failed to change the default password on one BES Cyber Asset (BCA) in accordance with CIP-007-6 R5, Part 5.4.</p> <p>A total of ██████████ active generic accounts were not properly documented pursuant to CIP-007-6 R5.2.</p> <p>This noncompliance started on July 1, 2016, when CIP-007-6 R5 became enforceable and ended on May 13, 2017, when all default passwords had been changed and all default accounts were documented.</p> <p>The root causes of this non-compliance were a lack of proper procedures and a failure to follow existing procedures. During the transition to CIP Version 5 the entity performed a gap analysis to determine the tasks that would need to be completed to achieve compliance. Upon review the entity does not appear to have considered a full inventory of application-layer identity stores to locate additional default accounts. In regards to the Cyber Asset with a default password, the entity changed the passwords on all but one Cyber Asset at that BES Asset location on two separate occasions.</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 in not identifying enabled default accounts is cyber security staff may be unaware of the accounts, which can lead to the accounts not having their passwords changed from their defaults, not being changed on a regular basis, etc. The risk in not changing default passwords is an attacker can use publicly known default credentials to gain access to a system and cause harm.</p> <p>The risk of these issues is mitigated due to the following:</p> <ol style="list-style-type: none"> 1) ██████████ the undocumented generic accounts cannot be used for interactive access. 2) ██████████ the undocumented generic accounts were only present on a single PCA. 3) The cyber asset with a default vendor password does not have External Routable Connectivity. <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) Documented the ██████████ previously undocumented generic accounts. 2) Changed the default password on the BES Cyber Asset that was using a default password. 3) Where feasible added automation to regularly check for new default accounts (such as those added by a patch). 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Mitigation Completion Date
TRE2017016876	CIP-010-2	R1; R1.1; R1.2; R1.3; R1.4; R1.5	[REDACTED]	[REDACTED]	07/01/2016	04/19/2017	Compliance Audit	11/01/2018
<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], Texas RE determined that [REDACTED] as a [REDACTED] was in noncompliance with CIP-010-2 R1 in two instances. Both instances were self-identified by [REDACTED] during the Compliance Audit.</p> <p>The first instance was discovered by [REDACTED] during the review of a daily baseline configuration monitoring report. [REDACTED] as required by CIP-010-2 R1, Part 1.2. Further, [REDACTED] failed to perform the security controls verification and testing requirements per CIP-010-2 R1, Parts 1.4 and 1.5. This instance of noncompliance lasted two days.</p> <p>The root cause of the first instance was insufficient processes and controls for deploying software. [REDACTED] used [REDACTED] As a result [REDACTED] Additionally, [REDACTED] also lacked internal controls to ensure effective communication among personnel that perform changes to Cyber Assets.</p> <p>The second instance was discovered by [REDACTED] during a review of [REDACTED]. [REDACTED] failed to classify [REDACTED] Cyber Assets as Electronic Access Control or Monitoring Systems (EACMS). During the transition to the CIP Version 5 Reliability Standards, the [REDACTED] Cyber Assets at issue were identified and intended to be classified as EACMS. However, [REDACTED] failed to appropriately classify the [REDACTED] Cyber Assets in its asset management system. Therefore, [REDACTED] failed to develop baseline configurations for the [REDACTED] Cyber Assets as required by CIP-010-2 R1, Part 1.1. Additionally, for each EACMS, [REDACTED] did not authorize and document changes that deviate from the baseline configuration, update the baseline configuration within 30 days of completing a change, and ensure CIP-005 and CIP-007 cyber security controls were not impacted by change, per CIP-010 2 R1, Parts 1.2, 1.3, and 1.4. This instance of noncompliance lasted less than ten months.</p> <p>The root cause of the second instance was insufficient controls to ensure Cyber Assets were appropriately classified during the transition to CIP Version 5 Reliability Standards. [REDACTED] method to classify a Cyber Asset as in-scope for the CIP Version 5 Reliability Standards required the manual completion of a compliance data tab in its asset management system.</p> <p>This noncompliance started on July 1, 2016, when CIP-010-2 R1 went into effect and [REDACTED] had not developed a baseline configuration for the [REDACTED] EACMS in the second instance. This noncompliance ended on April 19, 2017, when the baseline configurations were established for the [REDACTED] in the second instance.</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 is reduced by the following factors. Only [REDACTED] Cyber Asset was impacted in the first instance and [REDACTED] Cyber Assets were impacted in the second instance. In the first instance the issue was quickly detected through effective internal controls. Additionally, the first instance was quickly remediated so that the noncompliance duration was only two days. If the first instance had caused a malfunction of the impacted workstation, [REDACTED] stated that it had the ability [REDACTED]. For the second instance, the Cyber Assets were configured for [REDACTED]. Additionally, monthly operating system patching was taking place on the Cyber Assets in the second instance to address vulnerabilities. Lastly, the Cyber Assets in the second instance were [REDACTED]</p> <p>No harm is known to have occurred.</p> <p>Texas RE considered [REDACTED] and its affiliate's compliance history in determining the disposition track and determined that [REDACTED] compliance history should not serve as an aggravating factor.</p>					
<p>Mitigation</p>			<p>To mitigate the first instance of noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) removed the unauthorized software; 2) reviewed a list of all workstations to ensure the appropriate tagging and branch structure in the software deployment system; 					

Texas Reliability Entity, Inc. (Texas RE)

Compliance Exception

CIP

3 [REDACTED]
 ; [REDACTED]
 4) [REDACTED]
 ; [REDACTED]
 5) [REDACTED] and
 6) [REDACTED].

To mitigate the second instance of noncompliance, [REDACTED]

- 1) developed baseline configurations for the impacted Cyber Assets;
- 2) finalized compliance data in the asset management system to appropriately classify the impacted Cyber Assets as EACMS;
- 3) developed and implemented task lists for any new Cyber Asset that includes tasks for completing the compliance data tab and developing the baseline configuration; and
- 4) [REDACTED]

