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	MRO2017018870	Yes		Yes	Yes					Yes	Yes		Yes	Category 1: 3 years; Category 2 – 12: 2 years
2	MRO2018019235	Yes		Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 years
3	MRO2018020298			Yes	Yes					Yes				Category 2 – 12: 2 years
4	MRO2018020139	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
5	MRO2018020840			Yes	Yes								Yes	Category 2 – 12: 2 years
6	SPP2018019319			Yes	Yes								Yes	Category 2 – 12: 2 years
7	MRO2018020850			Yes	Yes									Category 2 – 12: 2 years
8	MRO2018020839			Yes	Yes									Category 2 – 12: 2 years
9	MRO2018020836	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
10	MRO2018020795	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
11	MRO2018020801			Yes	Yes									Category 2 – 12: 2 years
12	MRO2018020292			Yes	Yes									Category 2 – 12: 2 years
13	NPCC2017016902			Yes	Yes									Categories 3 – 4: 2 year
14	NPCC2017016905	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
15	NPCC2017017113		Yes	Yes	Yes									Category 2 – 12: 2 years
16	NPCC2017018778	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
17	NPCC2018018910		Yes	Yes	Yes				Yes					Category 2 – 12: 2 years
18	NPCC2018019288		Yes	Yes	Yes									Category 2 – 12: 2 years
19	NPCC2018019726		Yes	Yes	Yes									Category 2 – 12: 2 years
20	NPCC2018019894		Yes	Yes	Yes									Category 2 – 12: 2 years
21	NPCC2018020279		Yes	Yes	Yes				Yes					Category 2 – 12: 2 years
22	RFC2018020608	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
23	RFC2018020430	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
24	RFC2018020431	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
25	RFC2018020253	Yes		Yes	Yes			Yes	Yes					Category 1: 3 years; Category 2-12: 2 years
26	RFC2018019898	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
27	RFC2018019878	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2-12: 2 years
28	RFC2018020255	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	RFC2018020029	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
30	RFC2018020208	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
31	RFC2018019903	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
32	RFC2018020741	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
33	TRE2017017809	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
34	TRE2017018030	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
35	TRE2017016876	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
36	WECC2017017871	Yes		Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 year
37	WECC2017018751			Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 year
38	WECC2017017876			Yes	Yes				Yes				Yes	Category 1: 3 years; Category 2 – 12: 2 year
39	WECC2017018583			Yes	Yes						Yes		Yes	Category 2 – 12: 2 years
40	WECC2017017878	Yes		Yes	Yes				Yes				Yes	Category 1: 3 years; Category 2 – 12: 2 year
41	WECC2018020339	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
42	WECC2017017301	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
43	WECC2017017302	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
44	WECC2017017305	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
45	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
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.)	During a Compliance Audit conducted between [redacted], MRO determined that [redacted] The noncompliance occurred [redacted]. During the Compliance Audit, 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." The cause of the noncompliance was inadequate process for documenting the enabled ports and services for PACS controllers. 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.
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 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. 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.
Mitigation	To mitigate the noncompliance, [redacted]: 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. MRO verified the completion of the mitigating activities.