Texas RE 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
WECC2017017871	CIP-007-6	R1; P1.2	[REDACTED]	[REDACTED]	7/1/2016 (when the Standard and Requirement became mandatory and enforceable to [REDACTED])	6/27/2017 (when port locks, where possible, were installed, and signage was placed on the rack of the BCAs in scope)	Self-Report	8/31/2018
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, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED], it was in violation with CIP-007-6 R1. Specifically, [REDACTED] reported that on June 22, 2017, during a site walkthrough, it discovered that unnecessary physical input/output ports on [REDACTED] managed switches classified as Bulk Electric System (BES) Cyber Assets (BCAs) that were part of two High Impact BES Cyber Systems (HIBCS), were not protected according to the Standard and Requirement Part 1.2. The managed switches were connected to terminal servers, digital input/output devices and additional managed switches for the function of [REDACTED].</p> <p>After reviewing all relevant information, WECC determined that [REDACTED] failed to protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media for [REDACTED] ports on [REDACTED] BCAs that were part of the HIBCS, and not [REDACTED] BCAs as was originally Self-Reported by [REDACTED] as required by CIP-007-6 R1 Part 1.2.</p> <p>The root cause of the issue was a miscommunication between two [REDACTED] groups. Specifically, [REDACTED] compliance group believed that the technicians had logically disabled the physical input/output ports, when in fact they had not been disabled. There was also a lack of documentation of the physical input/output ports for each device in scope which also contributed to the cause.</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to [REDACTED] and ended on June 27, 2017, when port locks, where possible, were installed, and signage was placed on the rack of the BCAs in scope, for a total of 362 days of noncompliance.</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. In this instance, [REDACTED] failed to protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media for [REDACTED] ports on [REDACTED] BCAs that were part of the HIBCS, as required by CIP-007-6 R1 Part 1.2. Such failure could allow a malicious actor to gain access to the unprotected physical ports potentially causing the loss of visibility and/or inaccurate situational awareness. Additionally, network cables or USB devices could be connected to the BCAs, which could lead to undocumented network connectivity or allow a malicious actor to upload a malicious code, potentially compromising the data sent from the meters, and leading the Control Center personnel to adjust the load based on inaccurate readings. [REDACTED] owns and/or operates [REDACTED] MW of BES generation and has [REDACTED] MW of generation in its Balancing Authority footprint; [REDACTED] miles of transmission; [REDACTED] BES interconnection points with [REDACTED] other entities; and owns and operates elements of [REDACTED] Major WECC Transfer Paths, that were applicable to this issue. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as intermediate.</p> <p>However, [REDACTED] implemented good internal controls. WECC verified [REDACTED] that the BCAs were located within the Physical Security Perimeter (PSP) which required two-factor authentication for authorized entry and was constantly manned with operators who would notice any changes to the equipment. Also, operators had the ability to switch to an alternate source for the [REDACTED] or [REDACTED]. Additionally, [REDACTED] conducted baseline configuration checks every 35-calendar days and would have identified if any ports/services had changed. As further compensation, access to unprotected ports require a username and password as well as configuration settings where [REDACTED] failed login attempts would lockout the account. These login attempts would be logged and reviewed every 15 days. Lastly, the data that traverses the [REDACTED]; therefore, should the data be manipulated or otherwise be made unavailable due to the misuse of the [REDACTED], dispatchers would verify against the other data sources and take appropriate action. 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>Upon undertaking the actions outlined in the Mitigation Plan, [REDACTED] took voluntary corrective action to remediate this issue. WECC considered [REDACTED] compliance history in its designation of this remediated issue as a CE. [REDACTED] prior noncompliance with CIP-007 R1 includes NERC Violation IDs [REDACTED] and [REDACTED]. WECC determined that the circumstances and cause of those issues was distinct and separate than that of the current issue and are not considered an aggravating factor.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) installed signage on the racks that contained the devices in the [REDACTED] BES Cyber Systems which alerts individuals to the critical equipment and warns against touching the devices without possessing the proper authorization; 2) installed port blocks, where possible, to physically prevent individuals from using unnecessary input/output ports that have not already been logically disabled; 3) implemented a tracking spreadsheet to communicate the status and necessity of all physical input/output ports on BCAs in the [REDACTED] HIBCS; 4) updated its ports and services procedure to provide details regarding the physical input/output port tracking process and referenced the new tracking spreadsheet; and 5) provided awareness training to substation operator technicians regarding the changes to the ports and services 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
WECC2017018751	CIP-004-6	R5; P5.4	[REDACTED]	[REDACTED]	6/19/2017	6/30/2017	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 December 5, 2017, the entity submitted a Self-Report stating, as a [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED], it was in noncompliance with CIP-004-6 R5. Specifically, on June 30, 2017 during a quarterly review of individuals with electronic access to 45 Cyber Assets associated with the High Impact Bulk Electric System (BES) Cyber Systems (HIBCS), the entity discovered one non-shared user account, which did not have Interactive Remote Access, that was not revoked within 30 calendar days of Friday, May 19, 2017 when an individual resigned. On the date of resignation, a notification was sent to certain individuals responsible for revoking electronic access to the Cyber Assets. However, the individual who sent the notification inadvertently omitted certain staff who were responsible for revoking user accounts. The individuals who did receive the notification were under the assumption that the task was not their responsibility.</p> <p>After reviewing all relevant information, WECC determined the entity failed to revoke one terminated individual's non-shared user account within 30 calendar days of the effective date of the termination action, as required by CIP-004-6 R5 Part 5.4.</p> <p>The root cause of the issue was omission of steps due to assumptions for completion and responsibilities not well defined. Specifically, the individuals who received the termination notification assumed the task would be completed by other individuals.</p> <p>This noncompliance started on June 19, 2017, when the terminated individual's non-shared user account was not revoked within 30 calendar days of the termination action, and ended on June 30, 2017, when the terminated individual's access to non-shared user accounts was revoked, for a total of 12 days.</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. In this instance, the entity failed to revoke one individual's non-shared user account within 30 calendar days of the effective date of the termination action, as required by CIP-004-6 R5 Part 5.4. The BCAs in scope were protected by a Physical Security Perimeter, to which the terminated individual did not have unescorted physical access during the noncompliance, nor did they have Interactive Remote Access or access to any shared accounts to Cyber Assets. Additionally, the terminated individual's non-shared user account was restricted to read-only access and they could not operate the Energy Management System. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty. The entity's relevant prior compliance history with CIP-004-6 R5 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 a basis for escalating to an enforcement action and applying a penalty.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) revoked the terminated individual's non-shared user account; 2) reviewed records and did not find any additional instances of non-shared user account access not being revoked with 30 calendar days of termination actions. The review showed, with the exception of the earlier identified employee who resigned, all their accounts were revoked in a timely manner; 3) updated the contact list to include the group that issues physical access revocation and the group that issues electronic access revocation; 4) provided training to all individuals responsible for issuing electronic access revocation on what is expected for revoking electronic access and how they will be notified via email; and 5) assigned monthly reviews, for three months, of the new email process and electronic revocation put in place in order to ensure that they were understood and followed. <p>WECC 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
WECC2017017876	CIP-004-6	R4: P4.1	[REDACTED]	[REDACTED]	7/1/2016	3/15/2017	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 June 29, 2017, the entity submitted a Self-Report stating, as a [REDACTED] it was in noncompliance of CIP-004-6 R4. Specifically, during two separate internal reviews, the entity discovered ten individuals who had more access than was appropriate for their business needs. The first issue was identified during the entity's 2016 annual access review where it looked at roles, the access granted through those roles, and the individuals within those roles, and then cross referenced those individuals with their authorization record to ensure access was properly granted and documented. This review identified four instances where individuals had access through their role assignment that did not match their authorization record. During a separate internal review conducted in preparation for the implementation date for [REDACTED], the entity required its supervisors to confirm lists of personnel that had or would have a [REDACTED]. During this review, the entity identified six individuals that did not appear on its original list. These individuals had current Personnel Risk Assessments (PRAs) and CIP Training, but were not properly identified within the role or documented in the entity's [REDACTED]. All ten individuals had electronic access, unescorted physical access into a Physical Security Perimeter (PSP), and/or access to designated storage locations, whether physical or electronic, for BES Cyber System Information (BCSI) related to its High Impact BES Cyber System (HIBCS) and/or Medium Impact BES Cyber System (MIBCS) substations.</p> <p>The entity implemented access using defined roles. Using the defined roles, a supervisor's approval for an employee to be given a role provided the approval for the access defined within the role. In this case, the granted roles inadvertently allowed CIP access that was not specifically intended. In some cases, specific access should have been requested instead of being added to the defined role, and in others, the role privilege should not have included specialized CIP access. These identified roles have been updated to avoid the reoccurrence of this issue. For the documentation of individual access, updated access requests were submitted for the individuals that had access but no evidence of authorization.</p> <p>After reviewing all relevant information, WECC determined that for ten individuals, the entity failed to appropriately implement its process to authorize, based on need, electronic access; unescorted physical access into a PSP; and access to designated storage locations, whether physical or electronic, for BCSI, as required by CIP-004-6 R4 Part 4.1.</p> <p>The root cause of the issue was a less than adequate process. Specifically, in its process, the entity failed to account for all access applicable to R4.1. and consequently, grouped access roles together when all roles should not have included all access. Rather, specific access should have been requested instead of being added to the defined role.</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable, and ended on March 15, 2017, when the appropriate authorization was completed for individuals who needed access or the access was revoked for individuals who did not need it, for a total of 258 days.</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. In this instance, the entity failed to appropriately implement its process to authorize, based on need, electronic access; unescorted physical access into a PSP; and access to designated storage locations, whether physical or electronic, for BCSI, as required by CIP-004-6 R4 Part 4.1.</p> <p>However, the entity implemented good preventive controls. Specifically, it implemented a need-to-know process for Interactive Remote Access (IRA) to Cyber Assets. Although some of the individuals in scope of this issue had been granted IRA, they did not have login credentials for that access. Additionally, the entity utilized an internal application that would alert if any changes were made to the BCAs. All locations were monitored 24 hours a day. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty. The entity's relevant prior compliance history with CIP-004-6 R4 includes NERC Violation ID [REDACTED]. WECC determined the entity's compliance history should not serve as a basis for pursuing and enforcement action and/or applying a penalty. Regarding NERC Violation ID [REDACTED], this violation dealt with revoking access after an employee had left the entity, which was distinct, separate, and not relevant to these issues.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the access for individuals where it was not needed; 2) completed access requests and appropriately tracked individuals who did need access; 3) updated its process so that CIP access must be manually requested and granted; 4) updated its quarterly access review process to include reviews of all CIP roles; 5) created one team to handle the provisioning of unescorted physical and electronic access in order to create uniformity in its process and avoid errors in the future; and 6) created weekly meetings to discuss CIP access, including roles, groups, access requests, renaming groups, and CIP access for non-Active Directory integrated systems. <p>WECC 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
WECC2017018583	CIP-004-6	R4: P4.2	██████████	██████████	10/1/2016	12/29/2017	Compliance 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 violation.)			<p>During a Compliance Audit conducted from ██████████ through ██████████, WECC determined that the entity, as a ██████████, had a potential noncompliance of CIP-004-6 R4. Specifically, WECC auditors determined the entity had been verifying at least once each calendar quarter that individuals with active electronic access or unescorted physical access had authorization records; however, the entity was only verifying individuals that were authorized during the quarter, and was not performing a verification of all individuals with active electronic access or unescorted physical access to confirm they had authorization records. The entity was not aware that the review must include dated documentation of the verification between a list of individuals who had been authorized for access and a list of individuals provisioned for access, not just a change control listing of changes that occurred during the review period.</p> <p>After reviewing all relevant information, WECC determined the entity failed to verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access had authorization records, as required by CIP-004-6 R4 Part 4.2.</p> <p>The root cause of the issue was an incorrect interpretation of the newly enforceable CIP Version 5 Standard and Requirement. Specifically, the entity did not understand that CIP-004-6 R4 Part 4.2 required it to review quarterly all individuals with active electronic access or unescorted physical access to validate authorization records, and not just those that had been approved during the quarter.</p> <p>This noncompliance started on October 1, 2016, when the initial performance of the Requirement became enforceable, and ended on December 29, 2017, when the entity completed the verification of authorization records against active access for all individuals, for a total of 455 days.</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. In this instance, the entity failed to verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access had authorization records, as required by CIP-004-6 R4 Part 4.2.</p> <p>However, the entity implemented good controls. The entity had a process in place to review authorization records as least once before provisioning electronic access or unescorted physical access for all individuals. Additionally, the entity utilized an internal application that would alert if any changes were made to the Cyber Assets. All locations were monitored 24 hours a day. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty. The entity's relevant prior compliance history with CIP-004-6 R4 includes NERC Violation ID ██████████. WECC determined the entity's compliance history should not serve as a basis for pursuing and enforcement action and/or applying a penalty. Regarding NERC Violation ID ██████████, this violation dealt with revoking access after an employee had left the entity, which was distinct, separate, and not relevant to these issues.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) verified that all individuals who had active electronic access or unescorted physical access had authorization records; 2) updated its process to include desk-level procedures for the quarterly access reviews to include the verification of authorization records for all individuals with active electronic access or unescorted physical access; and 3) implemented a ticketing system to issue a quarterly work order at the time the quarterly review should be completed. The product of the review is reviewed by the entity's legal team before it is approved. <p>WECC 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
WECC2017017878	CIP-007-6	R2: P2.3	[REDACTED]	[REDACTED]	7/1/2016	3/26/2018	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 violation.)			<p>On July 7, 2017, the entity submitted a Self-Report stating, as a [REDACTED], it was in noncompliance of CIP-007-6 R2. Specifically, the entity reported that it identified three separate times in which it did not properly implement its security patching procedure. On September 26, 2016 during an assessment of security patches, it discovered a security patch for two BCAs in the MIBCS with External Routable Connectivity (ERC), which was released on July 12, 2016, but was not evaluated for applicability within the 35 days. Additionally, the entity identified security patches that were assessed as applicable for four other BCAs in the MIBCS with ERC that were never installed. On September 15, 2017 the entity identified additional security patches for four BCAs in the HIBCS that the entity had not evaluated as applicable; therefore, for applicable security patches did it apply the security patch; create a dated mitigation plan; or revise an existing mitigation plan, within the required 35 calendar days. Lastly, on March 6, 2018, the entity discovered a security patch that was released in July of 2017 and assessed as applicable for one BCA in the MIBCS without ERC, in a timely manner; however, the entity did not apply the applicable security patch, create a dated mitigation plan, or revise an existing mitigation plan, within the required 35 calendar days.</p> <p>After reviewing all relevant information, WECC determined the entity failed to effectively implement its security patch management process for tracking, evaluating, and installing cyber security patches, as required by CIP-007-6 R2 Part 2.1; failed to at least once every 35 calendar days, to 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; and failed for applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion either apply the applicable patches; create a dated mitigation plan; or revise an existing mitigation plan, as required by CIP-007-6 R2 Part 2.3.</p> <p>The root cause of the issue was a less than adequate security patch management process. Specifically, the entity did not have a process or a tool in place to receive security patch alerts from the patch sources associated with the security patches specific to this issue.</p> <p>This noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on March 26, 2018, when the entity completed mitigation, for a total of 634 days.</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. In this instance, the entity failed to effectively implement its security patch management process for tracking, evaluating, and installing cyber security patches, as required by CIP-007-6 R2 Part 2.1; failed to at least once every 35 calendar days, to 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; and failed for applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion either apply the applicable patches; create a dated mitigation plan; or revise an existing mitigation plan, as required by CIP-007-6 R2 Part 2.3., for 11 Cyber Assets associated with the HIBCS and MIBCS.</p> <p>The entity implemented good compensating controls in that its HIBCS and MIBCS were monitored 24 hours a day in real-time. If any abnormal activity had occurred, the entity's [REDACTED] team would have been alerted to troubleshoot and mitigate any potential attacks. Additionally, all Cyber Assets in scope were physically secured and only authorized individuals with a “need to know”, and a current Personnel Risk Assessment had access. The Cyber Assets used for physical access control and monitoring [REDACTED].</p> <p>No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty. The entity's relevant prior compliance history with CIP-004-6 R4 includes NERC Violation ID [REDACTED]. WECC determined the entity's compliance history should not serve as a basis for pursuing and enforcement action and/or applying a penalty.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) applied a security patch to one of the Cyber Assets; 2) created a mitigation plan for six of the Cyber Assets; 3) revised an existing mitigation plan to include four of the Cyber Assets; 4) updated its process to include a weekly review of security patches as part of its change control meetings, to include tracking patch mitigation plan deadlines and tracking the manual patch review process; 5) updated its security patch management workbook to more clearly define the timeframe for security patch assessments, application, and management of mitigation plans; 6) updated its security patch mitigation plan template to keep historical records of due date, mitigation plan dates, names, and compensating measures; 7) updated its security patch management procedure to include a notification process in which both the primary and back up personnel receive notifications of security patches; 8) updated its security patch management workbook to clarify the timeframe for security patch assessment and the security patch application or management of mitigation plans; and 9) conducted training on its updated security patch management process to applicable personnel. <p>WECC 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
WECC2018020339	CIP-003-6	R1	[REDACTED]	[REDACTED]	4/1/2017	7/5/2018	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 violation.)			<p>On September 4, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-003-6 R1. Specifically, on July 12, 2018, the entity discovered that an employee, who had delegated authority from the CIP Senior Manager, had reviewed and approved its documented cyber security policies, which addressed Cyber Assets associated with its Low Impact Bulk Electric System (BES) Cyber System (LIBCS). Based on the entity's interpretation of CIP-003-6 R4, it believed it could delegate authority for this specific action. However, CIP-003-6 R1 does not allow the CIP Senior Manager to delegate approval of cyber security policies.</p> <p>After reviewing all relevant information, WECC determined the entity failed to obtain approval from its CIP Senior Manager for its documented cyber security policies, which addressed assets associated with its LIBCS, as required by CIP-003-6 R1.</p> <p>The root cause of the issue was the entity's misunderstanding of the application of CIP-003-6 R4, and therefore it delegated the approval of its cyber security policies.</p> <p>This noncompliance started on April 1, 2017, when the entity's cyber security policies should have been approved by the CIP Senior Manager and ended on July 5, 2018, when the entity obtained said approval, for a total of 461 days.</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. In this instance, the entity failed to obtain approval from its CIP Senior Manager for its documented cyber security policies which address assets associated with its LIBCS as required by CIP-003-6 R1. This was a documentation issue and the employee who approved the documented cyber security policies had previously been the CIP Senior Manager. Additionally, the entity has [REDACTED] generating facility applicable to this issue, therefore the inherent risk is [REDACTED]. No harm is known to have occurred.</p> <p>WECC determined the entity did not have any relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) obtained CIP Senior Manager approval of its cyber security policies; and 2) updated its task management software with the logic to assign future approvals to the CIP Senior Manager to approve its cyber security policies. <p>WECC 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
WECC2017017301	CIP-007-6	R2	[REDACTED]	[REDACTED]	7/1/2016	5/8/2017	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 24, 2017, the entity submitted Self-Reports stating that, as a [REDACTED] and [REDACTED] it had several issues with CIP-007-6 R2, R4, R5, and CIP-010-2 R1.</p> <p>Specifically, the entity reported that in November of 2016 it hired a consultant to perform a mock audit of its CIP Version 5 implementation to ensure there were no gaps. In preparation for, and during the mock audit, the entity discovered the following issues:</p> <ol style="list-style-type: none"> Ten protection relays classified as Bulk Electric System (BES) Cyber Assets (BCAs) without External Routable Connectivity (ERC), one remote terminal unit (RTU) classified as a Physical Access Control System (PACS) and seven firewalls classified as Electronic Access Control or Monitoring Systems (EACMS) with ERC, all associated with the entity's Medium Impact BES Cyber System (MIBCS), located at its [REDACTED], were obsolete or at end-of-life; therefore security patches were no longer available. As such, the security patch source (Vendor) that the entity identified for tracking the release of applicable cyber security patches removed the obsolete or end-of-life Cyber Assets from the patching report but failed to notify the entity that they had done so. The entity did not notice the discrepancy from what it had originally submitted to the Vendor. (CIP-007-6 R2 Part 2.1) Eight protection relays classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] were originally submitted to the Vendor who acknowledged it could support the Cyber Assets; however, the Cyber Assets did not show up on the security patch report sent to the entity for patch evaluation and again, the entity did not notice the discrepancy from what it had originally submitted to the Vendor. (CIP-007-6 R2 Part 2.1) Three additional protection relays classified as BCAs associated with the entity's MIBCS without ERC, located at its [REDACTED], originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, were not included on the list of Cyber Assets sent to the Vendor to monitor for security patches; therefore, were not being tracked for security patches. These protection relays were installed after the entity had inventoried its substations in preparation for transitioning to CIP Version 5. The three protection relays had no network ports. (CIP-007-6 R2 Part 2.1) The entity security patch evaluation report from the Vendor for [REDACTED] software was received on September 12, 2016; however, the entity completed the evaluation on October 17, 2016, four days after the 35 calendar day requirement. The entity had switched from a patch aggregator tool that allowed personnel to login and access patches on their own schedule to a new Vendor who provided the monthly report which caused some timely confusion in completing the evaluations and patching within the required timelines for one BCA. (CIP-007-6 R2 Part 2.2) One protection relay classified as a BCA associated with the entity's MIBCS without ERC, located at its [REDACTED], had an applicable security patch identified by the Vendor and submitted to the entity on September 20, 2016; however, the entity failed to see that the security patch was released and subsequently it was not evaluated within 35 calendar days. (CIP-007-6 R2 Part 2.2) The entity did not create a mitigation plan or update an existing mitigation plan for a security patch for one protection relay classified as a BCA associated with the entity's MIBCS without ERC, located at its [REDACTED], that it had evaluated as applicable but could not apply due to compatibility issues. The entity had not considered that patching for some substation BCAs would be impacted by BCAs at the other end of the line and coordination with other entities might require additional time to execute a patch. (CIP-007-6 R2 Part 2.3) Three protection relays, classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] were originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, were not enabled to log events by July 1, 2016. The protection relays were installed after the entity had inventoried its substations in preparation for transitioning to CIP Version 5. The substation procedure applicable to Cyber Assets under CIP Version 5 detailed the requirements for logging events as required by CIP-007-6 R4 Part 4.1; however, it was not in effect at the time the three protection relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process. (CIP-007-2 R4 Part 4.1) Three protection relays classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, did not have the factory default passwords changed by July 1, 2016, the mandatory and enforceable date of CIP-007-6 R5 Part 5.4. The substation procedure applicable to Cyber Assets under CIP Version 5 detailed the requirements for changing default passwords; however, it was not in effect at the time the three protection relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process. (CIP-007-6 R5 Part 5.4) 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017301	CIP-007-6	R2	[REDACTED]	[REDACTED]	7/1/2016	5/8/2017	Self-Report	Completed
			<p>i. The entity did not develop a baseline configuration for the [REDACTED] software installed on two Energy Management System (EMS) servers, two Inter-Control Center Communication Protocol (ICCP) servers, and 18 Supervisory Control and Data Acquisition (SCADA) workstations, all classified as BCAs associated with the entity's HIBCS at its primary and backup Control Centers. The entity's subject matter experts did not adequately consider the requirement to baseline beyond the operating system and network configuration. (CIP-010-2 R1 Part 1.1 sub-parts 1.1.2 and 1.1.3)</p> <p>j. Three protection relays classified as BCAs without ERC associated with the entity's MIBCS located at its [REDACTED] originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, did not have baseline configurations developed by July 1, 2016. The substation procedure applicable to Cyber Assets under CIP Version 5 was not in effect at the time the three relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process, as such, the substation personnel did not know the steps they were to follow to ensure the new BCAs were CIP compliant. (CIP-010-2 R1 Part 1.1)</p> <p>Additionally, WECC determined that the entity had an increase in scope from what it originally Self-Reported. The entity did not enforce password parameters for one protection relay classified as a BCA associated with the MIBCS without ERC located at its [REDACTED], as required by CIP-007-6 R5 Part 5.5, and the entity did not consider sub-parts 1.4.1, 1.4.2, and 1.4.3 for a change that deviated from the existing baseline configuration for one Physical Access Control System (PACS) and two EACMS associated with the HIBCS, as required by CIP-010-2 R1 Part 1.4.</p> <p>After reviewing all relevant information, WECC determined, for CIP-007-6 R2, that the entity failed to appropriately implement a patch management process by not identifying patch sources for all applicable devices; at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the sources identified in Part 2.1; and for applicable patches, identified in Part 2.2, within 35 calendar days of the evaluation completion, either apply the applicable patch, create a dated mitigation plan, or revise an existing mitigation as required by CIP-007-6 R2 Parts 2.1, 2.2, and 2.3.</p> <p>The root cause of CIP-007-6 R2 was the entity did not have a process in place to compare the list of Cyber Assets requested to be monitored for patches against the report received from the source; for Part 2.2, the entity did not have a formal schedule to organize the various patch management activities and SME's were not familiar with the format of the new reports which contributed to them not seeing the applicable patch; and for Part 2.3, the entity did not have enough time built into the existing process to escalate a "bad patch" and to include a mitigation plan.</p> <p>WECC determined that the noncompliance start date for CIP-007-6 R2 began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable to the entity, and the ended on May 8, 2017 when the entity met the requirements of the Standards.</p>					
Risk Assessment			<p>WECC determined that CIP-007-6 R2 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). The entity failed to appropriately implement a patch management process by not identifying patch sources for all applicable devices; at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the sources identified in Part 2.1; and for applicable patches, identified in Part 2.2, within 35 calendar days of the evaluation completion, either apply the applicable patch, create a dated mitigation plan, or revise an existing mitigation as required by CIP-007-6 R2 Parts 2.1, 2.2, and 2.3. Such failure could potentially result in the inability to identify and patch vulnerabilities on CIP Cyber Assets which could allow malicious actors to gain access to the Cyber Assets using known vulnerabilities to cause misoperation. The entity has a HIBCS and MIBCS for which these Cyber Assets were applicable; it owns [REDACTED] of generation, has [REDACTED] transmission line, [REDACTED] transmission lines, and partially owns an additional [REDACTED] transmission line. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as minor.</p> <p>However, the entity implemented good internal controls. Specifically, the majority of Cyber Assets in scope were not configured with ERC and could only be accessed using dedicated laptops managed by the entity's IT department, which were updated with the latest anti-virus signatures before use. The relay network ports were covered with tamper tape. Additionally, the entity had implemented physical security measures where the Cyber Assets were located to include card reader access at the control center and control house and locked gates at the facility entrances. The entity identified this issue during a mock audit. Additionally, the entity had backup media for the Cyber Assets in scope. 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>					
Mitigation			<p>The entity submitted a Mitigation Plan on August 14, 2017 to address CIP-007-6 R2 and WECC accepted the entity's Mitigation Plans on March 20, 2018.</p> <p>To remediate and mitigation CIP-007-6 R2 the entity has:</p> <ol style="list-style-type: none"> 1) confirmed the status, and documented all Cyber Assets listed on the patch source vendor report that are obsolete, at end-of service, or no longer have patches available; 2) contacted the patch source vendor and confirmed that all device types that should be monitored for patch management are on their list; 3) added the three newly identified device types to the patch source; 4) completed patch evaluations for the [REDACTED] systems, and the [REDACTED] software security patch; and 5) created two patch mitigation plans, one for [REDACTED] EACMS and one for [REDACTED] relay. 6) created a patching and mitigation plan calendar to ensure patching and mitigation are completed on time; 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017301	CIP-007-6	R2	[REDACTED]	[REDACTED]	7/1/2016	5/8/2017	Self-Report	Completed
			7) trained specific subject matter experts on their CIP tasks and responsibilities regarding the match and mitigation plan calendar (across multiple departments). 8) completed a review of CIP procedures to identify CIP tasks and responsibilities between the different departments for managing the CIP Cyber Assets; 9) revised and updated its [REDACTED] for NERC Cyber Assets and updated workflows for tasks; and 10) provided additional training on [REDACTED], Substation Procedures for NERC Cyber Assets to [REDACTED] Engineering, Substation, and Operation Technician staff, including the handoffs to IT WECC verified completion of mitigating activities.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017302	CIP-007-6	R4	[REDACTED]	[REDACTED]	7/1/2016	3/2/2017	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 24, 2017, the entity submitted Self-Reports stating that, as a [REDACTED] it had several issues with CIP-007-6 R2, R4, R5, and CIP-010-2 R1.</p> <p>Specifically, the entity reported that in [REDACTED] it hired a consultant to perform a mock audit of its CIP Version 5 implementation to ensure there were no gaps. In preparation for, and during the mock audit, the entity discovered the following issues:</p> <ol style="list-style-type: none"> a. Ten protection relays classified as Bulk Electric System (BES) Cyber Assets (BCAs) without External Routable Connectivity (ERC), one remote terminal unit (RTU) classified as a Physical Access Control System (PACS) and seven firewalls classified as Electronic Access Control or Monitoring Systems (EACMS) with ERC, all associated with the entity's Medium Impact BES Cyber System (MIBCS), located at its [REDACTED], were obsolete or at end-of-life; therefore security patches were no longer available. As such, the security patch source (Vendor) that the entity identified for tracking the release of applicable cyber security patches removed the obsolete or end-of-life Cyber Assets from the patching report but failed to notify the entity that they had done so. The entity did not notice the discrepancy from what it had originally submitted to the Vendor. (CIP-007-6 R2 Part 2.1) b. Eight protection relays classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] were originally submitted to the Vendor who acknowledged it could support the Cyber Assets; however, the Cyber Assets did not show up on the security patch report sent to the entity for patch evaluation and again, the entity did not notice the discrepancy from what it had originally submitted to the Vendor. (CIP-007-6 R2 Part 2.1) c. Three additional protection relays classified as BCAs associated with the entity's MIBCS without ERC, located at its [REDACTED], originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, were not included on the list of Cyber Assets sent to the Vendor to monitor for security patches; therefore, were not being tracked for security patches. These protection relays were installed after the entity had inventoried its substations in preparation for transitioning to CIP Version 5. The three protection relays had no network ports. (CIP-007-6 R2 Part 2.1) d. The entity security patch evaluation report from the Vendor for [REDACTED] software was received on September 12, 2016; however, the entity completed the evaluation on October 17, 2016, four days after the 35 calendar day requirement. The entity had switched from a patch aggregator tool that allowed personnel to login and access patches on their own schedule to a new Vendor who provided the monthly report which caused some timely confusion in completing the evaluations and patching within the required timelines for one BCA. (CIP-007-6 R2 Part 2.2) e. One protection relay classified as a BCA associated with the entity's MIBCS without ERC, located at its [REDACTED], had an applicable security patch identified by the Vendor and submitted to the entity on September 20, 2016; however, the entity failed to see that the security patch was released and subsequently it was not evaluated within 35 calendar days. (CIP-007-6 R2 Part 2.2) f. The entity did not create a mitigation plan or update an existing mitigation plan for a security patch for one protection relay classified as a BCA associated with the entity's MIBCS without ERC, located at its [REDACTED], that it had evaluated as applicable but could not apply due to compatibility issues. The entity had not considered that patching for some substation BCAs would be impacted by BCAs at the other end of the line and coordination with other entities might require additional time to execute a patch. (CIP-007-6 R2 Part 2.3) g. Three protection relays, classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] were originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, were not enabled to log events by July 1, 2016. The protection relays were installed after the entity had inventoried its substations in preparation for transitioning to CIP Version 5. The substation procedure applicable to Cyber Assets under CIP Version 5 detailed the requirements for logging events as required by CIP-007-6 R4 Part 4.1; however, it was not in effect at the time the three protection relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process. (CIP-007-2 R4 Part 4.1) h. Three protection relays classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, did not have the factory default passwords changed by July 1, 2016, the mandatory and enforceable date of CIP-007-6 R5 Part 5.4. The substation procedure applicable to Cyber Assets under CIP Version 5 detailed the requirements for changing default passwords; however, it was not in effect at the time the three protection relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process. (CIP-007-6 R5 Part 5.4) 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017302	CIP-007-6	R4			7/1/2016	3/2/2017	Self-Report	Completed
			<p>i. The entity did not develop a baseline configuration for the [REDACTED] software installed on two Energy Management System (EMS) servers, two Inter-Control Center Communication Protocol (ICCP) servers, and 18 Supervisory Control and Data Acquisition (SCADA) workstations, all classified as BCAs associated with the entity's HIBCS at its primary and backup Control Centers. The entity's subject matter experts did not adequately consider the requirement to baseline beyond the operating system and network configuration. (CIP-010-2 R1 Part 1.1 sub-parts 1.1.2 and 1.1.3)</p> <p>j. Three protection relays classified as BCAs without ERC associated with the entity's MIBCS located at its [REDACTED] originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, did not have baseline configurations developed by July 1, 2016. The substation procedure applicable to Cyber Assets under CIP Version 5 was not in effect at the time the three relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process, as such, the substation personnel did not know the steps they were to follow to ensure the new BCAs were CIP compliant. (CIP-010-2 R1 Part 1.1)</p> <p>Additionally, WECC determined that the entity had an increase in scope from what it originally Self-Reported. The entity did not enforce password parameters for one protection relay classified as a BCA associated with the MIBCS without ERC located at its [REDACTED], as required by CIP-007-6 R5 Part 5.5, and the entity did not consider sub-parts 1.4.1, 1.4.2, and 1.4.3 for a change that deviated from the existing baseline configuration for one Physical Access Control System (PACS) and two EACMS associated with the HIBCS, as required by CIP-010-2 R1 Part 1.4.</p> <p>After reviewing all relevant information, WECC determined, for CIP-007-6 R4 Part 4.1, that the entity failed to log events at the BES Cyber System level or at the Cyber Asset level for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes as a minimum, detected successful login attempts; detected failed access attempts and failed login attempts; and detected malicious code as required by CIP-007-6 R4 Part 4.2 sub-parts 4.1.1, 4.1.2, and 4.1.3.</p> <p>The root cause of CIP-007-6 R4 Part 4.1 was the entity had individualized department compliance process documentation that did not explicitly assign responsibility to specific departments and does not address each requirement, thus highlighting compliance responsibility gaps between departments.</p> <p>WECC determined that the noncompliance start dates for CIP-007-6 R4 Part 4.1 began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable to the entity, and the ended on March 2, 2017 when the entity met the requirements of the Standards .</p>					
Risk Assessment			<p>WECC determined that CIP-007-6 R4 Part 4.1 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). The entity failed to log events at the BES Cyber System level or at the Cyber Asset level for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes as a minimum, detected successful login attempts; detected failed access attempts and failed login attempts; and detected malicious code as required by CIP-007-6 R4 Part 4.2 sub-parts 4.1.1, 4.1.2, and 4.1.3. Such failure could potentially cause Cyber Security incidents to go undetected resulting in the misoperation of protection system devices. The entity has a HIBCS and MIBCS for which these Cyber Assets are applicable; it owns [REDACTED] of generation, has [REDACTED] transmission line, [REDACTED] transmission lines, and [REDACTED] transmission line. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as minor.</p> <p>However, the entity implemented so good internal controls. Specifically, the majority of Cyber Assets in scope were not configured with ERC and could only be accessed using dedicated laptops managed by the entity's IT department, which were updated with the latest anti-virus signatures before use. The relay network ports were covered with tamper tape. Additionally, the entity had implemented physical security measures where the Cyber Assets were located to include card reader access at the control center and control house and locked gates at the facility entrances. The entity identified this issue during a mock audit. Additionally, the entity had backup media for the Cyber Assets in scope. 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>					
Mitigation			<p>The entity submitted a Mitigation Plan on September 5, 2017 to address CIP-007-6 R4 Part 4.1 and WECC accepted the entity's Mitigation Plans on February 7, 2018.</p> <p>To remediate and mitigation CIP-007-6 R4 Part 4.1 the entity has:</p> <ol style="list-style-type: none"> 1) updated relay database files to enable Device Security Event logging and alarming. 2) completed a review of CIP procedures to identify CIP tasks and responsibilities between the different departments for managing the CIP Cyber Assets; 3) revised and updated its [REDACTED] for NERC Cyber Assets and updated workflows for tasks; and 4) provided additional training on [REDACTED] Substation Procedures for NERC Cyber Assets to [REDACTED] Engineering, Substation, and Operation Technician staff, including the handoffs to IT staff. <p>WECC verified completion of mitigating activities.</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
WECC2017017305	CIP-007-6	R5	[REDACTED]	[REDACTED]	7/1/2016	6/16/2017	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 March 24, 2017, the entity submitted Self-Reports stating that, as a [REDACTED], it had several issues with CIP-007-6 R2, R4, R5, and CIP-010-2 R1.</p> <p>Specifically, the entity reported that in November of 2016 it hired a consultant to perform a mock audit of its CIP Version 5 implementation to ensure there were no gaps. In preparation for, and during the mock audit, the entity discovered the following issues:</p> <ol style="list-style-type: none"> Ten protection relays classified as Bulk Electric System (BES) Cyber Assets (BCAs) without External Routable Connectivity (ERC), one remote terminal unit (RTU) classified as a Physical Access Control System (PACS) and seven firewalls classified as Electronic Access Control or Monitoring Systems (EACMS) with ERC, all associated with the entity's Medium Impact BES Cyber System (MIBCS), located at its [REDACTED], were obsolete or at end-of-life; therefore security patches were no longer available. As such, the security patch source (Vendor) that the entity identified for tracking the release of applicable cyber security patches removed the obsolete or end-of-life Cyber Assets from the patching report but failed to notify the entity that they had done so. The entity did not notice the discrepancy from what it had originally submitted to the Vendor. (CIP-007-6 R2 Part 2.1) Eight protection relays classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] were originally submitted to the Vendor who acknowledged it could support the Cyber Assets; however, the Cyber Assets did not show up on the security patch report sent to the entity for patch evaluation and again, the entity did not notice the discrepancy from what it had originally submitted to the Vendor. (CIP-007-6 R2 Part 2.1) Three additional protection relays classified as BCAs associated with the entity's MIBCS without ERC, located at its [REDACTED], originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, were not included on the list of Cyber Assets sent to the Vendor to monitor for security patches; therefore, were not being tracked for security patches. These protection relays were installed after the entity had inventoried its substations in preparation for transitioning to CIP Version 5. The three protection relays had no network ports. (CIP-007-6 R2 Part 2.1) The entity security patch evaluation report from the Vendor for [REDACTED] software was received on September 12, 2016; however, the entity completed the evaluation on October 17, 2016, four days after the 35 calendar day requirement. The entity had switched from a patch aggregator tool that allowed personnel to login and access patches on their own schedule to a new Vendor who provided the monthly report which caused some timely confusion in completing the evaluations and patching within the required timelines for one BCA. (CIP-007-6 R2 Part 2.2) One protection relay classified as a BCA associated with the entity's MIBCS without ERC, located at its [REDACTED], had an applicable security patch identified by the Vendor and submitted to the entity on September 20, 2016; however, the entity failed to see that the security patch was released and subsequently it was not evaluated within 35 calendar days. (CIP-007-6 R2 Part 2.2) The entity did not create a mitigation plan or update an existing mitigation plan for a security patch for one protection relay classified as a BCA associated with the entity's MIBCS without ERC, located at its [REDACTED], that it had evaluated as applicable but could not apply due to compatibility issues. The entity had not considered that patching for some substation BCAs would be impacted by BCAs at the other end of the line and coordination with other entities might require additional time to execute a patch. (CIP-007-6 R2 Part 2.3) Three protection relays, classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] were originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, were not enabled to log events by July 1, 2016. The protection relays were installed after the entity had inventoried its substations in preparation for transitioning to CIP Version 5. The substation procedure applicable to Cyber Assets under CIP Version 5 detailed the requirements for logging events as required by CIP-007-6 R4 Part 4.1; however, it was not in effect at the time the three protection relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process. (CIP-007-2 R4 Part 4.1) Three protection relays classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, did not have the factory default passwords changed by July 1, 2016, the mandatory and enforceable date of CIP-007-6 R5 Part 5.4. The substation procedure applicable to Cyber Assets under CIP Version 5 detailed the requirements for changing default passwords; however, it was not in effect at the time the three protection relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process. (CIP-007-6 R5 Part 5.4) 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017305	CIP-007-6	R5			7/1/2016	6/16/2017	Self-Report	Completed
			<p>i. The entity did not develop a baseline configuration for the [REDACTED] software installed on two Energy Management System (EMS) servers, two Inter-Control Center Communication Protocol (ICCP) servers, and 18 Supervisory Control and Data Acquisition (SCADA) workstations, all classified as BCAs associated with the entity's HIBCS at its primary and backup Control Centers. The entity's subject matter experts did not adequately consider the requirement to baseline beyond the operating system and network configuration. (CIP-010-2 R1 Part 1.1 sub-parts 1.1.2 and 1.1.3)</p> <p>j. Three protection relays classified as BCAs without ERC associated with the entity's MIBCS located at its [REDACTED] originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, did not have baseline configurations developed by July 1, 2016. The substation procedure applicable to Cyber Assets under CIP Version 5 was not in effect at the time the three relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process, as such, the substation personnel did not know the steps they were to follow to ensure the new BCAs were CIP compliant. (CIP-010-2 R1 Part 1.1)</p> <p>Additionally, WECC determined that the entity had an increase in scope from what it originally Self-Reported. The entity did not enforce password parameters for one protection relay classified as a BCA associated with the MIBCS without ERC located at its [REDACTED], as required by CIP-007-6 R5 Part 5.5, and the entity did not consider sub-parts 1.4.1, 1.4.2, and 1.4.3 for a change that deviated from the existing baseline configuration for one Physical Access Control System (PACS) and two EACMS associated with the HIBCS, as required by CIP-010-2 R1 Part 1.4.</p> <p>After reviewing all relevant information, WECC determined, for CIP-007-6 R5 Parts 5.4 and 5.5, that the entity failed to change known default passwords per Cyber Asset capability as required by CIP-007-6 R5 Part 5.4. and technically or procedurally enforce password parameters where password length is at least the lesser of eight characters or the maximum length supported by the Cyber Asset and the minimum password complexity that is the lesser of three or more different types of characters or the maximum complexity supported by the Cyber Asset a required by CIP-007-6 R5 Part 5.5.</p> <p>The root cause of CIP-007-6 R5 Parts 5.4 and 5.5 was the entity had individualized department compliance process documentation that did not explicitly assign responsibility to specific departments and does not address each requirement, thus highlighting compliance responsibility gaps between departments.</p> <p>WECC determined that the noncompliance start dates for CIP-007-6 R5 Parts 5.4 and 5.5 began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable to the entity, and the ended on June 16, 2017 when the entity met the requirements of the Standards .</p>					
Risk Assessment			<p>WECC determined that CIP-007-6 R5 Parts 5.4 and 5.5 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). The entity failed to change known default passwords per Cyber Asset capability as required by CIP-007-6 R5 Part 5.4. and technically or procedurally enforce password parameters where password length is at least the lesser of eight characters or the maximum length supported by the Cyber Asset and the minimum password complexity that is the lesser of three or more different types of characters or the maximum complexity supported by the Cyber Asset a required by CIP-007-6 R5 Part 5.5. Such failure could potentially result in a malicious actor accessing and compromising an applicable Cyber Asset to adjust settings or render the Cyber Assets inoperable resulting in potential misoperations. The entity has a HIBCS and MIBCS for which these Cyber Assets are applicable; it owns [REDACTED] of generation, has [REDACTED] transmission line, [REDACTED] transmission lines, and [REDACTED] transmission line. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as minor.</p> <p>However, the entity implemented so good internal controls. Specifically, the majority of Cyber Assets in scope were not configured with ERC and could only be accessed using dedicated laptops managed by the entity's IT department, which were updated with the latest anti-virus signatures before use. The relay network ports were covered with tamper tape. Additionally, the entity had implemented physical security measures where the Cyber Assets were located to include card reader access at the control center and control house and locked gates at the facility entrances. The entity identified this issue during a mock audit. Additionally, the entity had backup media for the Cyber Assets in scope. 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>					
Mitigation			<p>The entity submitted a Mitigation Plan on August 14, 2017 address CIP-007-6 R5 Parts 5.4 and 5.5 and WECC accepted the entity's Mitigation Plans on February 7, 2018.</p> <p>To remediate and mitigate CIP-007-6 R5 Parts 5.4 and 5.5 the entity has:</p> <ol style="list-style-type: none"> 1) changed the default passwords on the Cyber Assets in scope and changed the password for the GEC relay to meet the complexity requirement. 2) completed a review of CIP procedures to identify CIP tasks and responsibilities between the different departments for managing the CIP Cyber Assets; 3) updated the change management check list in order to provide clearer direction for Relay Technicians, Protection Engineers and IT staff; 4) revised and updated its [REDACTED] for NERC Cyber Assets and updated workflows for tasks; and 5) provided additional training on [REDACTED] Substation Procedures for NERC Cyber Assets to [REDACTED] Engineering, Substation, and Operation Technician staff, including the handoffs to IT staff. <p>WECC verified completion of mitigating activities.</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
WECC2017017294	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/1/2016	5/11/2017	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 24, 2017, the entity submitted Self-Reports stating that, as a [REDACTED], it had several issues with CIP-007-6 R2, R4, R5, and CIP-010-2 R1.</p> <p>Specifically, the entity reported that in [REDACTED] 2016 it hired a consultant to perform a mock audit of its CIP Version 5 implementation to ensure there were no gaps. In preparation for, and during the mock audit, the entity discovered the following issues:</p> <ol style="list-style-type: none"> Ten protection relays classified as Bulk Electric System (BES) Cyber Assets (BCAs) without External Routable Connectivity (ERC), one remote terminal unit (RTU) classified as a Physical Access Control System (PACS) and seven firewalls classified as Electronic Access Control or Monitoring Systems (EACMS) with ERC, all associated with the entity's Medium Impact BES Cyber System (MIBCS), located at its [REDACTED], were obsolete or at end-of-life; therefore security patches were no longer available. As such, the security patch source (Vendor) that the entity identified for tracking the release of applicable cyber security patches removed the obsolete or end-of-life Cyber Assets from the patching report but failed to notify the entity that they had done so. The entity did not notice the discrepancy from what it had originally submitted to the Vendor. (CIP-007-6 R2 Part 2.1) Eight protection relays classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] were originally submitted to the Vendor who acknowledged it could support the Cyber Assets; however, the Cyber Assets did not show up on the security patch report sent to the entity for patch evaluation and again, the entity did not notice the discrepancy from what it had originally submitted to the Vendor. (CIP-007-6 R2 Part 2.1) Three additional protection relays classified as BCAs associated with the entity's MIBCS without ERC, located at its [REDACTED], originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, were not included on the list of Cyber Assets sent to the Vendor to monitor for security patches; therefore, were not being tracked for security patches. These protection relays were installed after the entity had inventoried its substations in preparation for transitioning to CIP Version 5. The three protection relays had no network ports. (CIP-007-6 R2 Part 2.1) The entity security patch evaluation report from the Vendor for [REDACTED] software was received on September 12, 2016; however, the entity completed the evaluation on October 17, 2016, four days after the 35 calendar day requirement. The entity had switched from a patch aggregator tool that allowed personnel to login and access patches on their own schedule to a new Vendor who provided the monthly report which caused some timely confusion in completing the evaluations and patching within the required timelines for one BCA. (CIP-007-6 R2 Part 2.2) One protection relay classified as a BCA associated with the entity's MIBCS without ERC, located at its [REDACTED], had an applicable security patch identified by the Vendor and submitted to the entity on September 20, 2016; however, the entity failed to see that the security patch was released and subsequently it was not evaluated within 35 calendar days. (CIP-007-6 R2 Part 2.2) The entity did not create a mitigation plan or update an existing mitigation plan for a security patch for one protection relay classified as a BCA associated with the entity's MIBCS without ERC, located at its [REDACTED], that it had evaluated as applicable but could not apply due to compatibility issues. The entity had not considered that patching for some substation BCAs would be impacted by BCAs at the other end of the line and coordination with other entities might require additional time to execute a patch. (CIP-007-6 R2 Part 2.3) Three protection relays, classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] were originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, were not enabled to log events by July 1, 2016. The protection relays were installed after the entity had inventoried its substations in preparation for transitioning to CIP Version 5. The substation procedure applicable to Cyber Assets under CIP Version 5 detailed the requirements for logging events as required by CIP-007-6 R4 Part 4.1; however, it was not in effect at the time the three protection relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process. (CIP-007-2 R4 Part 4.1) Three protection relays classified as BCAs associated with the entity's MIBCS without ERC located at its [REDACTED] originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, did not have the factory default passwords changed by July 1, 2016, the mandatory and enforceable date of CIP-007-6 R5 Part 5.4. The substation procedure applicable to Cyber Assets under CIP Version 5 detailed the requirements for changing default passwords; however, it was not in effect at the time the three protection relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process. (CIP-007-6 R5 Part 5.4) 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017294	CIP-010-2	R1			7/1/2016	5/11/2017	Self-Report	Completed
			<p>The entity did not develop a baseline configuration for the [REDACTED] software installed on two Energy Management System (EMS) servers, two Inter-Control Center Communication Protocol (ICCP) servers, and 18 Supervisory Control and Data Acquisition (SCADA) workstations, all classified as BCAs associated with the entity's HIBCS at its primary and backup Control Centers. The entity's subject matter experts did not adequately consider the requirement to baseline beyond the operating system and network configuration. (CIP-010-2 R1 Part 1.1 sub-parts 1.1.2 and 1.1.3)</p> <p>i. Three protection relays classified as BCAs without ERC associated with the entity's MIBCS located at its [REDACTED] originally installed in 2015, and at that time not subject to the NERC CIP Reliability Standards, did not have baseline configurations developed by July 1, 2016. The substation procedure applicable to Cyber Assets under CIP Version 5 was not in effect at the time the three relays were originally installed and during its CIP Version 5 transition, the entity did not include them in its CIP Version 5 change management process, as such, the substation personnel did not know the steps they were to follow to ensure the new BCAs were CIP compliant. (CIP-010-2 R1 Part 1.1)</p> <p>Additionally, WECC determined that the entity had an increase in scope from what it originally Self-Reported. The entity did not enforce password parameters for one protection relay classified as a BCA associated with the MIBCS without ERC located at its [REDACTED], as required by CIP-007-6 R5 Part 5.5, and the entity did not consider sub-parts 1.4.1, 1.4.2, and 1.4.3 for a change that deviated from the existing baseline configuration for one Physical Access Control System (PACS) and two EACMS associated with the HIBCS, as required by CIP-010-2 R1 Part 1.4.</p> <p>After reviewing all relevant information, WECC determined, for CIP-010-2 Parts 1.1 and 1.4, that the entity failed to develop a baseline configuration individually or by group, that includes operating system(s) or firmware and any custom software installed as required by CIP-010-2 R1 Part 1.1 sub-parts 1.1.1 and 1.1.3. and for a change that deviates from the existing baseline configuration prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change and document the results of the verification as required by CIP-010-2 R1 Part 1.4 sub-parts 1.4.1 and 1.4.3.</p> <p>The root cause of CIP-010-2 Parts 1.1 and 1.4 was the entity either had no procedures in place or what they had was not adequate to ensure compliance with the Standard and Requirement.</p> <p>WECC determined that the noncompliance start dates for CIP-010-2 Parts 1.1 and 1.4 began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable to the entity and the ended on May 11, 2017 when the entity met the requirements of the Standards.</p>					
Risk Assessment			<p>WECC determined that CIP-010-2 Parts 1.1 and 1.4 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). The entity failed to develop a baseline configuration individually or by group, that includes operating system(s) or firmware and any custom software installed as required by CIP-010-2 R1 Part 1.1 sub-parts 1.1.1 and 1.1.3. and for a change that deviates from the existing baseline configuration prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change and document the results of the verification as required by CIP-010-2 R1 Part 1.4 sub-parts 1.4.1 and 1.4.3. Such failure could potentially result in the entity not being able to detect unauthorized changes to Cyber Assets which could allow a malicious actor to modify the Cyber Assets, potentially affecting the BPS. The entity has a HIBCS and MIBCS for which these Cyber Assets are applicable; it owns [REDACTED] of generation, has [REDACTED] transmission line, [REDACTED] transmission lines, and [REDACTED] transmission line. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as minor.</p> <p>However, the entity implemented so good internal controls. Specifically, the majority of Cyber Assets in scope were not configured with ERC and could only be accessed using dedicated laptops managed by the entity's IT department, which were updated with the latest anti-virus signatures before use. The relay network ports were covered with tamper tape. Additionally, the entity had implemented physical security measures where the Cyber Assets were located to include card reader access at the control center and control house and locked gates at the facility entrances. The entity identified this issue during a mock audit. Additionally, the entity had backup media for the Cyber Assets in scope. 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>					
Mitigation			<p>The entity submitted a Mitigation Plan on September 5, 2017 to address for CIP-010-2 Parts 1.1 and 1.4 and, WECC accepted the entity's Mitigation Plans on February 20, 2018.</p> <p>To remediate and mitigate CIP-010-2 Parts 1.1 and 1.4 the entity has:</p> <ol style="list-style-type: none"> 1) documented baseline configurations for the three Cyber Assets in scope and the [REDACTED] software on the 22 applicable Cyber Assets. 2) implemented [REDACTED] alerts to remind staff to review open change tickets and follow-up on the status of those change tickets; and 3) added subject matter experts from the Transmission and Distribution division to those responsible for CIP requirements to ensure adequate coverage of responsibilities for substation device. <p>WECC verified completion of mitigating activities.</p>					