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.)	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]. 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]. [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. 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. 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. The cause of the noncompliance was [redacted] failure to follow its documented procedures regarding classification of certain substation equipment. 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.
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 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.
Mitigation	To mitigate this noncompliance, [redacted]: 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.)	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]. 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. 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. 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.
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 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.
Mitigation	To mitigate this noncompliance, [redacted]: To mitigate the first instance of noncompliance, [redacted]: 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. To mitigate the second instance of noncompliance, [redacted]: 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
MRO2018020139	CIP-007-6	R4	[redacted]	[redacted]	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 violation.)	On April 10, 2018, [redacted] submitted a self-log stating that, as a [redacted], it was in noncompliance with CIP-007-6 R4. [redacted] identified two instances of noncompliance in the self-log. In the first instance of noncompliance, [redacted] 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. [redacted] reports that this noncompliance impacted 35 Cyber Assets (all [redacted] 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 [redacted] changed the configuration to alert for all malicious code detection. In the second instance of noncompliance, [redacted] 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. [redacted] states that an extent of condition revealed the issue impacted 11 Cyber Assets. [redacted] 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. [redacted] 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 [redacted] deployed a secondary control to alert for the loss of logging. 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 re-configured to enable alerts.
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 first instance was minimal because per [redacted], the noncompliance was limited to a failure to alert for code that could be automatically resolved. The second instance was minimal because per [redacted], the noncompliance was limited to alerts on malicious code detection as the devices were still logging locally per P4.1 and [redacted] was still reviewing those logs per P4.4. Additionally, for both instances [redacted] reports that it reviewed logs and found no indications of any malicious code. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, [redacted]: To mitigate the first instance of noncompliance, [redacted]: 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. To mitigate the second instance of noncompliance, [redacted]: 1) re-enabled the log forwarder on the impacted devices; 2) configured the log server software to generate an alert [redacted]; 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
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.)			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. The cause of the noncompliance was weakness in implementing a new process for patching this specific server. 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.				
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 noncompliance only impacted a single BES Cyber Asset. No harm is known to have occurred. 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.				
Mitigation			To mitigate this noncompliance, [redacted]: 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.)	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. 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. 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.
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 [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. 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.
Mitigation	To mitigate this noncompliance, [redacted]: 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.)	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. The noncompliance was caused by [redacted] failing to follow its process to approve the cyber security policies. 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.
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. [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. [redacted] has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted]: 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.)	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. 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). 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.						
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. [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. [redacted] has no relevant history of noncompliance.							
Mitigation	To mitigate this noncompliance, [redacted]: 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.)	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]. [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]. The cause of the noncompliance is that [redacted] failed to implement adequate controls during its CIP v5 transition. This noncompliance started on July 1, 2016, when the standard became enforceable and ended on March 2, 2018, [redacted].
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. [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. BEPC has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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.)	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]. The cause of the noncompliance was a deficient process that did not have any controls related to staff misinterpreting a patch description. 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.
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 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.
Mitigation	To mitigate this noncompliance, [redacted]: 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.)	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). The cause of the noncompliance was that [redacted] failed to follow its process for granting access to BES Cyber System Information storage locations. The noncompliance began on March 2, 2018, when the access was granted, and ended on May 16, 2018, when the access was revoked.
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. [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. [redacted] has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted]: 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.)	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). 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. 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.
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 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. [redacted] has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted]: 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.)	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. 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. 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. 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. The root cause of this instance was failure to review PACS installation documentation to ensure that all required accounts have been inventoried. 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. 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. 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. 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.
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. 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. 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. 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. 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.

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		To mitigate this noncompliance, the entity: 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.)	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. 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. 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. 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. 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. 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. 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.
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. 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. [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. 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. 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	To mitigate this noncompliance, the entity: 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

To prevent recurrence:

Instance 1:

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.

Instance 2:

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.)	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. 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. Specifically, the entity failed to remove access to the entity's [redacted] application for one employee following a transfer date. 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.
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. 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. 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. 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	To mitigate this noncompliance, the entity: 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.)	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. 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. [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. 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.
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. 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. 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. 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	To mitigate this noncompliance, the entity: 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.)	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. 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. 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. 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.
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. 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. 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. 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	To mitigate this noncompliance, the entity: 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.)	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. 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. 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. The root cause of this noncompliance was failure to ensure that account review procedures were executed during the required timeframe.
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. 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. 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. 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	To mitigate this noncompliance, the entity: 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.)	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. 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. 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. The root cause of this noncompliance was failure to comply with documented IRA procedures.
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. 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. 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. 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	To mitigate this noncompliance, the entity: 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.)	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. 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. 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. 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.
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. 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. 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. 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. 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	To mitigate this noncompliance, the entity: 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.)	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. 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. 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. 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.
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 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. 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	To mitigate this noncompliance, the entity: 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.)	On October 22, 2018, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R2. 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. 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. 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. 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.						
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 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. 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.						
Mitigation	To mitigate this noncompliance, the entity: 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.)			On September 13, 2018, [redacted] submitted a Self-Report stating that, as a [redacted], they were in noncompliance with CIP-010-2 R1. [redacted] 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. 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. 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. 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. 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.				
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 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. 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.				
Mitigation			To mitigate this noncompliance, the entity: 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. 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
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.)			On September 13, 2018, the entity submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-010-2 R1. 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. 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. 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. 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. 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.				
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 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. 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.				
Mitigation			To mitigate this noncompliance, the entity: 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. 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
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.)

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].

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).

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.

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.

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.

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 (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.

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.

Mitigation

To mitigate this noncompliance, the entity:
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.