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 Exception 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	FRCC2019021077	Yes		Yes	Yes									Category 1 – 3 years Category 2 – 12: 2 years
2	MRO2018020807			Yes	Yes									Category 2 – 12: 2 years
3	MRO2018019204			Yes	Yes									Category 2 – 12: 2 years
4	MRO2018020299			Yes	Yes					Yes				Category 2 – 12: 2 years
5	MRO2018019578			Yes	Yes					Yes				Category 2 – 12: 2 years
6	MRO2018020301			Yes	Yes					Yes				Category 2 – 12: 2 years
7	MRO2017018870	Yes		Yes	Yes					Yes	Yes		Yes	Category 1: 3 years; Category 2 – 12: 2 years
8	MRO2018020139	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
9	NPCC2018018983			Yes	Yes									Categories 2 – 12: 2 year
10	NPCC2018019211			Yes	Yes									Categories 2 – 12: 2 year
11	NPCC2018020590			Yes	Yes									Categories 2 – 12: 2 year
12	NPCC2019020904			Yes	Yes									Categories 2 – 12: 2 year
13	RFC2018019982	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
14	RFC2018019838	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
15	RFC2018019648	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
16	RFC2019020946	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2-12: 2 years
17	RFC2019020947	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
18	RFC2019020948	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
19	RFC2018020204	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2-12: 2 years
20	RFC2018020084	Yes		Yes	Yes	Yes			Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
21	RFC2017018709	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2-12: 2 years
22	RFC2018019727	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
23	RFC2018019728	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
24	RFC2017018629	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2-12: 2 years
25	RFC2017018344	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; 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	RFC2018019812	Yes		Yes	Yes		Yes						Yes	Category 1: 3 years; Category 2-12: 2 years
27	RFC2018019811	Yes		Yes	Yes		Yes		Yes	Yes			Yes	Category 1: 3 years; Category 2-12: 2 years
28	RFC2018020085	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
29	SERC2018019354			Yes	Yes									Category 2 – 12: 2 years
30	SERC2018019036			Yes	Yes									Category 2 – 12: 2 years
31	SERC2018019355			Yes	Yes									Category 2 – 12: 2 years
32	SERC2018019923			Yes	Yes									Category 2 – 12: 2 years
33	SERC2017018900			Yes	Yes									Category 2 – 12: 2 years
34	SERC2018019035			Yes	Yes									Category 2 – 12: 2 years
35	SERC2017018901			Yes	Yes									Category 2 – 12: 2 years
36	SERC2018019938			Yes	Yes									Category 2 – 12: 2 years
37	WECC2018019139	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
38	WECC2018019142	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
39	WECC2019020912			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
40	WECC2018019188			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
41	WECC2018019008	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
42	WECC2018019930	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
43	WECC2018020223			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
44	WECC2018018916			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
45	WECC2018020047			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
46	WECC2017018616	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
47	WECC2017017877			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
48	WECC2018019303			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
49	WECC2018019293			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
50	WECC2018019341	Yes		Yes	Yes					Yes				Category 1: 3 years; 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
FRCC2019021077	CIP-006-6	R1. Part 1.5.	[REDACTED] ("the Entity")	[REDACTED]	4/12/2018	4/30/2018	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 21, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-006-6 R1 (Part 1.5).</p> <p>This noncompliance started on April 12, 2018, when the Entity failed to respond to detected unauthorized access through a physical access point into a PSP. The noncompliance ended on April 30, 2018, when the Entity corrected their alerting and alarming issues in the PSP in order to respond within the required timeframe.</p> <p>On April 30, 2018, the PACS server encountered a hardware failure and was offline for approximately three (3) hours. During this time, there were two (2) detected unauthorized access events into the PSP (one resulted from testing to verify whether the alerting function was operational and the other was a delayed door alarm issue). Although the PSP doors were being monitored and activity was being logged during these events, the associated email notifications were unable to be distributed while the PACS server remained offline.</p> <p>The delayed door alarm was assessed and determined to be a false alarm through review of authorized access reports to identify and follow-up with authorized personnel that were reported as entering/exiting the PSP during the timeframe that the alarms were triggered. The hardware issue was relieved by re-allocating the server memory on April 30, 2018.</p> <p>The extent of condition was conducted on July 30, 2018 and discovered three (3) additional instances of noncompliance. On April 12, 2018, the PACS server (which controls the alarming/alerting for detected unauthorized access through a physical access point into a PSP) was taken offline for maintenance. Once the maintenance was completed and the machine was set to reboot (remotely) at 11:38. A hardware malfunction was encountered that prevented the machine from completing the reboot on its own. The server was manually rebooted at 16:01 on April 12, 2018. Based on a review of available information and communications, the PACS server was offline for approximately four (4) hours, twenty-three (23) minutes. During this time, there were three (3) detected unauthorized access alarms. The additional instances were assessed and were determined to be false alarms through review of authorized access reports to identify and follow-up with authorized personnel that were reported as entering/exiting the PSP during the timeframe that the alarms were triggered.</p> <p>The causes for this noncompliance was the 'Request to Exit' sensors were out of adjustment that created a small area which sometimes prevented the request to exit sensor from detecting persons exiting 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.</p> <p>The risk was reduced due to layered security [REDACTED] as the PSP was located inside a generation plant. Furthermore, there was no potential risk from unauthorized entry.</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) replaced physical PACS server at PCC; 2) created redundant virtual PACS server at PCC; 3) created backup virtual PACS server at BUCC; and 4) completed Cause Analysis Review Meeting. 					

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
MRO2018020807	CIP-007-6	R2			12/2/2017	12/11/2017	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 violation.)			<p>On October 16, 2018, [REDACTED] submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-007-6 R2. Specifically, [REDACTED] created a patch mitigation plan under P2.3, the mitigation plan was required to be completed by December 1, 2017. [REDACTED] states that it recognized that it could not complete the last step of the mitigation plan in time, but did not process the revision in time to have the CIP Senior Manager approve the revision as required by P2.4.</p> <p>The cause of the noncompliance was that [REDACTED] did not process the revision in time to have the CIP Senior Manager approve the revision as required by P2.4.</p> <p>This noncompliance started on December 2, 2017, the day after the original plan completion date and ended on December 11, 2017, when the CIP Senior Manager approved the revised 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. The noncompliance was minimal because per [REDACTED], it instituted compensating controls to address the vulnerabilities identified by the patch during the completion of the mitigation plan; these compensating measures were in place during the period of noncompliance. 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) had its CIP Senior Manager approve the revised mitigation plan; 2) implemented a practice of using trigger events to alert mitigation plan approvals; and 3) implemented an improved work flow process to track time based requirements. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019204	CIP-005-5	R1	[REDACTED]	[REDACTED]	7/1/2016	12/4/2017	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 December 31, 2017, [REDACTED] submitted a self-log stating that, [REDACTED], it was in noncompliance with CIP-005-5 R1. Specifically, [REDACTED] reports that it failed to have a sufficient process in place to ensure that the justification for any inbound and outbound access permissions is sufficiently documented as required by P1.3. [REDACTED] states that during a documentation review, it discovered that the justifications failed to include the level of detail that it expects.</p> <p>The cause of the noncompliance is that [REDACTED] failed to provide sufficient instruction on the level of detail it expected regarding the justifications of inbound and outbound access permissions.</p> <p>The noncompliance began on July 1, 2016 when the standard became enforceable, and ended on December 4, 2017 when the documented process was 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. [REDACTED] reports that the noncompliance did not cause an Electronic Access Point to have an improperly broad access permission. 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 necessary documentation, its process description and associated procedure; and 2) provided training on the updated process description and 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
MRO2018020299	CIP-004-6	R5	[REDACTED]	[REDACTED]	4/14/2018	6/11/2018	self-log	Expected 3/29/2019
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 10, 2018, [REDACTED], submitted a self-log to MRO stating that, [REDACTED], it was in noncompliance with CIP-004-6 R5. [REDACTED] The self-log identified three instances of noncompliance. The noncompliance occurred [REDACTED].</p> <p>In the first instance of noncompliance, [REDACTED] states that a new manager reviewed the job duties of an existing employee and determined that the employee did not need three read-only entitlements to BES CSI. The BES CSI related to [REDACTED]. The manager submitted a revocation request, but due to an interface error between two applications, the access was not revoked. [REDACTED] states that the noncompliance was discovered on May 17, 2018, during a monthly review of revocation requests. The access was determined to be unnecessary on April 12, 2018, but was not revoked until June 7, 2018. The cause of the noncompliance was that the access revocation process was deficient, as it did not clearly direct security personnel to use an employee's ID number as well as the name. The noncompliance began on April 14, 2018, after the access was not revoked by the end of the next calendar day following the manager's request, and ended on June 7, 2018 when the access was revoked.</p> <p>In the second instance of noncompliance, [REDACTED] states that an [REDACTED] employee retired with an effective date of April 21, 2018. The employee's manager submitted a revocation form on April 2, 2018; security personnel reviewed the revocation and took no further action after discovering an employee with that name had an access badge that was deactivated in 2017. On April 23, 2018, the employee's manager contacted security personnel to confirm the revocation with security personnel, who upon further inspection, discovered there was an active badge under the employee's ID number, under the employee's preferred name (e.g., Bob as opposed to Robert). The cause of the noncompliance was that the access revocation process was deficient, as it did not clearly direct security personnel to search for access under an employee's ID number as well as the name. The noncompliance began on April 22, 2018, after the access was not revoked within 24 hours of the retirement, and ended on April 23, 2018 when the access was revoked.</p> <p>In the third instance of noncompliance, [REDACTED] states that on June 8, 2018, a union contractor with authorized physical access to one or more substations, informed an [REDACTED] foreman that the contractor was resigning due to being assigned to a different job and returned the access badge. [REDACTED] states that the foreman informed the supervisor, who was new to the position and did not know that he was required to immediately submit a revocation request form. [REDACTED] reports that revocation form was submitted on June 11, 2018 and the revocation was processed later that day. The cause of the noncompliance was that [REDACTED] failed to follow its process due to a lack of training in a new supervisor. The noncompliance began on June 9, 2018, after the access was not revoked within 24 hours of the resignation, and ended on June 11, 2018 when the access was revoked.</p> <p>The noncompliance was noncontiguous; it began on April 14, 2018, when access in the first instance was not revoked by the end of the next calendar day after the manager's request, and ended on June 11, 2018, when the access in the third instance was revoked.</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 because per [REDACTED], the access was read only, the removal was based on a new manager who refined the need for access without changing the employee's duties, and the employee did not log onto the entitlements during the period of noncompliance. The second and third instance were minimal, because per [REDACTED], the individuals surrendered the access badges upon resignation and the badges were secured by a supervisor during the noncompliance, the individuals did not have electronic access, and both resignations were not for cause. No harm is known to have occurred.</p> <p>[REDACTED] has not fully mitigated the noncompliance in the first instance. To reduce the risk during mitigation, [REDACTED] will continue utilizing the detective control that caught this instance of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]:</p> <p>To mitigate the first instance of noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) revoked the employee's access; 2) designed a fix for the interface between the two systems; and 3) estimated the work effort to implement the fix. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020299	CIP-004-6	R5	[REDACTED]	[REDACTED]	4/14/2018	6/11/2018	self-log	Expected 3/29/2019
			<p>To mitigate the first instance of noncompliance, [REDACTED] will by March 29, 2019:</p> <p>1) complete the changes to implement the fix.</p> <p>The reason for the duration of the mitigating activities is due to the technical complexity of the fix.</p> <p>To mitigate the second instance of noncompliance, [REDACTED]:</p> <p>1) revoked the former employee's access; and 2) updated the revocation process to include a search by the employee's name and employee ID.</p> <p>To mitigate the third instance of noncompliance, [REDACTED]:</p> <p>1) revoked the contractor's access; and 2) developed an action plan with the supervisor to follow for future revocation actions.</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
MRO2018019578	CIP-004-6	R5	[REDACTED]	[REDACTED]	3/10/2018	3/12/2018	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 April 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].</p> <p>Specifically, [REDACTED] stated that a contract employee with unescorted physical access to substations resigned with a last day of March 8, 2018. The revocation of access requires that the employee's manager submit a revocation form. [REDACTED] states that the employee's manager was on vacation at the time the resignation became effective and did not realize the need to complete the form prior to leaving on vacation. The employee's access was not revoked until March 12, 2018.</p> <p>The noncompliance was caused by [REDACTED] failing to follow its documented process regarding access revocation.</p> <p>The noncompliance began on March 10, 2018, when access was not revoked by the end of the next calendar day after the employee's resignation, and ended on March 12, 2018, when the access was revoked.</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 employee surrendered the access badge upon resignation and it was secured by a supervisor during the noncompliance. [REDACTED] states that the employee did not have Interactive Remote Access privileges. Finally, [REDACTED] states that it confirmed there was no access or access attempts by the employee 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) revoked the former employee's access; and 2) sent a letter to the manager on the importance of timely submitting revocation forms. <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
MRO2018020301	CIP-007-6	R2	[REDACTED]	[REDACTED]	3/29/2018	4/7/2018	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 July 10, 2018, [REDACTED] submitted a self-log to MRO stating that, [REDACTED], it was in noncompliance with CIP-007-6 R2. [REDACTED] The noncompliance occurred [REDACTED].</p> <p>Specifically, [REDACTED] failed to install a security patch on multiple BES Cyber Assets within 35 days of patch evaluation as required by P2.3. [REDACTED] reports that it discovered the noncompliance during a monthly patching cycle review.</p> <p>The noncompliance was caused by [REDACTED] failing to follow its documented process regarding patch application; specifically, [REDACTED] states that a SME was confused as to the version and believed that the patch had already been deployed.</p> <p>The noncompliance began on March 29, 2018, 36 days after the patch was evaluated, and ended on April 7, 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. [REDACTED] states that while the patch was not applied within 35 days of the evaluation, the patch was applied within 70 days of the release date of the patch. 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 patch; and 2) during a team meeting, emphasized the need to follow the procedure and double-check the patches scheduled for installation. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2017018870	CIP-007-6	R1	[REDACTED]	[REDACTED]	7/01/2016	4/06/2018	Compliance 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 between [REDACTED], MRO determined that [REDACTED] a [REDACTED], as a [REDACTED], was in noncompliance with CIP-007-6 R1. [REDACTED] [REDACTED] are [REDACTED]. The noncompliance occurred [REDACTED].</p> <p>During the Compliance Audit, seven out of seven sampled PACS controllers did not have adequate documented justifications regarding the enabled logical network accessible ports; the only documentation that [REDACTED] had was the vendor's manual that includes a description of ports and configurations. [REDACTED] was using this manual as documentation for the "deemed necessary ports."</p> <p>The cause of the noncompliance was inadequate process for documenting the enabled ports and services for PACS controllers.</p> <p>The noncompliance began on July 1, 2016 when the Standard and Requirement became enforceable and ended on April 6, 2018 when [REDACTED] documented the justifications for why the ports were logically enabled.</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 documenting the need for the enabled ports as [REDACTED] reports that all of the enabled ports are needed for security personnel [REDACTED]. Additionally, per [REDACTED] logical access to the PACS controllers is only possible from PACS servers accessed by authorized security personnel. No harm is known to have occurred.</p> <p>MRO reviewed [REDACTED] CIP-007-6 R1 compliance history. [REDACTED] relevant compliance history includes a Compliance Exception for CIP-007-6 R1 [REDACTED] that was mitigated on May 16, 2017. This noncompliance involved [REDACTED] failure to adequately document the enabled ports for the EACMS devices associated with a firewall management system. MRO determined that [REDACTED] compliance history should not serve as a basis for applying a penalty, as the current noncompliance was distinct in character (the current noncompliance was limited to utilizing vendor documentation for PACS controllers) and was not caused by a failure to mitigate the prior noncompliance.</p>					
Mitigation			<p>To mitigate the noncompliance, [REDACTED]:</p> <ol style="list-style-type: none"> 1) reviewed the panels' port documentation to determine which ports are required and why; 2) updated the control panels' documentation to include justifications for enabled ports; 3) updated the PACS ports and services management procedure to describe port/service scanning procedures and the required analysis of the results; and 4) trained support personnel on 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
MRO2018020139	CIP-007-6	R4	████████████████████	████████	12/13/2016	2/23/2018	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-007-6 R4. █████ identified two instances of noncompliance in the self-log.</p> <p>In the first instance of noncompliance, █████ states that it discovered that its anti-virus solution was not configured to generate alerts on all malicious code detection as required by P4.2.1, but only configured to generate alerts on malicious code that could not be automatically eliminated or quarantined. █████ reports that this noncompliance impacted 35 Cyber Assets (all █████ devices). The cause of this noncompliance was a lack of sufficient detail in its process for software patching to ensure that alerting was still functioning after a patch update. The noncompliance began December 13, 2016 when a patch application reverted the configuration of the anti-virus solution to its default settings (which did not generate alerts on all malicious code detection), and ended on February 23, 2018 when █████ changed the configuration to alert for all malicious code detection.</p> <p>In the second instance of noncompliance, █████ states that logs were not being sent to the centralized logging for some Cyber Assets that resulted in no alerting capability for detected malicious code as required by P4.2.1. █████ states that an extent of condition revealed the issue impacted 11 Cyber Assets. █████ vendor knew of this issue and was trying to resolve it through a patch release. The cause of this noncompliance was a failure to implement sufficient controls to alert for the failure of logging. █████ stated that the noncompliance began November 5, 2017 when logging and alerting stopped on the first device, and ended on December 15, 2017 when logging and alerting was re-enabled and █████ deployed a secondary control to alert for the loss of logging.</p> <p>This noncompliance started on December 13, 2016, when the configuration in the first instance reverted, and ended on February 23, 2018, when the Cyber Assets in the first instance were reconfigured to enable alerts.</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 instance was minimal because per █████ the noncompliance was limited to a failure to alert for code that could be automatically resolved. The second instance was minimal because per █████ the noncompliance was limited to alerts on malicious code detection as the devices were still logging locally per P4.1 and █████ was still reviewing those logs per P4.4. Additionally, for both instances █████ reports that it reviewed logs and found no indications of any malicious code. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, █████</p> <p>To mitigate the first instance of noncompliance, █████</p> <ol style="list-style-type: none"> 1) enabled the alerting function on its anti-malware software; 2) changed its process to include validation testing to ensure alerts are functional; and 3) added an additional log aggregator as a secondary alert source for malware events. <p>To mitigate the second instance of noncompliance, █████</p> <ol style="list-style-type: none"> 1) re-enabled the log forwarder on the impacted devices; 2) configured the log server software to generate an alert █████; and 3) applied the patch to resolve 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
NPCC2018018983	CIP-004-6	R5.	[REDACTED]	[REDACTED]	06/22/2017	06/26/2017	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 violation.)		<p>On January 16, 2018, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on June 26, 2017, it was in noncompliance with CIP-004-6 R5. after the entity performed its quarterly electronic CIP access review.</p> <p>This noncompliance started on June 22, 2017 when the entity failed to revoke two (2) individuals' electronic access that the entity determined not to be necessary by the end of the next calendar day following the date of the individuals' transfer. The noncompliance ended on June 26, 2017 when the entity disabled the electronic access for the two (2) individuals.</p> <p>Specifically, in an effort to remove electronic access, IT removed the active directory account from a specific active directory role group rather than disabling the active directory account completely. As a result, electronic access remained enabled.</p> <p>The root cause of this noncompliance was incomplete processing of the CIP Transfer QA process checklist.</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 timely revoking electronic access to individuals that the responsible entity determines that the individual no longer requires could result in unauthorized access to BES Cyber Systems. The individuals in scope had specific electronic access and could have rendered BES Cyber Systems unavailable, degraded, or misused due to the noncompliance.</p> <p>The risk of the individuals causing harm to BES Cyber Systems was reduced by revocations being due to an internal transfer. The entity revoked one individual's physical access to BES Cyber Systems on June 21, 2017. The other individual retained their physical access due to a business need in their new role. The individuals in scope had received the required training and background checks were current and up to date.</p> <p>The entity confirmed that the individuals did not attempt to electronically access the system they had electronic access to between June 21, 2017 and June 26, 2017.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>						
Mitigation		<p>To mitigate the noncompliance, the entity:</p> <ol style="list-style-type: none"> 1. Disabled the active directory Accounts at issue; 2. Coached, counselled, and retrained the IT individual on the procedure. <p>Details to Prevent Recurrence:</p> <ol style="list-style-type: none"> 1. A compliance awareness supervisor's brief was issued to IT Security and IT Applications personnel 2. A weekly meeting is now being held to review current transferred individuals to ensure timely identification and action will be taken 3. A process to notify to all supervisors who transfer individuals has been enhanced to include when a response is required by supervisors (date & time) to ensure access is revoked within 24 hours when it is determined that access is no longer needed. 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019211	CIP-011-2	R1.	[REDACTED]	[REDACTED]	03/19/2017	11/16/2017	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 February 20, 2018, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on November 16, 2017 it was in noncompliance with CIP-011-2 R1. (1.2.) after identifying that three (3) contractors were provided access to BES Cyber System Information without following the entity's authorization process.</p> <p>This noncompliance started on March 19, 2017 when the entity failed to follow its process to protect BES Cyber System Information. The noncompliance ended on November 16, 2017 when the entity provided training to one contractor and removed access for the other two contractors.</p> <p>Specifically, three contractors were rehired and their old network IDs were reactivated which had access to Medium Impact BES Cyber System Information (without ERC). Due to the network ID's being reactivated, the entity's process to authorize access to designated storage locations was not followed.</p> <p>The root cause of this noncompliance was lack of a process to review old network profile access to validate requirements and business need to old access prior to reactivation.</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 its authorization process and not providing individuals with CIP Training prior to granting access to BES Cyber System information, the individuals being granted access may not be familiar with how to properly handle BES Cyber System Information which could lead to the unintentional exposure of BES Cyber System Information.</p> <p>The entity performed a review of access history for all three individuals and found no access attempts into the system from their respective rehire dates to their access termination or retraining date. The three individuals in scope had received training in 2016 and the access was limited to electronic versions of Medium Impact BES Cyber Assets without External Routable Connectivity drawings</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. Revoked access to 2 contractors 2. Provided training to 1 contractor <p>To prevent recurrence</p> <ol style="list-style-type: none"> 1. Implemented a manual review of new hirees' credentials before granting electronic access to Confidential-CIP information 2. Amended the CIP-011 documents to be more prescriptive as to the training and retraining requirements. 3. Implemented a new process of validating CIP Training credentials for rehired vendors and employees prior to granting access to Confidential-CIP information 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018020590	CIP-004-6	R5.	[REDACTED]	[REDACTED]	09/09/2018	09/17/2018	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 violation.)			<p>On October 30, 2018, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it had discovered on September 17, 2018, it was in noncompliance with CIP-004-6 R5. (5.1.) after the entity's physical security team received a termination notice from their human resources system.</p> <p>This noncompliance started on September 9, 2018, when the entity failed to complete the removal of physical access within their physical access control system within 24 hours of the termination action. An employee had effectively retired on September 7, 2018. The retired employee's manager submitted the termination request ten (10) days late in the HR system which interfaces with the physical control access system to disable CIP physical access. The noncompliance ended on September 17, 2018, when the entity disabled the retired employee's card from the physical access control system.</p> <p>The root cause of this noncompliance was a failure by the manager to follow internal procedures and submit a termination transaction in the HR system for the employee.</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 revoke physical access to a retired employee, the employee may continue to access the locations that are associated with High Impact BES Cyber Systems without a valid business need.</p> <p>The entity reduced the risk of the noncompliance by collecting the employee's badge, laptop, and substation keys on the retirement date. Physical security verified and confirmed that the employee's badge was not used and that no replacement badge was issued to the employee during the noncompliance period.</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) Disabled the employee's physical access within the PACS 2) Communicated CIP access revocation protocol and required tools and timeliness to process employee and vendor terminations 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019020904	CIP-004-6	R5.	[REDACTED]	[REDACTED]	10/29/2018	11/30/2018	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 January 08, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it had discovered on November 30, 2018, it was in noncompliance with CIP-004-6 R5. (5.2.) after reviewing the automatic access revocation log file.</p> <p>This noncompliance started on October 29, 2018 when the entity failed to revoke unescorted physical access to one employee by the end of the next calendar day. The noncompliance ended on November 30, 2018, when the entity revoked the employee's access.</p> <p>Specifically, an employee with authorized unescorted physical access rights to BES cyber assets transferred departments. The employee no longer required such physical access to BES cyber assets in their new role.</p> <p>The root cause of this noncompliance was a failure of the supervisor to contact the security control center to ensure timely access revocation.</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 revoking unescorted physical access, the employee could continue to access the locations without a valid business need and could have the intent to cause harm to entity BES Cyber Systems.</p> <p>A review of access records confirmed that the employee did not access substations during the period of noncompliance. The employee had up-to-date CIP training and a Personnel Risk Assessment. The employee has worked for the entity since 2014 and continues to work for the entity. The employee did not have electronic access to BES Cyber Systems.</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) Removed unescorted physical access 2) Issued a communication to all employees regarding the NERC CIP access revocation process 3) Provided targeted communication to NERC CIP access requestors and approvers 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019982	CIP-007-6	R2	[REDACTED]	[REDACTED]	2/28/2018	4/18/2018	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 June 27, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-007-6 R2. The entity failed to apply one security patch to 14 production servers in the [REDACTED] during the entity's December 2017 Patch Cycle. The patch was released on November 28, 2017 and should have been applied by February 28, 2018. The entity, however, did not apply the patch until April 18, 2018.</p> <p>Although the entity was receiving patches from the patch source, the received patches were not properly populating from the entity's [REDACTED] server to the cache on the production servers. That failure to populate resulted in the patch not being timely applied.</p> <p>The entity discovered the delayed installation of the patch on 14 servers after the entity administrator cleared and refreshed the cache on the affected servers while performing other work. When the administrator cleared the cache and issued the update command, the patch was downloaded and installed. [REDACTED] had already evaluated and tested the patch on its servers (in the testing environment) before the patch was downloaded and installed. This download and installation triggered the entity's [REDACTED] tool for baseline configuration changes to identify undocumented changes caused by the patch installation on the servers. The change was undocumented because installing the patch initiated a baseline configuration change not associated with the current [REDACTED] or any planned changes. The subsequent investigation determined the patch was from the December 2017 Patch Cycle that had already been completed. As part of the investigation, the administrator opened a problem ticket with the vendor to inquire about any known problems with the cache when downloading patches. The vendor identified no known issues.</p> <p>This noncompliance involves the management practices of validation and verification. The entity failed to design and implement procedural controls to provide confirmation that patches were appropriately applied in the production environment. That failure to design and implement validation and verification controls is a root cause of this noncompliance. (The entity determined a cause of the patching delays was due to a technical issue whereby the server cache did not properly populate with the applicable patch for the servers. [REDACTED] The download problem was resolved once the server cache had been cleared and refreshed.)</p> <p>This noncompliance started on February 28, 2018, when the entity was required to have applied the patch at issue to the 14 servers and ended on April 18, 2018, when the entity applied the overdue patch to the 14 servers.</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 failing to timely apply one patch to 14 servers increases the opportunity for vulnerabilities that could provide a larger attack surface via the unpatched servers. The risk is minimized because only one patch was applied just six weeks late to 14 servers. During the noncompliance, the software did not identify any unauthorized baseline changes, and the entity's software continued to monitor for security log events and the entity investigated any relevant events. Additionally, the 14 servers reside in the entity's isolated network and the entity's electronic defenses and perimeter security help ensure that no entity energy management systems have Internet access to or from the Electronic Security Perimeters (ESPs), which further reduces the risks.</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 there were different causes for the prior violation and the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) installed the security patch and verified its installation on the 14 servers; 2) developed a cache strategy whereby the server cache will be refreshed daily on all servers in the entity's testing environment and in Production; 3) updated the patch work instructions to require the cache to be cleared before the beginning of each patch cycle for Testing and Production; and 4) developed an additional control in the patching process as a final validation check that all applicable security patches have been applied in the production environment. <p>ReliabilityFirst 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
RFC2018019838	CIP-009-6	R2	[REDACTED]	[REDACTED]	2/18/2018	5/7/2018	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 June 4, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-009-6 R2. Specifically, the entity failed to perform required testing of information used to recover the functionality of a [REDACTED] (the "Switch") within a 15-month interval provided for in CIP-009-6 R 2.2. Due to an actual incident, a full recovery of the Switch was completed on November 18, 2016. Since the actual recovery incorporated information used to recover the functionality of the Switch, the actual recovery was substituted for testing in accordance with CIP-009-6 R 2.2. Based on the foregoing, the next test relating to the Switch should have been completed within 15 months of the actual recovery (i.e., on or before February 18, 2018). But, the next test was not completed until May 7, 2018, which was approximately 18 months after the actual recovery.</p> <p>The root cause of this noncompliance was a program gap. The entity implemented and utilized a program to monitor and account for compliance with CIP-009 recovery-related testing requirements; however, the program did not adequately track deadlines. On May 16, 2017, entity personnel reviewed the [REDACTED] and completed testing for the listed assets. They did not test the Switch because the actual recovery on November 18, 2016, satisfied the testing requirements. This created a scenario where the deadline to retest the Switch (i.e., February 18, 2018) was earlier than the deadline to test the other assets listed in the [REDACTED] (i.e., August 16, 2018). However, the entity did not note or effectively manage the earlier deadline for the Switch. For example, the [REDACTED] lacked a column to track due dates. By the time entity personnel reviewed the [REDACTED] again in May, 2018, the testing deadline relating to the Switch had already passed.</p> <p>This noncompliance implicates the management practice of workforce management. Workforce management includes the need to manage systems in a way that minimizes human factor issues, which can oftentimes be accomplished through the implementation of comprehensive, clear, and executable procedures.</p> <p>This noncompliance started on February 18, 2018, after the entity failed to complete required testing within the 15-month interval set forth in CIP-009-6 R 2.2 and ended on May 7, 2018, after the entity completed the testing.</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. Outdated and untested recovery plans and information may be unusable or incompatible with existing configurations, which could lead to an inability to recover from various hazards affecting Bulk Electric System (BES) Cyber Systems in a timely manner. In this case, the risk was mitigated by the following facts. The entity implemented controls and safeguards to reduce the likelihood of the occurrence of a hazard affecting the functionality of the Switch. For example, the entity utilized physical access controls [REDACTED]. The entity also utilized electronic access controls [REDACTED]. Further, the Switch was hardened, which further reduced the surface of vulnerability. [REDACTED]. In addition, the potential impact on the BPS was reduced by the entity's use of [REDACTED]. Lastly, it is worth noting that the entity had a plan and backups of the configuration that could be used to recover the asset and, in fact, did recover the asset's functionality in November, 2016. 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. The prior violations involved a complete lack of procedures and other fundamental issues, whereas the current noncompliance relates to a more limited issue that the entity quickly identified and resolved.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) added CIP-009 discussions to its weekly meeting agenda to ensure that CIP-009 requirements are monitored at the weekly meetings; 2) completed required testing; 3) created a dashboard for tracking CIP-009 requirements to address the root cause of the noncompliance and serve as a single point of reference for all CIP-009 requirement deadlines by asset name/type; 4) updated relevant templates, which provide formatting, criteria, and expectations for the required evidence of compliance; and 5) required relevant personnel to read and acknowledge that they understood the revised templates. <p>ReliabilityFirst 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
RFC2018019648	CIP-010-2	R1	[REDACTED]	[REDACTED]	12/21/2017	5/10/2018	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 April 25, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. The entity built, configured, and deployed three virtual vulnerability scanning devices (the Devices), which were Protected Cyber Assets (PCAs), for a power plant on December 21, 2017. The Devices were going to be used to [REDACTED]. The Devices were [REDACTED] and immediately powered off after installation. At the time of installation, the entity did not yet need the Devices to perform any monitoring or scanning functions. The plan was to power the Devices on when their monitoring and scanning functions were required.</p> <p>On February 22, 2018, the Devices were powered on because entity personnel were in the process of changing passwords after staff changes. While changing the passwords, the entity discovered that the Devices were deployed even though the entity did not have documented baseline configurations as required by CIP-010-2 R1. The entity's failure to follow its documented processes related to the deployment of Cyber Assets caused additional compliance issues, including the following: the deployments rendered ESPs undefined (CIP-005-5 R 1); the entity failed to properly manage interactive remote access (CIP-005-5 R2); the entity failed to enable only necessary ports (CIP-007-6 R1); the entity did not identify and evaluate patch sources and apply patches or develop mitigation plans (CIP-007-6 R2); the entity did not deploy methods to deter, detect, or prevent malicious code (CIP-007-6 R3); the entity did not configure security event monitoring (CIP-007-6 R4); the entity did not implement or utilize adequate system access controls (CIP-007-6 R5); and the entity failed to utilize required information protection procedures and failed to implement appropriate safeguards to prevent unauthorized dissemination of information upon reuse or disposal (CIP-011-2 R1 & R2).</p> <p>The root cause of this noncompliance was a failure to follow the entity's asset management process. The responsible employees and a vendor representative were unaware of the process and, therefore, failed to follow it.</p> <p>This noncompliance involves the management practice of workforce management, which includes promoting awareness and providing effective training to staff in support of their roles in maintaining Bulk Electric System (BES) reliability and resilience.</p> <p>The noncompliance started on December 21, 2017, when the Devices were installed and ended on May 10, 2018, after the entity complied with applicable CIP requirements relating to 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 (BPS) based on the following factors. The risk of failing to account for and adequately monitor and protect assets is the potential introduction or persistence of vulnerabilities that could be exploited and cause corresponding instability in the BPS. The risk was reduced here because the Devices were powered off immediately after installation and were powered on only to change passwords, thereby drastically reducing the opportunity for exploitation. Additionally, the Devices were [REDACTED], thus further reducing the potential risk. 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 involved different facts and circumstances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) brought the Devices into compliance and automated logging, which included, in part, accounting for the Devices in the entity's asset management database, documenting the existence of the Devices within ESPs, managing interactive remote access via firewall configuration and permissions, accounting for and managing ports and services, identifying a patch source, hardening the Devices through network positioning, access controls, and configuration, and documenting baselines for the Devices; and 2) verified that all subject matter experts read and understood the entity's revised asset management process. <p>ReliabilityFirst 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
RFC2019020946	CIP-004-6	R5; P5.2	[REDACTED]	[REDACTED]	6/7/2017	6/21/2017	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 September 30, 2017, the entity submitted a self-log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5.2. The entity compliance group identified a late revocation during the quarterly access verification review. An entity [REDACTED] Shift Supervisor failed to revoke physical access for one individual for one Physical Security Perimeter within the required timeframe once the supervisor determined that access was no longer needed. On 6/7/2017, the Shift Supervisor determined that an employee no longer needed access, but he did not initiate the revocation process. The physical access was removed on 6/21/2017.</p> <p>The root causes of the noncompliance were a lack of adherence to documented processes and a lack of understanding of how the access verification system worked.</p> <p>This noncompliance started on June 7, 2017, when the entity should have revoked the employee's access after determining the employee no longer required access and ended on June 21, 2017 when the entity revoked the employee's access.</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 (BPS). The potential harm to the reliability of the BPS that could have occurred is allowing an unauthorized employee physical access to a Physical Security Perimeter. The risk is minimized because the individual had completed NERC CIP cyber security training and had a successful Personnel Risk Assessment at the time access was retained. The individual had a valid business need and was authorized for access prior to the supervisor determining access was no longer needed. The individual did not use the access during the period of late revocation and the entity quickly identified and corrected the noncompliance.</p> <p>No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity:</p> <ol style="list-style-type: none"> 1) entered a [REDACTED] to remove the physical access; 2) communicated to all [REDACTED] supervisors on their responsibilities regarding the quarterly verification process; and 3) reviewed the list of [REDACTED] individuals with access to NERC CIP Assets and revoked access, as necessary. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019020948	CIP-004-6	R5	[REDACTED]	[REDACTED]	7/30/2016	4/30/2017	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 September 30, 2017, the entity submitted a self-log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. Entity Compliance staff identified [REDACTED] tickets manually submitted to Remove All access did not include the same line items as automatically generated [REDACTED] tickets. Entity IT Security Administration identified a code error that caused [REDACTED] to generate line items for Active Directory (AD) account removal that were not automatically processed.</p> <p>Entity IT Security Administration researched [REDACTED] tickets for any other late revocations due to the code error and identified the following:</p> <ul style="list-style-type: none"> • An individual's last work day was 7/29/2016 (Retirement 7/31/2016) and his access was not revoked from Bulk Electric System Cyber System Information (BCSI) repository until 8/3/2016. • An individual's last work day was 4/28/2017 (Retirement 4/30/2017) and his access was not revoked from several BCSI repositories until 4/30/2017. • A contractor's last work day was 12/7/2016 and his access was not revoked from BCSI repository until 12/8/2016 (25 hours). • A contractor's last work day was 9/23/2016 and his access was not revoked from BCSI repository until 9/25/2016. <p>The root cause of this potential violation was entity IT Security Administration made updates to [REDACTED] for automatic revocation in readiness for NERC CIP V5 and did not configure automatic revocation of access for entity AD Accounts when manual SRS tickets are submitted. The root cause was the coding error.</p> <p>This noncompliance started on July 30, 2016, when the entity should have revoked the first employee's access after the employee retired and ended on April 30, 2017 when the entity revoked the last employee's access.</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 (BPS). The potential harm to the reliability of the BPS that could have occurred is allowing unauthorized employees access to BCSI repositories. The risk is minimized because the duration for each of the occurrences was less than 5 days. Also, each individual at issue maintained a current Personnel Risk Assessment, cyber security training and voluntarily separated from the entity.</p> <p>No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity:</p> <ol style="list-style-type: none"> 1) removed access via [REDACTED] tickets; 2) implemented a code fix to automate all actions to disable the AD Accounts; 3) performed an extent of condition to identify any additional issues of late revocation and identify any additional controls required; 4) implemented any required controls based upon the extent of condition. Specifically, Access Request system changes are implemented for automatic approval of revocations but not yet active. Prior to activating, additional system changes or controls will be implemented to mitigate the risk of inadvertent removal via the automatic approval process and still ensure timely revocation. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020204	CIP-004-3a	R3	[REDACTED]	[REDACTED]	10/13/2013	8/1/2018	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 August 2, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-3a R3.</p> <p>The entity maintains a program to assure compliance with the requirements established in CIP-004 for the granting of unescorted physical and electronic access for contractors to Bulk Electric System (BES) Cyber Systems. Prior to granting unescorted physical or electronic access, the entity requires that authorization records, Personnel Risk Assessment (PRAs) records, and training records are all stored in certain repositories. At the entity, [REDACTED] manages the PRAs for contractors and [REDACTED] manages the PRAs for employees. In the entity's request and authorization process, entity staff review PRA and training evidence and note completion dates on the access request forms prior to the forms being presented for approval by the approving manager. [REDACTED] stores contractor PRA records in a designated repository.</p> <p>On April 4, 2018, during a [REDACTED] review of supporting PRA and training records for a sample of contractors, the entity identified that two PRA documents could not be located within the designated repositories. The entity subsequently located these two PRA records. As a result of this initial review, the entity expanded the review from a small sample to include all contractor PRAs from February 1, 2012 to May 31, 2018 to identify if any additional PRA documents could not be readily located.</p> <p>Upon completion of the review, any contractors that had active unescorted physical and electronic access who had PRA records that could not be located had access revocation initiated. The entity completed the expanded review on July 31, 2018 and determined the following gaps in PRA records:</p> <ul style="list-style-type: none"> a) Four instances where contractors were granted unescorted physical access and their initial PRAs could not be located; b) One instance where a contractor had an initial PRA, but an updated PRA could not be located; and c) One instance where the entity granted authorized electronic access and PRA evidence could not be located. <p>Three of the six instances, all related to unescorted physical access, were submitted between May 2013 and November 2013, when a transition of administrative support personnel occurred at the entity. The remaining three errors occurred between 2014 and 2016 where PRAs were apparently reviewed, but evidence of the PRAs were not appropriately stored in the designated repository. The entity initiated access revocation for these six contractors on August 1, 2018.</p> <p>This noncompliance involves the management practices of work management, implementation, and verification. Some of these instances occurred during project implementation that involves the entity processing multiple requests for physical or electronic access. During the review of PRA record evidence, the entity did not properly separate or index bulk PRA evidence and that made it difficult to quickly identify and retrieve the correct artifacts. [REDACTED]</p> <p>[REDACTED] The entity did not have an effective process in place to sort incoming PRA evidence and to verify and validate that the evidence was sorted and indexed correctly. [REDACTED]</p> <p>[REDACTED] That process failure is a root cause of this noncompliance.</p> <p>This noncompliance started on October 13, 2013, when the entity first granted access to a contractor with a missing PRA and ended on August 1, 2018, when the entity finished revoking unescorted physical and electronic access to BES Cyber Systems for contractors with missing PRA records.</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 providing the opportunity for untrusted or unreliable individuals to physically or logically access Critical Cyber Assets (CCAs), resulting in the misuse or compromise of CCAs. The risk is minimized because the entity followed the proper process for authorizing and provisioning access when access was initially granted in each instance; the entity simply misplaced the PRA records after access was granted. In order to obtain access initially, an access request is submitted. Prior to authorizing access, the completion date of the PRA record is referenced in the entity's authorization record. Authorization records are stored separately from the PRA and the entity retains these authorization records for all of the contractors involved in this noncompliance. This is primarily an administrative error and a documentation issue and only six individuals were affected during a period of more than six years (from February 1, 2012 to May 31, 2018). (The issue reported is specific to the retention of evidence of the completion of PRA for contractors, which are stored in a designated repository. In order to obtain access, an access request is submitted. Prior to authorizing access, the completion date of the PRA record is referenced in the authorization record. Authorization records are stored separately from the PRA.) 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 root causes of the prior noncompliance and the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</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
RFC2018020204	CIP-004-3a	R3	[REDACTED]	[REDACTED]	10/13/2013	8/1/2018	Self-Report	Completed
			<p>1) performed a complete assessment of all contractor PRA records that received unescorted physical or electronic access to BES Cyber Systems and associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) from February 1, 2012 to May 31, 2018;</p> <p>2) compiled a list of impacted records and the current status of access privileges for completion of reporting process, and where necessary revoked unescorted physical or electronic access to BES Cyber Systems and associated EACMS and PACS;</p> <p>3) obtained updated PRA records and restored access through a documented request and authorization processes, where necessary;</p> <p>4) evaluated the process for archiving compliance artifacts related to PRAs and developed a plan to improve the process; and</p> <p>5) conducted a meeting with the responsible personnel to communicate the new plan and train them on the new process. The entity conducted a training meeting with personnel responsible for filing authorization records. The agenda covered written documentation and practical demonstration of records organization.</p> <p>ReliabilityFirst 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
RFC2018020084	CIP-006-6	R1	[REDACTED]	[REDACTED]	4/30/2018	4/30/2018	Self-Report	6/3/2019
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 16, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-006-6 R1.</p> <p>On April 29, 2018, a transformer caught fire at the entity's Station A (Station A is classified as a Medium Impact Physical Access Control System (PACS)), and personnel were forced to de-energize the station to control the fire. (The forced de-energizing took place at 13:44 hours on April 29, 2018.) De-energizing the station disabled the primary access control system and caused the station's access control systems to run on battery backup until the batteries were completely drained and had died. (The access control system continued to run on battery backup until the batteries were completely drained at 18:39 hours with network loss occurring at 20:03 hours on April 29, 2018.) At that point, there were no means for authorized personnel to get into the control house. Following this, the [REDACTED] lost the ability to monitor the station for unauthorized access attempts through their monitoring system for approximately two hours. The entity had workers on site either to make repairs or specifically for human observation for the duration of the outage, except on April 30, 2018 from 01:05 hours to 03:00 hours, approximately two hours. That approximately two hour period during the morning of April 30, 2018 is the duration of the noncompliance. (The entity restored power and brought monitoring back online on May 1, 2018 at 10:46 hours.)</p> <p>This noncompliance involves the management practices of workforce management and grid maintenance. A root cause of the violation is the prolonged failure of the access control system. Another contributing cause is that, due to ineffective training, [REDACTED] personnel did not advise individuals on-site that they must remain in place for human observation. Because individuals did not remain in place for human observation, the [REDACTED] personnel had no way of detecting unauthorized access. The [REDACTED] lacked oversight controls to ensure CIP outage procedures were followed, advising individuals on-site that they must remain in place for human observation, prior to the failure of the backup access control system. (On April 29, 2018 at 13:53 hours, approximately 9 minutes after the station was de-energized, the entity created an outage record to track the situation at the [REDACTED]. The [REDACTED] operator overlooked the subsequent access control failures notification that should have led the operator to ensure individuals remain on site for human observation. When another [REDACTED] employee arrived the next morning and inquired about the status of the access control failure notification, an analysis of the current state at Station A led to the determination that human observation should have been mandated.)</p> <p>This noncompliance started on April 30, 2018, when the access control system first failed and [REDACTED] lost the ability to monitor for unauthorized access attempts through their monitoring system and ended approximately two hours later on April 30, 2018, when [REDACTED] regained the ability to monitor for unauthorized access attempts.</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 making it easier for individuals to enter into a Medium Impact Physical Access Control System (PACS) without authorizing or monitoring access. The risk was minimized because during the noncompliance, the PACS had no power, meaning there was no chance that an unauthorized individual could have accessed the access control systems. The electronic lock and strike within the doors to the control house deny by default due to the loss of electricity during this noncompliance. Second, the systems were only down for a short time, approximately two hours, before the entity initiated manual logging. Throughout the noncompliance and the associated fire, the entity personnel were acting in the best interest of the BPS and the entity's personnel. 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 current noncompliance has a different cause. The entity is also undertaking thorough and comprehensive mitigation for this noncompliance to help prevent recurrence.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity will complete the following mitigation activities by June 3, 2019:</p> <ol style="list-style-type: none"> 1) corrected the immediate issue with human observation. Station personnel were able to restore power and network at the station from the control house. All failures were restored. All systems were tested by the [REDACTED] with the assistance of the technician; 2) will increase Security leadership awareness by receiving automatic alerts to notify of any failures that occur at a location the [REDACTED] monitors. These alerts will be sent to the [REDACTED] and the Director of Physical Security; 3) will conduct a NERC CIP Stand Down for all operators in the [REDACTED] to help ensure they understand the importance of handling these alarms properly; 4) will segregate the NERC CIP desk so that the NERC CIP desk in the [REDACTED] will have its terminal modified to see only NERC CIP sites. The operator's console currently views 13,675 sensors and, after the change, the sensor view will be limited to the 6,646 NERC CIP sensors. This will reduce the number of failure alerts displayed on the screen. By segregating the site list, the NERC CIP desk will only be able to view and handle NERC CIP alarms, which will reduce errors in seeing the failure alerts; and 5) will conduct a [REDACTED] for all [REDACTED] operators that will be covered as part of the operators' next training to help reinforce how to handle CIP outage protocol and alarms properly for similar incidents. The entity will require each operator to sign a document stating they received and understood the training. <p>These mitigating activities will not be able to be completed until June 2019 because of the large amount of time it will take to segregate the NERC CIP desk so that the NERC CIP desk in the [REDACTED] will have its terminal modified to see only NERC CIP sites and the amount of time needed to develop and deliver the [REDACTED] for all [REDACTED] operators.</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