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.

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
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.)			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. 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. 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.					
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 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. ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.					
Mitigation			To mitigate this noncompliance, the entity: 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.)	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). 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). 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. 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]. In all three instances, the devices were not redeployed on the system and have no recorded evidence of disposal in accordance with the policy. 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. 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.
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 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. ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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.)			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. 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. 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.				
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 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. ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.				
Mitigation			To mitigate this noncompliance, the entity: 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]. 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
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.)			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 [redacted] diagram that contained Bulk Electric System (BES) Cyber System Information (BCSI), including [redacted] of BES Cyber Assets (BCAs) at Substation A. 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] 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. 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. 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.				
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 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. 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.				
Mitigation			To mitigate this noncompliance, the entity: 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. 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
RFC2018020208	CIP-010-2	R1	[redacted]	[redacted]	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.)			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. 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. 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. 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. 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.				
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 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. 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.				
Mitigation			To mitigate this noncompliance, the entity: 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. 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
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.)	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. Generally, the majority of entity interns, [redacted] are managed more collectively by HR with pre-established termination dates. [redacted] 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]. 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. 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.					
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 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. 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.					
Mitigation	To mitigate this noncompliance, the entity: 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.)			On November 21, 2018, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R4. 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. 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. 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. This noncompliance involves the management practices of external interdependencies and verification. External interdependencies management is involved because the entity coordinated with the [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. 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.				
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 (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. 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.				
Mitigation			To mitigate this noncompliance, the entity: 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. ReliabilityFirst has verified the completion of all mitigation activity.				

Texas Reliability Entity, Inc. (Texas RE) | 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
TRE2017017809	CIP-004-6	R4.1.2	[redacted]	[redacted]	08/03/2016	10/01/2016	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.)	On June 21, 2017, [redacted] submitted a Self-Report to Texas RE stating that, as a [redacted] and a [redacted], it was in noncompliance with CIP-004-6 R4. [redacted] submitted the Self-Report to Texas RE under an existing multi-region registered entity agreement. Specifically, [redacted] did not implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 - Access Management Program. In August 2016 two IT Contractors needed access to an [redacted] PSP. Contractor A was approved and granted access to the PSP on August 5, 2016. During this authorization, [redacted]. Contractor B was approved and granted access to the PSP on August 3, 2016. During this authorization, [redacted]. After reviewing authorization records for personnel with electronic access, unescorted physical access, or access to BCSI, it was determined that authorization records for the two contractors were missing. This noncompliance started on August 3, 2016, when Contractor B was granted access to the PSP and ended on October 1, 2016, when authorization records were documented for both contractors. The root cause for this non-compliance was a lack of procedural controls to ensure the existence of and long-term storage of authorization records prior to the granting of unescorted access to a PSP.
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 risk posed by this noncompliance is allowing unauthorized individuals access to BES Cyber Systems could lead to intentional or unintentional misoperation of BES Cyber Assets. The risk in this occurrence is mitigated by the following factors: 1) Both individuals have had access to [redacted] infrastructure for years prior to the implementation date of CIP-004-6 R4.1.2. 2) Both individuals had recent PRAs performed. 3) Both individuals had recent Cyber Security Awareness training. Texas RE considered [redacted] compliance history and determined there were no relevant instances of noncompliance. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, [redacted] 1) Revoked both contractors' access to the PSP. 2) Updated their access provisioning procedure to [redacted]. 3) [redacted].

Texas Reliability Entity, Inc. (Texas RE) | 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
TRE2017018030	CIP-007-6	R5; R5.2; R5.4	[redacted]	[redacted]	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.)	On July 27, 2017, the entity submitted a Self-Report stating that, as a [redacted] 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. A total of [redacted] active generic accounts were not properly documented pursuant to CIP-007-6 R5.2. 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. 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.
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 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. The risk of these issues is mitigated due to the following: 1) [redacted] the undocumented generic accounts cannot be used for interactive access. 2) [redacted] 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. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, the entity: 1) Documented the [redacted] 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).

Texas Reliability Entity, Inc. (Texas RE) | Compliance Exception | CIP

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

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)

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.

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.

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.

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.

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.

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.

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 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]

No harm is known to have occurred.

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.

Mitigation

To mitigate the first instance of noncompliance, [redacted]

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] ; 4) [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.	