RFC2017018709	CIP-006-6	R2	[REDACTED]	[REDACTED]	8/24/2017	8/24/2017	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, the entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-006-6 R2. On August 24, 2017, an entity custodial contractor escorted two other custodial contractors into a Physical Security Perimeter (PSP), but left one of those visiting contractors unescorted within the PSP for approximately 3 minutes and 28 seconds. The entity discovered the issue the next day while conducting a routine review of available video and access logs. [REDACTED] equipment is located in the PSP, but the equipment is appropriately [REDACTED] or [REDACTED].</p> <p>The root cause of this noncompliance was the custodial contractor's failure to follow established procedures when serving as an escort for visitors. This major contributing factor involves the management practices of external interdependencies, which includes managing and monitoring external entity performance, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on August 24, 2017, when the entity custodial contractor left the visitor unescorted within the PSP, and ended approximately 3 minutes and 28 seconds later when the visitor 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 based on the following factors. The potential risk posed by failing to continuously escort visitors within a PSP is that the visitor could access protected equipment and systems. This risk was mitigated in this case by the following factors. First, the [REDACTED] equipment in the PSP was either [REDACTED] or [REDACTED], which reduces the likelihood that the visitor could have accessed any of that equipment. Second, the visitor was left alone for only 3 minutes and 28 seconds. This short duration reduces the likelihood that the visitor could have attempted to access the [REDACTED] equipment. Third, the entity identified this issue the next day during a routine review of video and access logs. This effective detective control reduces the risk in this case because if the visitor had done something nefarious to the [REDACTED] equipment, the entity would have discovered it the next day and could have taken corrective actions. 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 noncompliances involve conduct which ReliabilityFirst determined constitutes high frequency conduct for which the entity has demonstrated an ability to quickly detect and correct noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) suspended escorting privileges for the custodial contractor escort; and 2) provided verbal coaching for the custodial contractor escort. <p>ReliabilityFirst 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
RFC2018019727	CIP-010-2	R1	[REDACTED]	[REDACTED]	2/14/2018	3/12/2018	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 May 11, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-010-2 R1. On February 20, 2018, during the review of CIP-010 R2.1 configuration monitoring, the entity discovered that a software package was installed on a database server in the development environment of the entity [REDACTED] on February 14, 2018. The change was not authorized prior to deployment.</p> <p>As background, the database server was experiencing an issue with its backup functionality. An entity support team member opened a help desk ticket with the vendor and proceeded to install the software package at the vendor's suggestion. The support team member did not open a change management ticket because he did not realize that the device was classified as a Bulk Electric System (BES) Cyber Asset (BCA). [REDACTED]</p> <p>[REDACTED] Although the device was a development device, it was still classified as a BCA [REDACTED] for systems inside the Electronic Security Perimeter (ESP).</p> <p>The root cause of this noncompliance was the support team member's failure to recognize that this device was classified as a BCA. [REDACTED] These major contributing factors involve the management practice of workforce management, which includes managing the system to minimize human performance issues.</p> <p>This noncompliance started on February 14, 2018, when the entity support team member installed the software package and ended on March 12, 2018, when the entity created a change management ticket and updated the baseline to document the installation of the software package.</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 posed by failing to properly authorize and document a change that deviates from the baseline is that the unauthorized change could introduce vulnerabilities or system instability. This risk was mitigated in this case by the following factors. First, the entity identified the issue quickly (i.e., within 6 days) through effective detective controls [REDACTED]. Second, the software package involved in this noncompliance was a stable, established software that was installed at the direction of the vendor to further reduce risk. Third, the affected device has minimal operational interaction with BCAs within the ESP associated with the BES Cyber System. Therefore, the loss of this device would not negatively impact the operation of the BES Cyber System at issue in this case. ReliabilityFirst also notes that this software was installed on all similar devices with no negative impact to those devices. 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 noncompliances were either the result of different causes or involve conduct that ReliabilityFirst determined constitutes high frequency for which the entity has demonstrated an ability to quickly identify and correct noncompliance. Thus, the prior noncompliance does not warrant an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) sent an awareness email to the entity [REDACTED] group directing them to verify the NERC CIP classification/assessment of devices prior to making changes; 2) performed a stand-down meeting with the performer in question as well as members of the [REDACTED] group, expanding upon the directives contained in the awareness email. Agenda items of the stand-down included: verifying the assessment of devices, location of [REDACTED], and proper [REDACTED]; 3) entered a change management request to document the vendor software package installation and update the baseline change authorizations for the device; 4) provided change management refresher class to the applicable entity technicians and leads with assigned responsibilities to update devices in any entity IT environment; and 5) [REDACTED] <p>[REDACTED] The entity communicated job aid update to change management personnel required to use the job aid in performing their duties.</p> <p>ReliabilityFirst 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
RFC2018019728	CIP-011-2	R1	[REDACTED]	[REDACTED]	8/11/2017	6/4/2018	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 May 14, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-011-2 R1. During a station drawing update on March 9, 2018, the entity discovered 2 prints containing Bulk Electric System (BES) Cyber System Information (BCSI) for a medium impact location that were not labeled as BCSI and were not stored in a CIP-protected location. (These two prints [REDACTED] that are typically considered BCSI at the entity.) [REDACTED]</p> <p>Prior to July 1, 2016, the 2 prints at issue here were in a "project" status in the document management system, [REDACTED]. In preparation for CIP v5, the entity reviewed and evaluated master prints for BCSI applicability, but did not consider project prints. Therefore, when these 2 projects prints were published as master prints on August 11, 2017, the BCSI contained on these prints was not properly identified and protected accordingly.</p> <p>During its extent of condition review, the entity discovered another 21 drawings that should been stored in the CIP-protected vault but were not. The entity failed to properly identify and protect these drawings as containing BCSI due to a technical issue with the document management system. [REDACTED]</p> <p>[REDACTED] Essentially, the document management system crisscrossed the drawings and sent them to the wrong vault.</p> <p>The root causes of this noncompliance are as follows. For the original 2 prints, the root causes were the responsible individual's failure to validate the classification of the prints prior to making a change, and the fact that the job aid did not explicitly require the responsible individual to do so. For the other 21 drawings, the root cause was the software issue that caused the drawings to be sent to the wrong vault. These major contributing factors involve the management practices of workforce management, which includes managing the system to minimize human performance issues, and verification, in that the entity failed to have a verification step in its processes related to identifying and protecting BCSI.</p> <p>This noncompliance started on August 11, 2017, when the entity published the first 2 prints as master prints without identifying and protecting them appropriately and ended on June 4, 2018, when the entity relocated the 21 additional drawings to the CIP-protected vault.</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 posed by failing to properly identify and protect BCSI is that it increases the likelihood that an unauthorized individual could obtain sensitive information and cause adverse impact to the BPS. This risk was mitigated in this case by the following factors. First, although they were not stored in the CIP-protected vault, these drawings were still stored in the main vault, which provided some protection. For example, [REDACTED]. Second, the drawings at issue relate to substations without external routable connectivity. This means that even if an unauthorized person were able to obtain these drawings, that person would only be able to use the information while they were physically present at the associated substation. These substations are physically secured as medium impact substations, which reduces the likelihood that a person could gain unauthorized physical access. 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 they were the result of different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) labeled and stored the two prints in the CIP-protected vault according to the entity's information protection program requirements; 2) met with respective contractors to reinforce the entity's information protection program requirements; 3) instituted a new reporting mechanism to account for project drawings associated with Medium Impact sites; 4) identified the list of CIP Protected documents impacted by the technical software limitation and relocated them to the CIP-protected vault (with respect to the additional 21 drawings identified); 5) worked with the vendor to identify system issues and provided status and initial direction to the team; 6) compiled a draft list of all Medium Impact project prints to be evaluated for BCSI; 7) implemented the proposed initial solution for near term work and confirmed its implementation; 8) performed a Peer Check/Quality Review of the list [REDACTED] to verify that all project prints have been accounted for and provided the final list to [REDACTED]; 9) revised NERC CIP BCSI QA Review to account for design package reviews; 10) provided awareness to CIP drawings administrators on the vaults crisscrossing issue and prevention steps; 11) continued working with the vendor to identify the possibilities of a longer term technical solution to the software limitation, and communicated the results to impacted employees; and 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019728	CIP-011-2	R1	[REDACTED]	[REDACTED]	8/11/2017	6/4/2018	Self-Report	Completed
			12) reviewed and evaluated applicable prints [REDACTED] to determine which prints, if any, contain BCSI and mitigated applicable prints per program requirements. ReliabilityFirst has verified the completion of all mitigation activity.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018629	CIP-002-5.1	R1	[REDACTED]	[REDACTED]	7/1/2016	9/13/2017	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 3, 2017, the entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-002-5.1 R1. On July 19, 2017, while reviewing substation connectivity for CIP-003 applicability, the entity discovered that a substation was not included in the approved list of assets containing low impact Bulk Electric System (BES) Cyber Systems (BCSs). This substation is a non-BES substation, but contains cyber assets that function in conjunction with the cyber assets that protect BES equipment at another substation, which is a part of the BES. The entity performed an extent of condition review and discovered two additional substations that were not included on the approved list.</p> <p>The root causes of this noncompliance are as follows. For two of the substations, the root cause was that assets containing devices in scope for PRC-005, including non-BES substations, were not considered in the [REDACTED] asset evaluation process. For the third substation, the root cause was the fact that the substation was previously deemed out of scope, but due to a device upgrade, was pulled in-scope, but the entity failed to reevaluate the site. These root causes involve the management practice of asset and configuration management, which includes identifying assets and configuration items, and defining their attributes.</p> <p>This noncompliance started on July 1, 2016, when the entity should have [REDACTED] and ended on September 13, 2017, when the entity [REDACTED].</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 associated with failing to identify assets that contain low impact BES Cyber Systems is that the entity will not properly secure those assets due to lack of awareness. This risk was mitigated in this case by the following factors. First, this issue was limited to 3 out of 37 possible sites. So, this was an isolated incident and not indicative of a programmatic issue. Second, the three sites in question do not have external routable connectivity and are secured through the entity's standard physical and electronic access controls, including at a minimum, [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 noncompliances were either the result of a different cause or involve conduct that was isolated in nature and not indicative of any programmatic issues that would warrant an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the CIP-002 asset list based on review of PRC-005 in-scope list and CIP-002 asset lists; 2) updated the CIP-002 [REDACTED] Procedure to capture that the entity [REDACTED] unit will notify [REDACTED] of all potential assets containing Low Impact BCSs that need to be reviewed for CIP-002 applicability; and 3) developed a document to capture the CIP-002 review process for [REDACTED] and communicated to CIP Subject Matter Experts. <p>ReliabilityFirst 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
RFC2017018344	CIP-010-2	R1	[REDACTED]	[REDACTED]	1/11/2017	11/8/2017	Self-Report	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 September 8, 2017, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. The entity identified six change management issues where it did not adequately execute its process to authorize and document changes that deviate from the existing baseline for in-scope devices. The entity self-identified the first three instances during the normal course of its day-to-day work. The entity self-identified the remaining three instances during the extent of condition review it initiated as a result of the first three instances.</p> <p>First, on June 24, 2017, the entity self-identified a case where a printer driver downloaded automatically and impacted the baseline of a [REDACTED] supporting the entity energy management system (EMS) system. On June 7, 2017, the team member was logged into a console in the Electronic Security Perimeter (ESP). That team member initiated a [REDACTED] to the affected [REDACTED] in the same [REDACTED]. Upon connecting to the [REDACTED], an update of a printer driver automatically initiated on the [REDACTED], pulling the source files from the console. This installation was initiated without any prompting to the logged-on team member. Because the driver download was not planned, there was no change management ticket submitted for this installation. The major factor contributing to the cause of this instance of the noncompliance was the automatic printer mapping setting on the [REDACTED].</p> <p>Second, a planned change to software was scheduled to be installed on 49 servers supporting the entity EMS systems on July 17, 2017. This was considered to be a baseline affecting change. The change management ticket had manager approval, but the ticket was returned by entity [REDACTED] due to required fields on a new installation template not being completed. The team member submitting the ticket was not familiar with how to use the new template and advanced the change without the full approval needed from entity [REDACTED]. Consequently, on July 14, 2017, the software was installed on 24 of the in-scope devices prior to being approved by [REDACTED]. Entity [REDACTED] discovered the issue on July 18, 2017, and contacted entity [REDACTED]. The installation ticket was edited, and the ticket was approved. After that, the software was installed on the other 25 in-scope devices.</p> <p>Third, while deploying security updates to the entity [REDACTED] EMS system on April 12, 2017, one of the backup production consoles was inadvertently targeted for deployment, and had [REDACTED] installed on it prior to completing testing in the [REDACTED] environment. A member of the entity [REDACTED] team identified the issue on April 21, 2017, while verifying the installation of patches in the [REDACTED] environment. The deployment was approved for the entity [REDACTED] EMS system under an existing work management ticket. However, the additional production console at issue was inadvertently included when selecting devices in the deployment list for the [REDACTED]. Additionally, the responsible individual failed to verify successful deployment of the change on all targeted assets, which resulted in an unplanned deployment of the change to an asset during troubleshooting on September 18, 2017.</p> <p>Fourth, on March 22, 2017, a member of the entity [REDACTED] submitted a change management ticket to install software on 3 servers supporting the entity EMS system. On March 28, 2017, the software was installed without obtaining the proper approvals. The software at issue is used for [REDACTED]. The entity identified this issue during the extent of condition review it initiated for the previous three instances. The extent of condition review was completed by August 18, 2017.</p> <p>Fifth, on April 12, 2017, a member of the entity [REDACTED] submitted a change management ticket to install software on 13 servers supporting the entity EMS system. On April 16, 2017, the software was installed without obtaining the proper approvals. The software at issue is used for [REDACTED]. The entity identified this issue during the extent of condition review it initiated for the previous three instances. The extent of condition review was completed by August 18, 2017.</p> <p>Sixth, on January 10, 2017, a member of the entity [REDACTED] submitted a change management ticket to decommission a server that had previously supported the entity EMS system. On January 11, 2017, the asset was turned off and unplugged from the ESP without submitting the appropriate change management ticket. The entity identified this issue during the extent of condition review it initiated for the previous three instances. The extent of condition review was completed by August 18, 2017.</p> <p>The root cause of this noncompliance was insufficiencies in the entity’s change management program, including oversight and task management. This root cause involves the management practices of asset and configuration management, which includes controlling changes to assets and configuration items and baselines, and workforce management, which includes managing the system to minimize human performance issues.</p> <p>This noncompliance started on January 11, 2017, when the entity was required to comply with CIP-010-2 R1 and ended on November 8, 2017, when the entity corrected the issue with the automatic printer mapping setting on the [REDACTED].</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 implementing changes without full approval is that the change may have an adverse impact on the affected devices. This risk was mitigated in this case by the following factors. First, in 4 of the 5 instances where software was installed prior to full approval, the software was tested in the [REDACTED] environment prior to deployment, which reduced the risk that adverse impact would have occurred. In fact, the entity maintenance</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
RFC2017018344	CIP-010-2	R1	[REDACTED]	[REDACTED]	1/11/2017	11/8/2017	Self-Report	Completed
			<p>procedures dictate that all maintenance is performed on the inactive system, which reduces the likelihood that an adverse impact would have occurred on the active system. Second, the entity has built-in redundancy for the assets at issue, so if an adverse impact had occurred, it would have been unlikely to cause performance issues with the system overall. 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 or involve conduct that ReliabilityFirst has determined constitutes high frequency conduct that does not dictate an alternative disposition method.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) held a stand-down with entity [REDACTED] emphasizing the importance of verifying asset lists in deployment groups prior to scheduling deployment; 2) conducted an investigation into incident #1 with all relevant groups to determine if incident #1 was a cyber incident (it was not); 3) held a stand-down with entity [REDACTED] to reinforce the importance of verifying all approvals are completed prior to beginning work; 4) reverted change in printer driver version; 5) established and conducted a weekly review of entity change management tickets at a new or through existing meeting; 6) disabled printer redirection and automatic driver updates for entity [REDACTED] in the energy management system; 7) implemented methods to enhance visibility of ticket status in database/change management communication; and 8) hosted review session for performer-level documentation with entity [REDACTED] covering the following areas: (i) Change Management; (ii) Security Control Testing; (iii) Asset Onboarding; and (iv) Asset Decommissioning. Updated documentation based on review sessions. <p>ReliabilityFirst 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
RFC2018019812	CIP-006-6	R2	[REDACTED]	[REDACTED]	3/8/2018	3/8/2018	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 May 24, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R2. On March 8, 2018, while performing maintenance at a substation, the entity discovered that an employee incorrectly plugged his laptop (a non-CIP Cyber Asset) into a switch [REDACTED] within the substation Physical Security Perimeter (PSP).</p> <p>The switch that the employee plugged the laptop into was connected to Intelligent Electronic Devices (IEDs) [REDACTED]. After the laptop had been plugged into the switch for less than two minutes, the supervisor noticed what had occurred and instructed the employee to unplug the laptop.</p> <p>At the time of the incident (on March 8, 2018), the employee that plugged his laptop into the switch had approved electronic access, but had not yet received approved physical access to the PSP. As a result, the employee was treated as a visitor. When the supervisor directed the employee to plug his laptop into the corporate LAN in order to access the intermediate system and perform relay maintenance, the employee inadvertently plugged his laptop into the switch [REDACTED]. The supervisor did not immediately notice this action because the supervisor had his back turned when he plugged the laptop into the switch. The employee had the laptop connected to the switch for less than two minutes. The noncompliance arises from the supervisor leaving the employee unescorted inside the PSP by briefly turning his back to the employee.</p> <p>This noncompliance involves the management practice of workforce management through ineffective training. The supervisor was not effectively trained on the strict requirements of continuous escorting. That ineffective training is a root cause of this noncompliance.</p> <p>This noncompliance started on March 8, 2018, when the entity supervisor left the employee unescorted by turning his back to the employee while the employee was inside the PSP and ended two minutes later on March 8, 2018, when the entity supervisor turned around and began properly escorting the employee again.</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 a visitor to be unescorted inside a PSP which could cause harm to BES Cyber Systems. The risk is minimized because the supervisor only left the employee unescorted for two minutes inside the PSP when the entity supervisor turned his back to the employee. Additionally, the employee had approved electronic access, had completed the 2018 Annual CIP Training, and had a valid personnel risk assessment. [REDACTED]</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 instant noncompliance is distinguishable from the prior noncompliances because of different causes. Additionally, the entity promptly identified, assessed, and corrected the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) had the supervisor complete supplemental training that reiterates the entity's escorting requirements; 2) had the supervisor discuss the incident with his team and reiterate the entity's requirement that personnel who have not been authorized for unescorted access to an applicable PSP, must be continuously escorted by an employee with authorized access to the PSP; 3) distributed two internal electronic communications to all entity Transmission employees to reiterate the entity's escorting policy' 4) posted a guide and short video outlining Escort Responsibilities within NERC CIP PSPs on the entity's internal security website; and 5) modified the Physical Security Visitor Logging process to better describe the escort's responsibilities. <p>ReliabilityFirst 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
RFC2018019811	CIP-010-2	R4	[REDACTED]	[REDACTED]	1/24/2018	3/8/2018	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 May 24, 2018, the entity submitted two Self-Reports stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R4.</p> <p>First, on March 8, 2018, while performing maintenance at a substation, the entity discovered that an employee plugged his laptop (a non-CIP Cyber Asset) into a switch [REDACTED] within the substation Physical Security Perimeter (PSP). That action resulted in this first noncompliance.</p> <p>The switch that the employee plugged the laptop into was connected to Intelligent Electronic Devices (IEDs) [REDACTED]. After the laptop had been plugged into the switch for less than two minutes, the supervisor noticed what had occurred and instructed the employee to unplug the laptop.</p> <p>At the time of the incident (on March 8, 2018), the employee that plugged his laptop into the switch had approved electronic access, but had not yet received approved physical access to the PSP. As a result, the employee was treated as a visitor. When the supervisor directed the employee to plug his laptop into the corporate LAN in order to access the intermediate system and perform relay maintenance, the employee inadvertently plugged his laptop into the switch [REDACTED]. The supervisor did not immediately notice this action because the supervisor had his back turned when he plugged the laptop into the switch. The employee had the laptop connected to the switch for less than two minutes.</p> <p>This first noncompliance involves the management practice of workforce management through ineffective training. The employee was not effectively trained to only plug his laptop into the corporate LAN and not into the switch. That ineffective training is a root cause of this noncompliance.</p> <p>Second, on January 24, 2018, two of the entity's [REDACTED] field personnel needed to modify relays settings on an IED, classified as a [REDACTED] located within a substation Electronic Security Perimeter (ESP).</p> <p>When attempting to modify the settings through the intermediate system, network communications were intermittent and the field personnel could only complete a partial settings update. The field personnel contacted the [REDACTED] to request permission to connect serially to the front port of the IED in order to complete the settings update. The PCE employee escalated the issue to his supervisor, who was unavailable at the time. The field personnel also considered using a cellular hot spot or remotely pushing the settings, [REDACTED]. Because of the delay in receiving approval from the [REDACTED] the field personnel's manager gave permission to connect serially to the IED without the use of an intermediate system. That decision created this second noncompliance.</p> <p>This second noncompliance involves the management practices of workforce management and work management. Both are involved because the [REDACTED] field personnel's manager was not effectively trained to wait for a response from the [REDACTED] group before authorizing a serial connection to the IED without the use of an intermediate system. That ineffective training and failure to follow the proper procedure are both root causes of this noncompliance.</p> <p>The noncompliances started on January 24, 2018, the date the second noncompliance began, when the entity employee connected his laptop serially to the IED without the use of an intermediate system and ended on March 8, 2018, the date the first noncompliance ended, when the entity employee unplugged his corporate laptop from the Medium Impact BES Cyber System.</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. Regarding the first instance, [REDACTED] the risk posed by this noncompliance is allowing an unauthorized laptop to connect to a BES Cyber System that could cause harm to the BES Cyber System. The risk is minimized because [REDACTED] was disabled within the SCADA critical LAN at the station, meaning the corporate laptop did not receive a valid IP address and could not connect to the IEDs. In order to exploit the connection, the employee would have had to assign his laptop a static IP address within the IP subnet used by the switch or that was the gateway IP address to access other transmission substation ESPs. Since the employee did not have administrative capabilities to configure a static IP address, it was impossible for the employee's laptop to obtain interactive access to BES Cyber Systems within the ESP.</p> <p>Regarding the second instance, the risk posed by this noncompliance is allowing a serial connection to the IED without the use of an intermediate system and that could cause harm to BES Cyber Systems. The risk is minimized because the field personnel were physically at the substation and only connected serially. The laptop that was serially connected to the IED was protected with regular security patching and anti-virus. The risk is further reduced because the entity completed the relay settings update without any harm or misuse of the BES Cyber System.</p> <p>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
RFC2018019811	CIP-010-2	R4	[REDACTED]	[REDACTED]	1/24/2018	3/8/2018	Self-Report	Completed
			<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 instant noncompliance is distinguishable from the prior noncompliances because of different causes. Additionally, the entity promptly identified, assessed, and corrected the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <p>For the first instance:</p> <ol style="list-style-type: none"> 1) The entity disconnected the laptop; and 2) The entity discussed the incident with the team and reiterated the laptop restrictions during a safety meeting. <p>For the second instance:</p> <ol style="list-style-type: none"> 1) updated its "CIP Laptop Computer Usage Policy" to clearly communicate the prohibition of directly connecting to BES Cyber Systems within an Electronic Security Perimeter (ESP); 2) clarified the exceptions for when field personnel can directly connect to an IED. In each exception, the IED is disconnected from the ESP; and 3) issued an announcement to all affected personnel communicating the revisions to the policy. <p>ReliabilityFirst 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
RFC2018020085	CIP-010-2	R1	[REDACTED]	[REDACTED]	2/27/2018	5/2/2018	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 July 16, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-010-2 R1. The entity commissioned a [REDACTED] and put it into service on February 27, 2018. Subsequently, on April 18, 2018, the entity discovered that the [REDACTED] did not have the approved firmware identified in the baseline [REDACTED]. During the commissioning process, the asset manager and the asset administrator for the [REDACTED] overlooked the fact that the firmware [REDACTED] did not match the approved baseline set for the commissioning of the device. Specifically, the device was shipped with a newer version of the firmware than what was contained in the baseline. Consequently, the entity installed the firmware versions [REDACTED] without conducting the requisite testing. On May 2, 2018, the entity sent a [REDACTED] technician to install the correct, approved version of firmware to each of the [REDACTED].</p> <p>The root cause of this noncompliance was the nature of how the firmware revision levels are identified in the baseline [REDACTED] causing the asset handlers to not notice the discrepancies in the numbering. 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 workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on February 27, 2018, when the entity commissioned and placed the [REDACTED] into service and ended on May 2, 2018, when then entity installed the correct, approved version of the firmware to each of the [REDACTED].</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 making changes that deviate from the baseline without proper testing is that the changes could have an adverse effect on the associated devices. This risk was mitigated in this case by the following factors. First, the firmware version that was installed on the [REDACTED] was newer than what was contained in the baseline. These newer versions contained bug fixes to improve the performance of the device. Second, the discrepancies in the firmware were not security related, reducing the risk that the discrepancies would present a security-related problem. 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 violations and noncompliance were the result of different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) contacted the [REDACTED] vendor to lock firmware versions; 2) installed approved version of the firmware; 3) provided or reinforced training to new and current Asset Administrators on CIP controls; and 4) provided or reinforced training to new and current Engineering Asset Managers on CIP controls. <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
SERC2018019354	CIP-007-6	R5.7	[REDACTED]	[REDACTED]	7/1/ 2016	1/4/2018	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 2, 2018, [REDACTED] (the entity) submitted a Self-Report that, as a [REDACTED] and [REDACTED], it had an issue with CIP-007-6, R5.7.</p> <p>On July 1, 2016, the entity identified four devices that required Technical Feasibility Exception (TFE). While the servers met CIP-007-6, R5.7, the application residing on the servers did not. The application is not capable of logging and does not have the technical feasibility to limit unsuccessful login attempts or generate alerts after a threshold of unsuccessful attempts.</p> <p>The root cause of this issue was that the control process by which changes were controlled and implemented needed additional improvements to accommodate the new business needs.</p> <p>The noncompliance began on July 1, 2016, when CIP-007-6 became effective, and ended on January 4, 2018, when TFE for the devices was approved.</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>Although the entity did not have an approved TFE in place for the application, the logging and alerting were enabled and functioning at the operating system level of the Cyber Asset. Also, the four BES Cyber Asset (BCA) systems that were not covered under a TFE at the time of this issue, represented less than one percent of the total BCAs in production at that time.</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) Received an approved TFE. 2) Enhanced its internal control related to TFEs by establishing a standard questionnaire for all new CIP assets that will require a TFE. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019036	CIP-004-6	R5.5	[REDACTED]	[REDACTED]	8/3/2017	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 January 24, 2018, [REDACTED] (the entity) submitted a Self-Report that, as [REDACTED] and [REDACTED] it was in noncompliance with CIP-004-6, R5.5.</p> <p>On July 3, 2017, an employee was promoted from a supervisor to a manager. The transferee possessed knowledge of shared account passwords that would no longer required retention of. The password to the shared account was ultimately changed on August 4, 2017, which was 2 days past the CIP 30 days timeframe of August 2, 2017. Although the password was not changed within 30 days, the transferee's domain access and access to the password vault in the ESP were both revoked which would not allow access to the shared account.</p> <p>The root causes of this issue was that entity's internal control did not account for the personnel/department interactions needed in this particular situation.</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 noncompliance was short in duration (2 days). Although the shared account password was not changed within 30 days as required, the transferee's ability to access the shared account password was prevented by removal of the domain account and the ability to interactively access the password vault in the ESP where the password was stored.</p> <p>Entity does not have a relevant compliance history.</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) Updated its internal document to require specific steps and email notifications for staff transfers to prepare for required shared account password changes. 2) Required all relevant staff to read and sign the updated 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
SERC2018019355	CIP-004-6	R5.2			10/17/2017	4/6/2018	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 2, 2018, [REDACTED] (the entity) submitted a Self-Report that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-004-6, R5.2.</p> <p>On October 16, 2017, an employee officially transferred to a new position. Under the old and new position, the employee still required access to operating logging tool. On October 17, 2017, the user's account to operating logging tool was deactivated as no exception was requested or granted before the transfer date. Although the access removal appeared successful, the system did not actually remove the user account. On October 19, 2017 the transferee access was removed then subsequently approved and re-provisioned on October 24, 2017.</p> <p>On April 2, 2018, an employee officially transferred to a new position. Under the old and new position, the employee still required access to a specific database however no exemption was requested prior to the employee's transfer. On April 4, 2018, entity's Compliance staff executing the detective controls, identified that access still existed although it was marked as work completed by the database administration staff. The transferee access was subsequently approved and re-provisioned on April 6, 2018.</p> <p>The root cause of the first issue was ambiguous and incomplete instructions while the root cause of the second issue was human performance.</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>Both transferees still required access to the same systems in their new jobs as they did with their old position. Entity's detective controls worked properly in identifying the issues very quickly and modifying the controls further to minimize recurrences.</p> <p>No harm is known to have occurred.</p> <p>Regional Entity determined that the entity does not have a relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <p>Issue 1:</p> <ol style="list-style-type: none"> 1) Removed the transferee's access and re-provisioned it on October 24, 2017. 2) Revised its internal procedure for operating logging tool access to include additional instructions on removing user accounts. <p>Issue 2:</p> <ol style="list-style-type: none"> 1) Removed the transferee's access and re-provisioned it on April 6, 2018. 2) Revised its control process which included changing the detective control performed by Compliance staff to a preventative control. All relevant staff were updated of the changes. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019923	CIP-004-6	R5.2	[REDACTED]	[REDACTED]	5/20/2017	5/9 /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 25, 2018, [REDACTED] (the entity) submitted a Self-Report that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-004-6, R5.2.</p> <p>On May 15, 2017, an employee was granted unescorted physical access to the entity's control and data centers Physical Security Perimeter (PSP) for a 5 day training period. The entity uses a badge color system as a visual cue to staff to identify whether staff are in areas for which they are authorized. The employee was issued a badge color for unescorted physical access to the PSP with no provision to access the data center for the duration of the training. After the training, the access was changed back to physical access to the general building offices. Although the employee physical badge was changed to general building access only, due to an error, the badge access remained associated with the previously authorized PSP access.</p> <p>The root cause of this issue was incomplete instructions of internal procedure. The written document did not explicitly cover that controls needed for cases when a temporary access should be granted therefore the details of the written communication were incomplete.</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 employee is a long-term member of management team with a valid Personnel Risk Assessment (PRA) on file and has taken CIP Standards and Security Awareness training each year since being employed at the entity. In addition staff and guards in the PSP are trained to recognize badge colors, escort out and to report any unauthorized person immediately. The employee was unaware of such access and never accessed the PSP following completion of the training program.</p> <p>No harm is known to have occurred.</p> <p>Regional Entity determined that the entity did not have a relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) Removed physical access to a PSP from the employee's physical badge. 2) Updated its internal document that in the event access is requested for a defined duration, an automated incident ticket will be created at the time the access is granted. This will trigger a request to revoke the access on the end date of the duration set forth in the work order that granted the access. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018900	CIP-010-2	R2.1			5/2/2017	6/5/2017	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 22, 2017, (the entity) self-reported that as a , it had a possible instance of noncompliance for CIP-010-2, R2.1.</p> <p>On May 22, 2017, the entity discovered that it had missed monitoring one Cyber Asset baseline configuration for one review period. The asset's last review and update was on March 28, 2017 therefore the next review should have been performed by May 3, 2017.</p> <p>This asset has a baseline that has to be manually updated each month by the baseline owner and entered into baseline tracking tool, citing the incident as evidence. Due to a combination of administrative and human error, the 35-day required review was overlooked.</p> <p>Upon discovery, on June 5, 2017, minor adjustments were made to the asset baseline configurations. The changes were entered in the baseline tracking tool for monitoring.</p> <p>There were no baseline configuration changes to the asset between March 28, 2017 and June 5, 2017.</p> <p>The root cause of the issue due to the less than adequate changes that were made to the baseline tracking tool to include the asset for monitoring and tracking purposes.</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 asset was a CIP storage and switch device used for allowing primary and backup data centers to talk and determine which data center is currently running. If the Cyber Asset had lost functionality, the data centers continue to function and there would be no impact to the bulk power system (BPS). In addition, the Cyber Asset was located behind a firewall protecting the Electronic Security Perimeter (ESP). On September 7, 2017, the Cyber Asset was declassified as a CIP asset and removed from the ESP.</p> <p>No harm is known to have occurred.</p> <p>The entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1- Reviewed the baseline for changes in the baseline monitoring tool. 2- Created a specific group in the baseline monitoring tool to group the manually collecting storage assets. 3- Amended its internal procedure to require baseline tool administrators to check the accuracy of all manual entry CIP Asset groups. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019035	CIP-010-2	R1.2	[REDACTED]	[REDACTED]	7/24/2017	7/25/ 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 24, 2018, [REDACTED] (the entity) self-reported that as a [REDACTED] it was in noncompliance with CIP-010-2 R1.2.</p> <p>On July 24, 2017, an analyst failed to follow the entity's Baseline Configuration Management and Change Management Processes when making configuration changes into two CIP Assets (servers). The analyst incorrectly assumed that the server build ticket was acceptable to use as approval for the software installation therefore did not request or receive proper change request approval. Upon discovery of the issue on July 25, 2017, the configuration changes were backed out and after properly following the entity's Baseline Configuration Management and Change Management process, installed again on the two CIP Assets.</p> <p>This noncompliance duration was 1 day.</p> <p>The root cause of this issue was incorrect assumption that a correlation existed between request for change and the required approval to implement the change requests.</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 entity discovered this issue through an internal control and promptly mitigated it. The two servers were in the process of an initial build and were not in service or used for any reliability functions at the time the noncompliance occurred. The unauthorized changes were required for the function of the two CIP assets and upon receipt of proper approval were installed on the assets after following the entity's Baseline Configuration Management and Change Management processes.</p> <p>The entity does not have a relevant compliance history.</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- Backed out the unauthorized changes to the CIP Assets and ran a baseline verification that baseline exceptions no longer existed. 2- Implemented a new control where the applications support staff are not granted access to the asset until proper approval is received before the asset can advance into the "Staged" status. 3- Counseled the staff that no applications may be installed or configuration changes made unless proper steps and approval are received per Baseline Configuration Management and Change Management processes. 4- Provided refresher training for relevant staff. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018901	CIP-010-2	R1.5	[REDACTED]	[REDACTED]	4/7/2017	3/30/ 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 December 22, 2017, [REDACTED] (the entity) as a [REDACTED] self-reported two instances of noncompliance with CIP-010-2, R1.5.</p> <p>On April 7, 2017, during a restart of an internet proxy server to address the slow internet response time, a new version of the Google Chrome browser application had been installed on three physical desktop consoles because Google Chrome updates was allowed to bypass the proxy during restart of the firewalls. The auto-update occurred without the change being tested in a non-production environment prior to going into to the production environment.</p> <p>On March 27, 2018, the entity applied a software patch to eight physical production energy management system (EMS) production servers (BES Cyber Assets) before testing the patches in a non-production environment. The patch was for a software that allows control and monitoring of certain servers from a remote location. It is a service or enhancement as it helps the entity manage their servers easier.</p> <p>The first issue started on April 7, 2017 when the Chrome updates were installed and ended on April 10, 2017 when latent change process approvals were received (3 days). The second issue started on March 27, 2017 and ended on March 30, 2017 when patch was tested and redeployed into production (3 days).</p> <p>The root cause of the first issue was omitted steps due to staff distraction during unplanned tasks and the root cause of the second issue was that certain system interactions were not considered or identified previously in order for proper controls to be implemented accordingly.</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>Issue 1: The entity had planned to make the Google Chrome browser upgrade at a later time therefore once discovered the change had already occurred, submitted a latent change request for installation. The Google Chrome automatic update was applied to backup virtual machines used only in the event the primary virtual machines fail. The issues was discovered 3 days after the auto-update through a routine weekly review, and it was promptly mitigated to prevent recurrence. The three Cyber Assets involved have anti-malware software which alerts Cyber Security staff on a 24/7/365 basis. Any malicious activity detected on the Electronic Access Point (EAP) for the entity's Electronic Security Perimeter (ESP) would be detected by entity's intrusion prevention systems that alert the Cyber Security staff as well.</p> <p>Issue 2: The security patch has no impact to the EMS/BES reliability functionality because it is a service that helps entity's management of certain serves. Upon discovery, the patch was applied in a non-production test environment with no adverse effects. Furthermore, the EMS production systems were patched within 35 days of the patch assessment with no security vulnerability risk to the BPS.</p> <p>No harm is known to have occurred.</p> <p>Entity does not have a relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <p>Issue 1:</p> <ol style="list-style-type: none"> 1- Submitted a latent change request to complete the appropriate tasks needed to justify installation of the Google Chrome browser update on the three consoles. 2- Implemented a manual script to turn off the Google Chrome updates runs on both the physical and virtual consoles during the monthly patch cycle. The script deletes the scheduled task every time the PC boots to prevent the issue from occurring again without being vetted through the proper change management process. 3- A new technology was implemented that includes new configuration which does not allow Google Chrome to bypass the proxy and apply automatic updates during firewall reboots at the data center. <p>Issue 2:</p> <ol style="list-style-type: none"> 1- Applied the software patch to a non-production test environment with no adverse effects to the BES Cyber Assets. 2- Discussed and reminded the responsible employees the requirements for testing a patch in a non-production environment before applying the patch to the production environment and steps for better managing unscheduled changes and coordination. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019938	CIP-010-2	R2.1	[REDACTED]	[REDACTED]	8/5/2016	5/8/2018	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 25, 2018, [REDACTED] (the entity) as a [REDACTED] self-reported a noncompliance with CIP-010-2 R1.1.</p> <p>On March 1, 2016, a CIP Bulk Electric System (BES) Cyber Asset (BCA) was on-boarded for baseline monitoring into the entity's baseline configuration management and monitoring tool. On March 24, 2016, the IP address of the CIP asset was changed however its previous IP address was assigned to a similar asset that is non-CIP. Both CIP and non-CIP assets are same type of switches with same configuration. The entity's internal weekly asset verification process at the time only compared asset names and not IP addresses for accuracy. Since the two assets in this issue were switches and configured the same, it looked like the monitoring tool was monitoring the correct asset.</p> <p>The root cause of this issue was ineffective verification and validation practices.</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 is minimal due to the static nature of this asset. During this time period, no changes were made to the asset's baseline configuration and no vulnerabilities have been identified on it either.</p> <p>Entity ran a full IP script to verify address on all CIP assets and did not identify any other discrepancies with CIP Assets.</p> <p>No harm is known to have occurred.</p> <p>Entity does not have a relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1- Corrected IP address of the BCA in its monitoring tool. 2- Ran a full comparison between its asset management database and monitoring tool to determine if any additional IP addresses did not match. 3- Modified the existing control for weekly CIP asset verification between its asset management database and monitoring tool. 4- Incorporated changes to internal procedures to include new control steps. 5- Trained relevant staff on new procedural and system changes. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019139	CIP-004-6	R5			10/11/2016	4/6/2017	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 [REDACTED] WECC determined the entity, as a [REDACTED] [REDACTED] had a potential noncompliance with CIP-004-6 R5 Parts 5.1 and 5.2.</p> <p>Specifically, the audit team determined the entity did not complete the removal of two contractor's unescorted physical access, within 24 hours of the termination actions for those contractors. Additionally, the entity did not revoke an employee's authorized unescorted physical access by the end of the next calendar day following the entity's determination that the access was no longer needed when the employee was reassigned. The three individuals had unescorted physical access to a Physical Security Perimeter (PSP) for the Medium Impact BES Cyber System (MIBCS) at the primary and backup Control Centers.</p> <p>After reviewing all relevant information, WECC Enforcement concurs that the entity failed to complete the removal of unescorted physical access for two contractors within 24 hours of the termination action, as required by CIP-004-6 R5 Part 5.1, and failed to revoke authorized unescorted physical access that the entity determined was no longer needed by the end of the next calendar day following that determination for one employee who was reassigned, as required by CIP-004-6 R5 Part 5.2.</p> <p>The root cause of this issue was less than adequate procedures. Specifically, the CIP-004-6 procedures did not clearly define the processes, roles, and responsibilities to ensure compliance, especially as it related to the completion of access revocation for contractors or role reassignments, as those processes were manual.</p> <p>These issues began on October 11, 2016, November 5, 2016, and February 8, 2017, respectively when the entity should have completed access revocations, and ended on October 11, 2016, November 8, 2016, and April 6, 2017, when access was revoked, for a total of 12 hours, four days, and 58 days, respectively.</p>					