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
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.)	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]. 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. 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. 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.
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. 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. 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. 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.
Mitigation	To mitigate this noncompliance, [redacted] 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.)			On December 5, 2017, the entity submitted a Self-Report stating, as a [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. 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. 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. 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.				
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. 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. 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.				
Mitigation			To mitigate this noncompliance, the entity: 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. WECC 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
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.)	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. 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. 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. 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. 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.
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. 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. 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. WECC 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
WECC2017018583	CIP-004-6	R4: P4.2	[redacted]	[redacted]	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.)	During a Compliance Audit conducted from [redacted] through [redacted], WECC determined that the entity, as a [redacted], 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. 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. 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. 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.
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. 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. 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. WECC 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
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.)	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. 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. 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. 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.
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. 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. 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]. [redacted]. No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. WECC 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
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.)	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. 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. 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. 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.
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. 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. WECC determined the entity did not have any relevant compliance history.
Mitigation	To mitigate this noncompliance, the entity: 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. 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
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.)

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.

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:

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
WECC2017017301	CIP-007-6	R2	[redacted]	[redacted]	7/1/2016	5/8/2017	Self-Report	Completed

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)

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)

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.

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.

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.

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.

Risk Assessment

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.

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.

Mitigation

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.

To remediate and mitigation CIP-007-6 R2 the entity has:

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.)

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.

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:

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	[redacted]	[redacted]	7/1/2016	3/2/2017	Self-Report	Completed

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)

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)

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.

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.

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.

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 .

Risk Assessment

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.

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.

Mitigation

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.

To remediate and mitigation CIP-007-6 R4 Part 4.1 the entity has:
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.

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
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.)

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.

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:

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
WECC2017017305	CIP-007-6	R5	[redacted]	[redacted]	7/1/2016	6/16/2017	Self-Report	Completed

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)

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)

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.

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.

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.

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 .

Risk Assessment	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. 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.
Mitigation	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. To remediate and mitigate CIP-007-6 R5 Parts 5.4 and 5.5 the entity has: 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. 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
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.)

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.

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:

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
WECC2017017294	CIP-010-2	R1	[redacted]	[redacted]	7/1/2016	5/11/2017	Self-Report	Completed

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)

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)

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.

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.

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.

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.

Risk Assessment

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.

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.

Mitigation

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.

To remediate and mitigate CIP-010-2 Parts 1.1 and 1.4 the entity has:
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.

WECC verified completion of mitigating activities.

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.)	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). 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. 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. 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. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the Entity: 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	[redacted]	[redacted]	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.)	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. 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. 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.
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 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. [redacted] does not have any relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted]: 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.)			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. 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. The noncompliance began on July 1, 2016 when the standard became enforceable, and ended on December 4, 2017 when the documented process was updated.					
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. [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.					
Mitigation			To mitigate this noncompliance, [redacted]: 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.)	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]. 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. 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. 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. 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.
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 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. [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.
Mitigation	To mitigate this noncompliance, [redacted]: To mitigate the first instance of noncompliance, [redacted]: 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
			To mitigate the first instance of noncompliance, [redacted] will by March 29, 2019: 1) complete the changes to implement the fix. The reason for the duration of the mitigating activities is due to the technical complexity of the fix. To mitigate the second instance of noncompliance, [redacted]: 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. To mitigate the third instance of noncompliance, [redacted]: 1) revoked the contractor's access; and 2) developed an action plan with the supervisor to follow for future revocation actions.					

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.)			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]. 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. The noncompliance was caused by [redacted] failing to follow its documented process regarding access revocation. 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.					
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. [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.					
Mitigation			To mitigate this noncompliance, [redacted]: 1) revoked the former employee's access; and 2) sent a letter to the manager on the importance of timely submitting revocation forms. Mitigation was limited to 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
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.)			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]. 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. 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. 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.					
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. [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.					
Mitigation			To mitigate this noncompliance, [redacted]: 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.)	During a Compliance Audit conducted between October 23, 2017 and October 26, 2017, MRO determined that [redacted] a [redacted], as a [redacted], was in noncompliance with CIP-007-6 R1. [redacted]) are [redacted]. The noncompliance occurred in the operating areas of [redacted]. 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." The cause of the noncompliance was inadequate process for documenting the enabled ports and services for PACS controllers. 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.
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 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 to remotely configure the controllers. 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. 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.
Mitigation	To mitigate the noncompliance, [redacted]: 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. MRO verified the completion of the mitigating activities.