Risk Assessment			<p>WECC determined these issues posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In these instances, the entity failed to complete the removal of unescorted physical access for two contractors within 24 hours of the termination action, as required by CIP-004-6 R5 Part 5.1, and failed to revoke authorized unescorted physical access that the entity determined was no longer needed by the end of the next calendar day following that determination for one employee who was reassigned, as required by CIP-004-6 R5 Part 5.2.</p> <p>However, as compensation, the Cyber Assets associated with the MIBCS were physically protected 24x7 by entity employees who would have prevented any malicious activity. The three individuals did not have electronic access to any CIP Cyber Assets; the issue for the contractors was limited to 12 hours and four days in duration, during which time they did not attempt to access the PSP, and the role reassignment for the employee was not for disciplinary reasons. No harm is known to have occurred.</p> <p>The entity has no compliance history for this Standard and Requirement.</p>					
Mitigation			<p>To remediate and mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> completed physical access revocations for the contractors and employee in scope; updated its CIP-004-6 Account Management and Review Procedure, to include detailed physical access revocation processes that also covers contractors, defines roles and responsibilities for its Facilities, Information Technology, and Compliance Department personnel, and created an Access Revocation Termination and Transfer flowchart; created a Termination / Transfer Record Form to be used by personnel to collect measurable validation data to document the revocation of access within 24 hours of a termination action or transfer; and provided training to all AEPC personnel responsible for compliance with CIP-004-6 R5 to ensure each understands AEPC's updated CIP-004-6 Account Management and Review Procedure and what is required of each to meet the requirements of this standard. <p>WECC 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
WECC2018019142	CIP-005-5	R1	[REDACTED]	[REDACTED]	7/1/2016	1/31/2018	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 [REDACTED], WECC determined the entity, as a [REDACTED], had a potential noncompliance with CIP-005-5 R1 Part 1.3.</p> <p>Specifically, the audit team found the entity didn't require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default when the Electronic Access Point (EAP) rules could allow access from the MIBCS Electronic Security Perimeter (ESP) at the backup Control Center, to other networks allowed through the non-explicit access control lists (ACLs) of the EAP and further communication to non-trusted networks, through the routing of packets from the ESP network. This instance includes two EAPs to the MIBCS.</p> <p>After reviewing all relevant information, WECC Enforcement concurs that the entity failed to require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default, as required by CIP-005-5 R1 Part 1.3.</p> <p>The root cause of the issue was less than adequate processes. Specifically, the entity was using the EAP rule prior to the implementation of CIP Version 5 to maintain reliability of Supervisory Control and Data Acquisition services and to determine normal network traffic. However, due to the lack of documented processes, and roles and responsibilities, the EAP rule was not monitored and tracked for removal when CIP Version 5 was implemented.</p> <p>WECC determined this issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on January 31, 2018, when the entity removed the ACL rule, for a total of 580 days.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default, as required by CIP-005-5 R1 Part 1.3.</p> <p>However, the entity implemented internal controls to deter, detect, and prevent malicious code, physical port protections, and password protections. As further compensation, the entity implemented a tiered network design that included a demilitarized zone with Intrusion Prevention System devices which monitored traffic between networks. No harm is known to have occurred.</p> <p>The entity has no compliance history for this Standard and Requirement.</p>					
Mitigation			<p>To remediate and mitigate this issue, the entity has:</p> <ul style="list-style-type: none"> a. removed the ACL rule on the two Cyber Assets in scope; b. revised its ESP and Interactive Remote Access procedure to include the following procedural controls: <ul style="list-style-type: none"> i. ACLs that permit Internet Protocol any-any rules on an EAP firewall are not allowed ii. all test ACLs will include the word "test" in the description, a description for what service, protocol or application is being tested in the test ACL, "CreatedOnDate" of the test ACL, and "ToBeRemovedAfterDate" of the test ACL; and iii. secondary subject matter expert (SME) task to review the above controls are in place as a regular activity that generates evidence of compliance; and iv. conducted training with all SMEs to ensure understanding of the updated procedures, and what is required in order to be compliant with the Standard. <p>WECC 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
WECC2019020912	CIP-006-6	R1; P1	[REDACTED]	[REDACTED]	12/28/2018	12/28/2018	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 violation.)			<p>On January 10, 2019, the entity submitted a Self-Report stating, as a [REDACTED] it was in noncompliance with CIP-006-6 R1.</p> <p>Specifically, the entity reported that on December 28, 2018, an unauthorized individual entered a Physical Security Perimeter (PSP) containing High Impact Bulk Electric System (BES) Cyber Assets, due to a mechanical failure at the PSP access point. The individual inadvertently entered the PSP while looking for a private business that resides within the same building as the entity. A forced door alarm was generated within the entity's Physical Access Control Management System (PACS) which was immediately responded to by the entity's Security Officer; however, an entity employee within the PSP had already noticed the unescorted individual and was escorting them out of the PSP. Upon further investigation, the entity determined that the PSP access point door lock had sustained a solenoid failure and it replaced the door lock that same day.</p> <p>After reviewing all relevant information, WECC determined the entity failed to utilize two or more different physical access controls to collectively allow unescorted physical access into the PSP to only those individuals who have authorized unescorted physical access, as required by CIP-006-6 R1 Part 1.3.</p> <p>The root cause of the issue was a damaged, defective, or failed part. Specifically, the entity determined that the door lock to the PSP access point sustained a failure of the electronic-mechanical locking mechanism.</p> <p>This issue began on December 28, 2018, when two or more physical access controls were not utilized to enter a PSP, and ended on December 28, 2018, when the entity replaced the door lock that had malfunctioned, for a duration of approximately four hours.</p>					
Risk Assessment			<p>WECC determined 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 failed to utilize two or more different physical access controls to collectively allow unescorted physical access into the PSP to only those individuals who have authorized unescorted physical access, as required by CIP-006-6 R1 Part 1.3.</p> <p>The entity implemented strong detective controls. Specifically, the entity implemented an audible alert within five seconds for doors forced opened without the use of a badge or without motion detected by a motion sensor. The entity had a security guard station which was manned 24x7 for monitoring of forced open alarms. Security guards were required to investigate forced open alarms within five minutes, which this security guard did. As further compensation, the entity had implemented good compensating controls. Specifically, personnel working within the PSP at the time of the issue recognized an unescorted individual and immediately escorted the individual out of the PSP, as required by the entity's Physical Security Plan. The PSP is typically manned during normal business hours. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty because the root cause and fact pattern was distinct and separate from the issue in this CE.</p>					
Mitigation			<p>To remediate and mitigate this issue, the entity has:</p> <ul style="list-style-type: none"> a. removed the unauthorized individual from the PSP; b. replaced the PSP door lock and tested its functionality; c. tested all the PSP doors at this location to ensure this was an isolated event; and d. created a procedure to check all PSP door locks on a quarterly basis, to include a requirement for manual monitoring of the PSP access point if a lock should need to be replaced. <p>WECC verified the entity's 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
WECC2018019188	CIP-006-6	R2; P2	[REDACTED]	[REDACTED]	1/30/2018	1/30/2018	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 10, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in noncompliance with CIP-006-6 R2.</p> <p>Specifically, the entity reported that on January 30, 2018, a contractor who was being escorted while in a Physical Security Perimeter (PSP) containing High Impact Bulk Electric System (BES) Cyber System, needed to leave the PSP and retrieve supplies from his truck. The contractor was instructed by the escort to have the security officer, whose station was in the lobby which was also within the PSP, call the escort when escorting needed to resume. When the contractor returned, the security officer let him into the PSP and made several attempts to locate the escorts phone number but was unsuccessful because the security officer did not know how to find phone numbers in the phone system. The contractor was then told to remain in the lobby while the security officer went to look for the escort. It was confirmed that the contractor remained in the lobby unescorted for approximately 90 seconds, at which time the security officer and the escort returned and continued to escort the contractor within the PSP.</p> <p>After reviewing all relevant information, WECC determined the entity failed to continuously escort a visitor within the PSP as required by CIP-006-6 R2 Part 2.1.</p> <p>The root cause of the issue was less than adequate training on the entity's phone system. Specifically, the security officer attempted to find the phone number to reach the escort, however had not been properly trained on how to use the phone system and was unable to find the number.</p> <p>This issue began on January 30, 2018, when continuous escorting of a visitor within a PSP ceased, and ended that same day, when escorting commenced, for a total of approximately 90 seconds.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to continuously escort a visitor within the PSP as required by CIP-006-6 R2 Part 2.1.</p> <p>However, while the lobby was considered part of the PSP, there were no Energy Management System workstations or other CIP Cyber Assets located in the lobby. [REDACTED] The contractor was authorized to be escorted within the PSP and the duration of this issue was under two minutes. Additionally, the contractor was visible on video surveillance for the duration of the time he was unescorted, and the entity confirmed that the contractor never left the area. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty because the root cause and fact pattern was distinct and separate from the issue in this CE.</p>					
Mitigation			<p>To remediate and mitigate this issue, the entity:</p> <ul style="list-style-type: none"> a. commenced escorting of the contractor; b. provided training to all security officers as to how to use the phone system; c. sent out a security awareness reminder to all team members; and d. provided CIP-006-6 Visitor Control Training to all applicable personnel. <p>WECC verified the entity's 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
WECC2018019008	CIP-007-6	R2; P2	[REDACTED]	[REDACTED]	2/28/2017	1/12/2018	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 19, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in noncompliance with CIP-007-6 R2.</p> <p>Specifically, the entity reported that on January 3, 2018, during a reconciliation of baseline deviations, it discovered an application that had been removed from the patch source list was still present on the [REDACTED] servers. Upon review of the application, the entity discovered that while baseline configurations continued to be monitored, security patch evaluations for applicability had not been performed since January 23, 2017 for 30 Protected Cyber Assets (PCAs) associated with its High Impact Bulk Electric System (BES) Cyber System (HIBCS). Upon discovery, the entity performed a full review of baseline applications and associated patch evaluations for the affected Cyber Assets.</p> <p>After reviewing all relevant information, WECC determined the entity failed to evaluate security patches for applicability that had been released since the last evaluation from the source or sources identified in Part 2.1, at least once every 35 calendar days, as required by CIP-007-6 R2 Part 2.2.</p> <p>The root cause of the issue was a less than adequate process. Specifically, the entity used an independent patch tracker which had no correlation to the software inventory list leading to an inaccurate determination of which applications needed patches evaluated.</p> <p>This issue began on February 28, 2017, the 36th day security patches should have been evaluated for applicability for the affected PCAs, and ended on January 12, 2018, when the entity performed the security patch evaluations for applicability, for a total of 318 days.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to evaluate applicable security patches that had been released since the last evaluation from the source or sources identified in Part 2.1, at least once every 35 calendar days, as required by CIP-007-6 R2 Part 2.2.</p> <p>As compensation, no security patches had been released for the PCAs in scope of this issue during the issue timeframe. Additionally, all devices within the entities HIBCS had up-to-date antivirus installed, and the PCAs resided within an Electronic Security Perimeter, and in a defined Physical Security Perimeter. No harm is known to have occurred.</p> <p>The entity does not have any relevant previous violations of this or similar Standards and Requirements.</p>					
Mitigation			<p>To remediate and mitigate this issue, the entity:</p> <ol style="list-style-type: none"> a. completed the security patch evaluation for the PCAs in scope; b. developed and implemented an automated daily report which cross-checks commercially available security patch tracking entries against the security patch review log to ensure all available patches are evaluated. This is an automated process to compare the software inventory list to the patch list; and c. created an automated report to evaluate all baseline items for inactive security patch review application entries. This will alert if there are any patches that have not been reviewed. <p>WECC verified the entity's 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
WECC2018019930	CIP-007-6	R2; P2			4/1/2018	5/9/2018	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 Jun 20, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-007-6 R2.</p> <p>Specifically, the entity reported that on December 13, 2017, during the entity's monthly patch review for software products, it identified an applicable security patch. A mitigation plan was created in accordance with CIP-007-6 R2 Part 2.4, with a due date of March 31, 2018. The entity deployed the security patch on March 27, 2018 and closed the mitigation plan. On May 9, 2018, the entity's security analyst was performing baseline updates and validations documented procedures (Plan). Internal controls inherent to the Plan revealed that the software security patch had not been deployed on two SIEM servers in accordance with the previous software security patch mitigation plan. The two servers were classified as Electronic Access Control or Monitoring Systems (EACMS) associated with the High Impact BES Cyber System and were responsible for collecting, normalizing, and correlating logs within the entity's Electronic Security Perimeter to monitor for malicious activities. The security analyst notified the Information Technology team and the patch was immediately deployed to both EACMS. Additionally, the mitigation plan created for the security patch was originally scheduled to be completed no later than February 2018; however, on February 23, 2018, the plan was extended to March 31, 2018. The entity extended the mitigation plan without first obtaining CIP Senior Manager or delegate's approval.</p> <p>After reviewing all relevant information, WECC determined the entity failed to implement the mitigation plan within the designated timeframe or obtain approval from the CIP Senior Manager or delegate for an extension on the mitigation plan, as required by CIP-007-6 R2 Part 2.4.</p> <p>The root cause of the issue was a less than adequate documented process and unclear roles and responsibilities. Specifically, the process used by the entity to determinate which systems required security patches for discovered application vulnerabilities relied on a configuration manager used initially to deploy the software. These groups were statically configured and failed to capture systems such as the EACMS in scope of this issue, where software was initially deployed without the use of the configuration manager server. Additionally, tangible gaps were present in the process for notifying the owners of impacted systems and determining the party responsible for the deployment of security patches.</p> <p>This issue began on April 1, 2018, when the entity failed to implement the mitigation plan within the designated timeframe and failed to obtain approval from the CIP Senior Manager or delegate for an extension to the mitigation plan, and ended on May 9, 2018, when the entity applied the security patch to the two EACMS, for a total of 39 days.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to implement the mitigation plan within the designated timeframe and failed to obtain approval from the CIP Senior Manager or delegate for an extension to the mitigation plan, as required by CIP-007-6 R2 Part 2.4.</p> <p>The entity implemented good detective controls. Specifically, it utilized a baseline management plan which identified that the software security patch had not been applied on the two EACMS. As further compensation, the entity implemented hourly local system accounts monitoring for unauthorized access with immediate notifications of any suspicious activity; had host-based antivirus that monitors for and prevents the execution of malicious code on the local system and had firewall rules preventing unjustified traffic traversing to or from the collector network zone. No harm is known to have occurred.</p> <p>The entity does not have any relevant previous violations of this or similar Standards and Requirements.</p>					
Mitigation			<p>To remediate and mitigate this issue, the entity:</p> <ol style="list-style-type: none"> deployed the software security patch to the two EACMS; updated its security patch management and malicious software prevention policy to include language identifying the oversight of the CIP Senior Manager or delegate approval of patch mitigation plans; updated its process to include an email to be sent to the compliance department when a patch mitigation plan is created, extended, or updated, and when it is approved; and sent an email to all personnel notifying them of the procedure was updated. <p>WECC verified the entity's 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
WECC2018020223	CIP-010-2	R1; P1	[REDACTED]	[REDACTED]	7/4/2018	7/23/2018	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 August 16, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>Specifically, the entity reported that during its review of completed "business as usual" changes, a compliance security analyst identified a change control ticket that impacted CIP-010-2 baseline configurations. A change ticket with the "business as usual" categorization designated the change as non-CIP; therefore, it did not require the baseline configuration to be updated. The entity learned that on June 4, 2018, the change implementer who was completing the change ticket inadvertently categorized the change as a "business as usual" change instead of a CIP change for two BES Cyber Assets (BCAs) without External Routable Connectivity (ERC). Upon discovery, the entity immediately updated the baseline configuration documentation.</p> <p>After reviewing all relevant information, WECC determined the entity failed to update baseline configurations as necessary within 30 calendar days of completing a change that deviated from the existing baseline configuration for two BCAs, as required by CIP-010-2 R1 Part 1.3.</p> <p>The root cause of the issue was the accuracy and/or effectiveness of a change was not verified or validated. Specifically, the entity had no peer review or oversight in place to ensure the accuracy of work performed by the change implementer.</p> <p>This issue began on July 4, 2018, the 31st day when baseline configurations changes should have been updated on two BCAs, and ended on July 23, 2018, when those baseline configurations were updated, for a total of 20 days.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to update baseline configurations as necessary within 30 calendar days of completing a change that deviated from the existing baseline configuration for two BCAs, as required by CIP-010-2 R1 Part 1.3.</p> <p>The entity implemented strong detective controls. Specifically, it implemented an internal review of change records to determine if any baselines were not compliant, which is how this issue was discovered. As further compensation, the entity implemented physical security controls to prevent physical access to the BCAs as verified by WECC. Additionally, the BCAs in scope had no ERC. No harm is known to have occurred.</p> <p>The entity does not have any relevant previous violations of this or similar Standards and Requirements.</p>					
Mitigation			<p>To remediate and mitigate this issue, the entity:</p> <ol style="list-style-type: none"> a. updated the baseline configurations for both BCAs; b. created a script that will detect if a change control ticket for a CIP device is improperly categorized as a business as usual change; c. added content validation to the categorizing of change control tickets (All "business as usual" categorization will inhibit the CIP-010 selection field); d. added two additional reports to the CIP Report which can be used to review baselines that are required to be updated and the analyst assigned; e. developed and implemented a change control review and archive procedure; and f. provided knowledge reinforcement of change control and configuration management policy to applicable employees. <p>WECC verified the entity's 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
WECC2018018916	CIP-010-2	R2; P2			6/30/2017	8/15/2017	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 December 29, 2017, the entity submitted a Self-Report stating, as a [REDACTED] it was in noncompliance with CIP-010-2 R2.</p> <p>Specifically, the entity reported that while conducting an internal compliance review, it identified that its manual baseline configurations were not monitored within the 35-day timeframe. The entity discovered that the system which sends workflow email reminders when the monitoring of the baselines task to be completed, was being upgraded, which caused the notifications to fail. As systems personnel were not notified by email that baselines reviews were due, the task was not completed for the affected devices. The devices subject to this instance included six BES Cyber Assets (BCAs) without External Routable Connectivity (ERC), which were part of the entity's High Impact BES Cyber System. While no baseline changes were identified during this time it was determined that the monitoring reviews were not performed in a timely manner.</p> <p>After reviewing all relevant information, WECC determined the entity failed to monitor, at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1) and document and investigate detected unauthorized changes, as required by CIP-010-2 R2 part 2.1.</p> <p>The root cause of this instance was a software failure. Specifically, during an upgrade to the workflow system, the task reminder notifications failed to be sent.</p> <p>This issue began on June 30, 2017, when monitoring at least once every 35 calendar days for changes to the baseline configuration did not occur, and ended on August 15, 2017, when the entity completed its monitoring of the baseline configuration, for a total of 47 days.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to monitor, at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1) and document and investigate detected unauthorized changes, as required by CIP-010-2 R2 part 2.1.</p> <p>These BCAs utilize serial connections available only while physically present at the device. Additionally, the BCAs did not have ERC which removes the risk associated with compromise due to network connectivity. No harm is known to have occurred.</p> <p>The entity does not have any relevant previous violations of this or similar Standards and Requirements.</p>					
Mitigation			<p>To remediate and mitigate this issue, the entity:</p> <ol style="list-style-type: none"> completed baseline configuration reviews for the BCAs in scope; created a compliance report which is emailed to applicable personnel which identifies all manual baselines to be completed, a workflow list and an identification of primary and secondary personnel responsible for task completion; and created a Compliance Dashboard to track and identify the baseline configurations that have a monitoring task due. <p>WECC verified the entity's 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
WECC2018020047	CIP-010-2	R3; P3	[REDACTED]	[REDACTED]	2/7/2018	8/31/2018	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 July 19, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in noncompliance with CIP-010-2 R3.</p> <p>Specifically, the entity reported that while processing a Cyber Asset change in accordance with its change management procedures, it identified two new Cyber Assets that did not have a vulnerability assessment (VA) completed prior to adding them to the Electronic Security Perimeter network for the High Impact Bulk Electric System (BES) Cyber System (HIBCS). This instance included two video conferencing devices with no External Routable Connectivity (ERC) that were classified as Protected Cyber Assets (PCAs) associated with its HIBCS. These systems provide video conferencing capability between the primary Control Center and the backup Control Center for [REDACTED].</p> <p>After reviewing all relevant information, WECC determined the entity failed, prior to adding a new applicable Cyber Asset to a production environment, to perform an active VA of the new Cyber Asset, as required by CIP-010-2 R3 Part 3.3. Additionally, the entity failed to document the results of the VA conducted, as required by CIP-010-2 R3 Part 3.4, and or create an action plan to remediate or mitigate the vulnerabilities identified in the VA including the planned date of completing the action plan and the execution status of any remediation or mitigation action items, as required by CIP-010-2 R3 Part 3.4.</p> <p>The root cause of the issue was an outdated procedure which did not specifically identify the roles and responsibilities for the applicable staff who were required to complete the VA and document and mitigate identified results.</p> <p>This issue began on February 7, 2018 when it failed to perform and document the results of a VA for two PCAs, and ended on August 31, 2018, when it completed the VA and completed all required documentation, for a total of 206 days.</p>					
Risk Assessment			<p>WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed, prior to adding a new applicable Cyber Asset to a production environment, perform an active VA of the new Cyber Asset, as required by CIP-010-2 R3 Part 3.3. Additionally, the entity failed to document the results of the VA conducted, as required by CIP-010-2 R3 Part 3.4, and or create an action plan to remediate or mitigate the vulnerabilities identified in the VA including the planned date of completing the action plan and the execution status of any remediation or mitigation action items, as required by CIP-010-2 R3 Part 3.4.</p> <p>However, the PCAs did not have ERC which mitigated the risk associated with compromise due to network connectivity. No harm is known to have occurred.</p> <p>The entity does not have any relevant previous violations of this or similar Standards and Requirements.</p>					
Mitigation			<p>To remediate and mitigate this issue, the entity:</p> <ol style="list-style-type: none"> a. performed a vulnerability scan on the two PCAs; b. documented the results of the VA scan which included the identification, solution, and the timeframe, to address each vulnerability; c. updated its change control procedure to include: <ol style="list-style-type: none"> 1. the roles and responsibilities to identify applicable personnel responsible for conducting associated tasks; 2. detailed process steps for new device implementations; and d. trained applicable staff on the updated procedures. <p>WECC verified the entity's mitigating activities.</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
WECC2017018616	CIP-007-6	R2; P2.2	[REDACTED]	[REDACTED]	7/19/2017 (when [REDACTED] should have evaluated security patches for applicability)	9/18/2017 (when [REDACTED] completed its security patch evaluations)	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 9, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-007-6 R2. Specifically, [REDACTED] reported that on September 18, 2017, during a review of its "Evidence and Log Review" spreadsheet, it discovered that a new [REDACTED] application was not included on its Security Patch Monitoring Log for on-going maintenance and evaluation of applicable security patches, therefore the application had not been evaluated for applicable security patches at least once every 35 calendar days since its installation. The [REDACTED] application was installed on June 13, 2017 on [REDACTED] Cyber Assets [REDACTED] Medium Impact Bulk Electric System (BES) Cyber System (MIBCS) BES Cyber Assets (BCAs), [REDACTED] Physical Access Control Systems (PACS), and [REDACTED] Electronic Access Control or Monitoring Systems (EACMS) associated with the MIBCS, located at [REDACTED] primary and backup Control Centers), as part of an Energy Management System (EMS) upgrade project. [REDACTED] confirmed during its review that the patch source list used to document and identify all security patch sources included the [REDACTED] patch source location necessary to conduct the evaluations to determine applicable security patches; however, the System Administrator assigned to perform on-going patch maintenance to the [REDACTED] application had not attended the Security Patch Management Process training, which may have led to a misunderstanding of the expectation to create the Security Patch Monitoring Log to document the evaluation of security patches for the [REDACTED] application. On September 18, 2017, [REDACTED] completed an evaluation of security patches for the [REDACTED] Cyber Assets which it determined that no applicable security related patches were released [REDACTED] e two missed evaluation periods. Additionally, upon discovery, [REDACTED] reviewed its patch source lists and monitoring logs and determined that the [REDACTED] application was the only application missing from the log.</p> <p>After reviewing all relevant information, WECC determined that [REDACTED] failed to implement its process 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., for [REDACTED] Cyber Assets associated with the MIBCS located at its primary and backup Control Centers, as required by CIP-007-6 R2 Part 2.2.</p> <p>The root cause of the issue was a lack management follow-up to ensure compliance. Specifically, [REDACTED] provided training for the task assignment and the role and responsibilities of the Security Patch [REDACTED] Process, however the individual responsible for the on-going patch maintenance for the [REDACTED] application was not able to attend the training. Once the individual was available, Management did not ensure that they were aware of their responsibilities in regard to patch management.</p> <p>This noncompliance started on July 19, 2017, when [REDACTED] should have evaluated security patches for applicability, and ended on September 18, 2017, when [REDACTED] completed its security patch evaluations, for a total of 62 days.</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 implement its process 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., for [REDACTED] Cyber Assets associated with the MIBCS located at its primary and backup Control Centers as required by CIP-007-6 R2 Part 2.2. Such failure could result in out-of-date antivirus/malware protection. This could result in vulnerabilities with known exploits that a malicious actor could leverage to compromise the system. Additionally, with out-of-date antivirus/malware protection, a preventable virus could spread from one device to another resulting in loss of BES equipment, loss of generation or load, and loss of visibility to [REDACTED] transmission and generation stations. [REDACTED] owns [REDACTED] MW of generation and operates [REDACTED] MW of generation with [REDACTED] MW of generation within its [REDACTED] footprint; owns and operates [REDACTED] miles of [REDACTED] kV and [REDACTED] miles of [REDACTED] kV transmission lines; is the [REDACTED] and [REDACTED] for parts of [REDACTED] WECC Major Transfer Paths; and has [REDACTED] connectivity to four other entities; for which the [REDACTED] Cyber Assets are applicable to this issue. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as intermediate.</p> <p>[REDACTED] implemented week preventive and detective controls; however, it had implemented good compensating controls. Specifically, the [REDACTED] Cyber Assets were located within the Electronic Security Perimeter (ESP) which was controlled by firewalls, software restrictions, and physical access was restricted to only those personnel with authorized access. Additionally, no external media, file shares, email, file downloads, or browsing outside the ESP was allowed. 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] has no relevant compliance history for this noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) completed the security patch evaluations; 2) documented a new [REDACTED] Log to track and monitor the status of patches; 3) reviewed its patch source lists and monitoring logs to ensure that the [REDACTED] application was the only application missing from the log; and 4) developed a Patch Assessment Assignment and Notification procedure. This procedure ensures proper notification to, and acknowledgement from, personnel who are assigned duties as a System Administrator of their responsibility for performing routine security patch assessments and the review process. <p>WECC 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
WECC2017017877	CIP-004-6	R5	[REDACTED]	[REDACTED]	2/23/2017	3/22/2017	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, [REDACTED] submitted a Self-Report stating that, as a Balancing Authority, Distribution Provider, Generation Owner, Generation Operator, Transmission Owner and Transmission Operator, it was in noncompliance with CIP-004-6 R5.</p> <p>Specifically, [REDACTED] reported that on March 22, 2017, during its quarterly physical access review employment verification with its third-party contractor employment firm, [REDACTED] was informed that a janitor still on [REDACTED] list had been terminated from the employment firm on February 22, 2017. Further investigation revealed that the janitor had two last names on file with the contracting firm, and that the contracting firm's Human Resources incorrectly processed the contractor under both last names when sending the access request to [REDACTED] processed each of the last names as separate individuals per its documented procedures and issued two badges, one for each last name; one on December 2, 2016, with authorized unescorted physical access to the Physical Security Perimeter (PSP) protecting the High Impact Bulk Electric System (BES) Cyber Systems, and the other with non-CIP access (which was never picked up by the janitor). [REDACTED] received a notice of termination for the janitor on March 7, 2017 with the last name associated with the non-CIP access. Since the badge had never been picked up, [REDACTED] took no immediate action. However, because no notice was received for the last name associated with the CIP physical access, [REDACTED] did not know to complete the removal of access within 24 hours of the termination action, which was the notice later received from the employment firm on March 7, 2017. [REDACTED] completed the removal for both badges issued to the one janitor with two different last names when it deactivated the badges on March 22, 2017.</p> <p>After reviewing all relevant information, WECC determined that [REDACTED] failed to complete the removal within 24 hours of a termination action, as required by CIP-004-6 R5 Part 5.1, for one janitor with authorized unescorted physical access to HIBCS.</p> <p>The root cause of the issue was an incorrect processing of the contractor's identity by the human resources department of the employment firm.</p> <p>WECC determined that this issue began on February 23, 2017, when removal of unescorted physical access should have been completed, and ended March 22, 2017 when [REDACTED] deactivated the two security badges, for a total of 28 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 complete the removal of unescorted physical access within 24 hours of a termination action, as required by CIP-004-6 R5 Part 5.1, for one janitor. Such failure could allow an unauthorized individual to access the HIBCS which could potentially lead to misuse, disruption, destruction, misconfiguration and unauthorized control of Cyber Assets. [REDACTED] owns and/or operate [REDACTED] of BES generation, and [REDACTED] of generation in their [REDACTED] footprint. [REDACTED] transmission system consists of approximately [REDACTED] of transmission which includes [REDACTED], [REDACTED], and [REDACTED]. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as intermediate.</p> <p>However, [REDACTED] had implemented a strong preventive control. Specifically, [REDACTED] policy required that janitorial contractors with unescorted physical access to Physical Security Perimeters leave their security badges with the Physical Security team at the end of each shift. [REDACTED] confirmed it was in possession of both badges. 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] has no relevant compliance history for this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <ol style="list-style-type: none"> 1) deactivated the two physical access badges; 2) created a process to perform a check of identification cards for all contractors to confirm the full legal name is listed in the system; 3) updated the language for relevant contracts to now require contractors and subcontractors to immediately notify Corporate Physical Security within eight hours when a contractor is no longer employed with the contracting or subcontracting company. <p>WECC 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
WECC2018019303	CIP-002-5.1	R1	[REDACTED]	[REDACTED]	7/1/2016	2/22/2018	Self-Certification	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 28, 2018, [REDACTED] submitted a Self-Certification stating that as a [REDACTED], it was in noncompliance with CIP-002-5.1 R1.</p> <p>Specifically, on August 23, 2017, [REDACTED] executed a 15-month review of its CIP-002-5.1, R1 identification of facilities and Bulk Electric System (BES) Cyber Systems as required by CIP-002-5.1 R2. The Medium Impact BES Cyber Systems (MIBCS) identified in the 15-month review was the same identification initially made prior to the July 1, 2016 effective date of the CIP Version 5 Standards. On December 7, 2017, during a review of compliance, a concern came to the attention of the compliance group that criteria 2.8 was omitted from the original CIP-002-5.1 BES Cyber System categorization assessment. Upon verification of this omission, [REDACTED] rationale for omitting criteria 2.8 was that it was not applicable to a [REDACTED]. However, after further research, and conversations with WECC, it was determined the applicability of the criteria, in the context of the CIP-002-5.1 categorization assessment, should not have been based on registration; therefore, criteria 2.8 should have been part of the assessment.</p> <p>After reviewing all relevant information, WECC determined that [REDACTED] failed to appropriately implement its process that identified each of the MIBCS according to Attachment 1, Section 2, if any, at each asset, by omitting criteria 2.8 in its assessment, as required by CIP-002-5.1 R1.</p> <p>The root cause of the issue was a misunderstanding of the applicability of the criteria in Attachment 1, Section 2 of CIP-002-5.1 in the context of the CIP-002-5.1 categorization assessment process.</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 February 22, 2018, when a new review of the identifications in CIP-002-5.1 was performed which included criteria 2.8 of Attachment 1, for a total of 602 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 appropriately implement its process that identified each of the MIBCS according to Attachment 1, Section 2, if any, at each asset, by omitting criteria 2.8 in its assessment, as required by CIP-002-5.1 R1. Such failure could potentially result in miscategorizing a BES Cyber System which could lead to a failure to implement all applicable NERC CIP Standards; thereby exposing [REDACTED] to a multitude of physical and/or electronic attacks that could potentially affect one MIBCS with External Routable Connectivity, two Low Impact BES Cyber Systems, and one generation facility that generates [REDACTED] and was [REDACTED]. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as intermediate.</p> <p>However, [REDACTED] the new owner of [REDACTED] implemented good detective controls. Specifically, [REDACTED] was conducting a review of the identifications made in CIP-002-5.1 R1 which is how this issue was discovered. As further compensation, when the new assessment was performed, which included criteria 2.8, there was no change to the impact rating of the existing BES Cyber Systems from what was originally identified and no new BES Cyber Systems identified. Effectively, this issue was a documentation error and not a technical error. 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] has no relevant compliance history for this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, [REDACTED]</p> <p>1) updated its BES Cyber System Impact Rating process to include criteria 2.8; and 2) performed a new R1 Part 1.2 identification to include Attachment 1, Section 2, criteria 2.8.</p> <p>WECC verified completion of mitigating activities.</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
WECC2018019293	CIP-002-5.1	R2	[REDACTED]	[REDACTED]	10/1/2017	2/26/2018	Self-Certification	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 26, 2018, [REDACTED] submitted a Self-Certification stating that, as a [REDACTED], it was in noncompliance with CIP-002-5.1 R2.</p> <p>Specifically, [REDACTED] report that on February 26, 2018 while preparing its Self-Certification, it discovered that it had not performed the 15-calendar month review and approval of its CIP-002-5.1 R1 identifications.</p> <p>After reviewing all relevant information, WECC determined that [REDACTED] failed to review the identifications in R1 and its parts at least once every 15 calendar months, even if it had no identified items in R1, and have its CIP Senior Manager approve the identifications reviewed, as required by CIP-002-5.1 R1 Parts 2.1 and 2.2.</p> <p>The root cause of the issue was [REDACTED] not adequately distributing duties amongst its personnel. Specifically, a single person was responsible for ensuring the 15-calendar month review and approval required by CIP-002-5.1 R2 was performed which created a single point of failure in that when it came time to perform the review, the responsible person was out on medical leave.</p> <p>WECC determined that this issue began on October 1, 2017, the latest day the review and approval should have been completed, and ended on February 26, 2018, when [REDACTED] performed the review and approval, for a total of 149 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 review the identifications in R1 and its parts at least once every 15 calendar months, even if it had no identified items in R1, and have its CIP Senior Manager approve the identifications reviewed, as required by CIP-002-5.1 R1 Parts 2.1 and 2.2. Such failure could potentially result in a miscategorization of Bulk Electric System (BES) Cyber Systems which could lead to inadequate or non-existent protective measures of applicable CIP Standards. This could potentially result in a compromise or misuse of BES Cyber Systems affecting real-time operation of the BPS. CIP Senior Manager approval ensures proper oversight of the identification of the impact rating of BES Cyber Systems. [REDACTED] owns [REDACTED] transmission lines that were applicable to this issue. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as negligible.</p> <p>[REDACTED] had not implemented internal controls to detect or prevent this issue from occurring. However, [REDACTED] had no BES Cyber Systems and had a very small transmission footprint. The subsequent review did not change the identifications made in its initial review of CIP-002-5.1 R1. Based on this, WECC determined that there was a remote likelihood of causing negligible 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 a review of its R1 identifications and obtained CIP Senior Manager approval of that review; and 2) set up an outlook reminder, that is sent to the CIP Senior Manager as well as another person in the company to complete the CIP-002-5.1 R2 review and approval. <p>WECC verified completion of mitigating activities.</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
WECC2018019341	CIP-007-6	R5			7/19/2017	12/19/2017	Self-Certification	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 1, 2018, [REDACTED] submitted a Self-Certification stating that, as a [REDACTED] it was in noncompliance with CIP-007-6 R5.</p> <p>Specifically, [REDACTED] reported that on December 14, 2017, during its annual Cyber Vulnerability Assessment, it determined that one Protected Cyber Asset (PCA) associated with a Medium Impact Bulk Electric System (BES) Cyber Asset (MIBCS) had an administrator account password that had not been changed since April 18, 2016. A Subject Matter Expert (SME) was tasked with changing the passwords for the 15-calendar month password change requirement. The SME was given a checklist that identified all Cyber Assets where the passwords were to be changed, and once the passwords were changed, the SME was to mark the Cyber Asset on the checklist for which the password had been changed. While working through the list of Cyber Assets, the SME inadvertently marked a PCA as having the password changed when it had not been changed. The PCA was a PI Historian with no control capabilities that was used for Supervisory Control and Data Acquisition information on the energy flows and was not used for real-time decision making.</p> <p>After reviewing all relevant information, WECC determined that [REDACTED] failed to, where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes at least once every 15 calendar months to one PCA associated with a MIBCS, as required by CIP-007-6 R5 Part 5.6.</p> <p>The root cause of the issue was the accuracy or effectiveness of a change that was not verified or validated. Specifically, [REDACTED] did not conduct any validation or verification that the passwords were changed. If [REDACTED] had validated the accuracy of the work, the issue would have been identified prior to becoming a noncompliance issue.</p> <p>WECC determined that this issue began on July 19, 2017, when the administrator account password on one PCA should have been changed, and ended on December 19, 2017, when the password was changed, for a total of 154 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, where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes at least once every 15 calendar months for an administrator account on one PCA associated with a MIBCS, as required by CIP-007-6 R5 Part 5.6. Such failure increased the risk of the password being compromised by a brute force attack which could lead to a compromised account on a critical system, potentially providing full control (installation of software, exfiltration of data, remote control, manipulation of data, etc.) of the compromised system, and an anchor point for reconnaissance and spreading through the environment, which could have a severe negative affect on [REDACTED] connected BES Cyber Systems. [REDACTED] performs the [REDACTED] of generation for which it [REDACTED]; [REDACTED] transmission lines applicable to this issue. However, the PCA is a Pi Historian and compromising the account would not have allowed access to any other systems, nor provided the ability to control the BES. There was no way to alter the functionality of the Cyber Asset to enable BES control. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as minor.</p> <p>[REDACTED] implemented weak preventive and detective controls; however, it had implemented good compensating controls. Specifically, the PCA was located within an Electronic Security Perimeter (ESP), which was secured by a Physical Security Perimeter (PSP). The ESP was protected with a firewall which limited connectivity to known authorized users. The PCA had no control capabilities and was not used for real-time decision making. 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 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) changed the password on the PCA; 2) document the requirement to enforce technical controls on the new EMS, where feasible, for password policy for applicable assets in the System Security Management plan; and 3) enable technical controls to enforce password policy on the new EMS for Medium Impact CIP Cyber Assets as part of the EMS Update, scheduled for go-live in July 2018. <p>WECC has verified the completion of all mitigation activity.</p>					

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			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			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	██████████	██████████	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 ██████████ submitted a self-log to MRO stating that, as a ██████████, it was in noncompliance with CIP-007-6 R2. ██████████ Subsequently, during a Compliance Audit that occurred between ██████████, 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 ██████████ Cyber Assets (EACMS, ██████████ PCAs) that could not provide evidence of successful and unsuccessful logins. The noncompliance impacted devices that were associated with ██████████. The cause of the noncompliance was that ██████████ 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, ██████████ 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 ██████████. The cause of the noncompliance was that ██████████ 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 ██████████ the Cyber Assets were still logging for detected malicious code (P4.1.3) and ██████████. The second instance was minimal because MRO determined that all the Cyber Assets were reviewed within 20 days. Additionally, per ██████████ this represented a single incident out of 200 review periods. Finally, ██████████ states that a ██████████. No harm is known to have occurred.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, ██████████</p> <p>To mitigate the first instance of noncompliance, ██████████</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 ██████████ 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, ██████████</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>					

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	[REDACTED]	[REDACTED]	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, [REDACTED] submitted a self-log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5. Specifically, [REDACTED] failed to revoke a transferred employee's access by the end of the next calendar day as required by P5.2. [REDACTED] reports that on January 15, 2018 compliance personnel were notified that an employee no longer required access to a medium impact substation. [REDACTED] 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. [REDACTED] reports that the employee is still employed in good standing with [REDACTED]. 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, [REDACTED]</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. 					