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	[redacted]	[redacted]	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.)	On April 10, 2018, [redacted] submitted a self-log stating that, as a [redacted], it was in noncompliance with CIP-007-6 R4. [redacted] identified two instances of noncompliance in the self-log. In the first instance of noncompliance, [redacted] 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. [redacted] reports that this noncompliance impacted 35 Cyber Assets (all Windows 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 [redacted] changed the configuration to alert for all malicious code detection. In the second instance of noncompliance, [redacted] 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. [redacted] states that an extent of condition revealed the issue impacted 11 Cyber Assets. [redacted] 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. [redacted] 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 [redacted] deployed a secondary control to alert for the loss of logging. 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.
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 first instance was minimal because per [redacted] the noncompliance was limited to a failure to alert for code that could be automatically resolved. The second instance was minimal because per [redacted] the noncompliance was limited to alerts on malicious code detection as the devices were still logging locally per P4.1 and [redacted] was still reviewing those logs per P4.4. Additionally, for both instances [redacted] reports that it reviewed logs and found no indications of any malicious code. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, [redacted] To mitigate the first instance of noncompliance, [redacted] 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. To mitigate the second instance of noncompliance, [redacted] 1) re-enabled the log forwarder on the impacted devices; 2) configured the log server software to generate an alert if it does not receive a log from a Cyber Asset for four hours; 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.)	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. 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. 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. The root cause of this noncompliance was incomplete processing of the CIP Transfer QA process checklist.
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. 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. 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. 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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate the noncompliance, the entity: 1. Disabled the active directory Accounts at issue; 2. Coached, counselled, and retrained the IT individual on the procedure. Details to Prevent Recurrence: 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.)	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. 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. 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. 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.
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. 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. 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 No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1. Revoked access to 2 contractors 2. Provided training to 1 contractor To prevent recurrence 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.)	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. 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. 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.
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. 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. 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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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.)		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. 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. 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. The root cause of this noncompliance was a failure of the supervisor to contact the security control center to ensure timely access revocation.					
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. 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. 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. No harm is known to have occurred as a result of this noncompliance.					
Mitigation		To mitigate this noncompliance, the entity: 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.)	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. 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. 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. 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.) 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.				
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 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. No harm is known to have occurred. 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.				
Mitigation	To mitigate this noncompliance, the entity: 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. 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
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.)	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. 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. 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. 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.				
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 (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. 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.				
Mitigation	To mitigate this noncompliance, the entity: 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. 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
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.)			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. 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). 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. 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. 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.				
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 (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. 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.				
Mitigation			To mitigate this noncompliance, the entity: 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. 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
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.)			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. 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. 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.				
Risk Assessment			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. No harm is known to have occurred.				
Mitigation			To mitigate this issue, the entity: 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
RFC2019020947	CIP-004-6	R4; P4.1	[redacted]	[redacted]	12/15/2016	2/24/2017	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.)	On September 30, 2017, the entity submitted a self-log stating that, as a [redacted], it was in noncompliance with CIP-004-6 R4.1. A Corporate Security (CS) individual was researching an unrelated question on physical keys when he identified that a terminated individual was assigned three Physical Security Perimeter (PSP) keys. Upon further research, CS determined the Director - Facilities Operations collected two (2) key rings from the individual (a Facilities Operations Supervisor) upon termination on 12/15/2016. Facilities Operations determined one key ring contained keys to two (2) PSPs and the third key to a PSP was stored in the Facilities Operations Supervisor office. Director - Facilities Operations stored the key rings in his office and on occasion loaned the key ring with two PSP keys to Facilities Operations Supervisor A between 12/15/2016 and 1/30/2017 during which time the Facilities Operations Supervisor A did not have authorized access. Director - Facilities Operations promoted an existing employee to Facilities Operations Supervisor B and gave him the key rings with the two PSP keys prior to him having authorized access to the two PSPs. Facilities Operations Supervisor B was authorized to the two PSPs in his prior role. As part of the entity access control process, all NERC CIP Access was revoked from Facilities Operations Supervisor B on 1/30/2017 with the job change. Facilities Operations Supervisor B was reauthorized and provisioned access to the three PSPs on 2/24/2017. Additionally, authorization records for the physical key holders were not reviewed with the physical badge and electronic access quarterly authorization reviews. The causes of this noncompliance were: 1. The extended time period between the termination and the onboarding of the new supervisor; 2. Director – Facilities Operations was not aware the Facilities Operation Supervisor A did not have authorized access to 2 PSPs when he loaned him the key ring; and 3. The physical key review report did not contain individuals with an inactive status that were key holders. The root cause of this noncompliance was the insufficient key review report. This noncompliance started on December 15, 2016, when the entity Director-Facilities Operations improperly loaned the PSP keys out and ended on February 24, 2017 when Facilities Operations Supervisor B was reauthorized and provisioned access to the three PSPs and the keys.