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
MRO2018020698	CIP-009-6	R2	██████████	██████████	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, █████ submitted a self-log stating that, as a █████, it was in noncompliance with CIP-009-6 R2. Specifically, █████ failed to test its recovery plan at least once every 36 months as required by P2.3. █████ 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, █████ 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			This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. █████ promptly detected the noncompliance, which limited the duration of the noncompliance to less than 20 days. No harm is known to have occurred.					
Mitigation			<p>To mitigate this noncompliance, █████</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. 					

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
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			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
<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 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>					
<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. 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>					
<p>Mitigation</p>			<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"> 1) 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. 2) 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, [REDACTED] (the entity) submitted a Self-Report stating that, as [REDACTED] and [REDACTED], 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			To mitigate this noncompliance, [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
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; 2) applied the security patch to one Cyber Asset and removed the affected software from the second Cyber Asset; 3) contacted the vendor to confirm patches were no longer released. and designated the applicable patch source as inactive; 4) revised its deadline tracking system to send notifications to a group distribution list instead of a single individual; 5) modified the dashboard in the risk and compliance tool to identify all patching statuses; 6) created new control reports to monitor patching deadlines, monitor all active sources, and alert personnel of upcoming patch deadlines; 7) monitored and analyzed the results of the control reports. No additional changes to the control reports were identified; and 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	[REDACTED]	[REDACTED]	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
<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 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>					
<p>Risk Assessment</p>			<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>					
<p>Mitigation</p>			<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	[REDACTED]	[REDACTED]	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
<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 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>					
<p>Risk Assessment</p>			<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>					
<p>Mitigation</p>			<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. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

Compliance Exception

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. 					

A-2 Public CIP - Compliance Exception Consolidated Spreadsheet

Compliance Exception

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. 					

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: a) devices with TFE; b) devices that should be remotely manageable; c) device Risk Profile; and</p> <p>2) Created a report with executive review information: 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.</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
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. 					

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
<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 [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>					
<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. 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>					
<p>Mitigation</p>			<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). 					

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]</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>					

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
<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 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>					
<p>Risk Assessment</p>			<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>					
<p>Mitigation</p>			<p>To mitigate this issue, the entity:</p> <p>1) removed the firewall connection between the [REDACTED] facility and the [REDACTED] substation.</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
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. 					

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. 					

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
<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 [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>					
<p>Risk Assessment</p>			<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>					
<p>Mitigation</p>			<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.			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
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 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>					
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. 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>					
Mitigation			<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	██████████	██████████	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 ██████████ ReliabilityFirst determined that ██████████ as a ██████████ and ██████████ was in violation of CIP-005-5 R1. ReliabilityFirst identified the violation during a Compliance Audit conducted from ██████████. 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 ██████████. 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. ██████████ 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] 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	[REDACTED]	[REDACTED]	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, [REDACTED] submitted a Self-Report to ReliabilityFirst stating that, as a [REDACTED] [REDACTED] and [REDACTED] 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, [REDACTED], 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 [REDACTED] discovered that the firmware version on an [REDACTED] Electronic Access Control or Monitoring systems (EACMS) located at the entity's [REDACTED] 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 [REDACTED] datacenter. Therefore, the [REDACTED] cyber asset was being scanned twice, while the [REDACTED] 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 [REDACTED] examined all similar cyber assets in [REDACTED] and found no other discrepancies.</p> <p>In the second instance, the recurring configuration monitoring task was not set up in [REDACTED] 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 [REDACTED] 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 [REDACTED] 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 ([REDACTED] 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 [REDACTED] cyber asset would have been detected by the other [REDACTED] cyber asset in the cluster, thus triggering an investigation and corrective actions. Regarding the second instance ([REDACTED]) 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 [REDACTED] cyber asset's record in [REDACTED] to reflect the correct IP address and enable the monitoring task for the firewall cyber assets in [REDACTED] 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 [REDACTED]t service is implemented via the entity's [REDACTED] 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	[REDACTED]	[REDACTED]	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, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], 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 [REDACTED] 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 [REDACTED]. Subsequently, the entity identified eight more BCAs classified as medium impact without ERC that had an older firmware version listed in [REDACTED], 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 [REDACTED]. 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 [REDACTED], 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 [REDACTED] 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 [REDACTED] 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 [REDACTED]; 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 [REDACTED], 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	██████████	██████████	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, ██████████, as a ██████████, submitted a Self-Report to ReliabilityFirst stating that it was in noncompliance with CIP-007-3a R5. On July 10, 2017, ██████████ determined that two previously unknown default accounts associated with ██████████ assets were not identified or inventoried. Because these default accounts were not identified or inventoried, the ██████████ 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 ██████████ 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 ██████████ application integrated into each of the ██████████ 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 ██████████ and ██████████ 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 ██████████ failed to identify the update.</p> <p>This noncompliance started on April 30, 2015, when the ██████████ activated the accounts and ended on November 16, 2017, when the ██████████ 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 ██████████ 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 ██████████ of the accounts. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the ██████████' 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 ██████████ 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 ██████████ to identify changes; 2) updated ██████████ to include ██████████ and ██████████ accounts for each area of responsibility: ██████████, ██████████ and ██████████ 3) compared Shared Accounts from ██████████ environments to the current ██████████. The ██████████ also verified the accounts are accounted for and are represented in a consistent manner. Updated Inventory as necessary. Provided resultant ██████████ report of all ██████████ Shared Accounts to ██████████ performer via email; ██████████ performer must acknowledge receipt of report; 4) updated ██████████ with the ██████████ Shared Accounts ██████████ and ██████████ Also updated the roles that will authorize access and administer these accounts for each area of responsibility: ██████████, ██████████ and ██████████ 5) compared consolidated list of Shared Accounts from ██████████ to the Current Shared Accounts in ██████████. The ██████████ 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
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 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>					
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 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>					
Mitigation			<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>					

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
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
<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 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>					
<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 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>					
<p>Mitigation</p>			<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, ██████ submitted a Self-Report stating that, as a ██████ and ██████ 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 ██████ 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 ██████ 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 ██████ 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] [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. 					

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
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
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 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>					
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 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			<p>To mitigate this noncompliance, the entity:</p> <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
<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-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>					
<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). 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>					
<p>Mitigation</p>			<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
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-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>					
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
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	██████████	██████████	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, ██████████ submitted a Self-Report stating that, as a ██████████ 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 ██████████ 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 ██████████ 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
<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 ██████████ ██████████ ██████████ 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>					
<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 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>					
<p>Mitigation</p>			<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
			<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>					

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	[REDACTED]	[REDACTED]	7/1/2016	2/16/2018	Self-Report	Completed
Mitigation			<p>To remediate and mitigate this issue, [REDACTED]</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 [REDACTED] 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.	████████████████████	████████	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, ██████ submitted a Self-Report stating that, as a ██████ and ██████, it was in noncompliance with CIP-004-6 R2. Specifically, ██████ 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 ██████ 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 ██████ 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 ██████ 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 ██████ 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. ██████ 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, ██████ 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 ██████ 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, ██████ 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. ██████ owns and/or operates ██████ of generating capacity with a peak load of ██████ 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, ██████ 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 ██████ compliance history in its designation of this remediated issue as a CE. ██████ prior compliance history with CIP-004-6 R4 includes NERC Violation IDs ██████ and ██████ WECC determined that ██████ 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 ██████ 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, ██████</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. 					

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
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. 					

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.					