Risk Assessment	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 was allowing unauthorized individuals to have access to the PSP keys and thus the PSPs. The risk posed by this noncompliance is minimized because Facilities Operations Supervisor A, who was loaned the 2 PSP keys, is a supervisor with authorized access to PSPs elsewhere in the company. Facilities Operations Supervisor B, who was transitioned the keys, was an emergency responder to the 2 PSPs prior to 1/30/2017 and had authorized badge access. Both employees had completed NERC CIP cyber security training and had a successful Personnel Risk Assessment at the time they had the physical keys. The employees were authorized for access to other NERC CIP PSPs and understood their obligations. The key use would have activated an alarm to alert Corporate Security of an entry. Corporate Security dispatches a responder to this type of alarm. The employees did not use the keys to access the PSP during the period of unauthorized access. No harm is known to have occurred.
Mitigation	To mitigate this issue, the entity: 1) entered [redacted] ticket to authorize access to PSPs for Facilities Operations Supervisor B; 2) updated the [redacted] work flow to include physical keys; 3) included physical keys in the verification of authorization access records; 4) installed key lock boxes at PSPs without physical security officers and Corporate Security placed the PSP keys in the lock boxes with access controlled by Corporate Security; 5) retrieved all physical keys to PSPs from assigned individuals and no longer issues keys to individuals external to CS. Keys will either be in a lock box or the PSPs will have 24x7 physical security officers that will maintain keys for emergency use; and 6) reviewed and updated, as appropriate, physical security procedure on key 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
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.)	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. Entity IT Security Administration researched [redacted] tickets for any other late revocations due to the code error and identified the following: • 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. 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. 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.				
Risk Assessment	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. No harm is known to have occurred.							
Mitigation	To mitigate this issue, the entity: 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.)	On August 2, 2018, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-004-3a R3. 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. 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. 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: 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. 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. 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] 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] That process failure is a root cause of this noncompliance. 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.
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 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 contactors, 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. 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.
Mitigation	To mitigate this noncompliance, 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
RFC2018020204	CIP-004-3a	R3	[redacted]	[redacted]	10/13/2013	8/1/2018	Self-Report	Completed
			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; 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; 3) obtained updated PRA records and restored access through a documented request and authorization processes, where necessary; 4) evaluated the process for archiving compliance artifacts related to PRAs and developed a plan to improve the process; and 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. 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
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.)	On July 16, 2018, the entity submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-006-6 R1. 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.) 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.) 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity will complete the following mitigation activities by June 3, 2019: 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. 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.

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.)			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]. 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. 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.				
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 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. 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.				
Mitigation			To mitigate this noncompliance, the entity: 1) suspended escorting privileges for the custodial contractor escort; and 2) provided verbal coaching for the custodial contractor escort. 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
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.)	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 [redacted] 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. 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] Although the device was a development device, it was still classified as a BCA [redacted] for systems inside the Electronic Security Perimeter (ESP). 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. 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.						
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 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. 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.						
Mitigation	To mitigate this noncompliance, the entity: 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] The entity communicated job aid update to change management personnel required to use the job aid in performing their duties. 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
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.)	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] 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. 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] Essentially, the document management system crisscrossed the drawings and sent them to the wrong vault. 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. 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.
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 (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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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.)			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. 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. This noncompliance started on July 1, 2016, when the entity should have [redacted] and ended on September 13, 2017, when the entity [redacted]				
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 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. 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.				
Mitigation			To mitigate this noncompliance, the entity: 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. 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
RFC2017018344	CIP-010-2	R1	[redacted]	[redacted]	1/11/2017	11/8/2017	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.)

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.

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].

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.

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.

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.

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.

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.

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.

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].

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 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

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
			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. 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.					
Mitigation			To mitigate this noncompliance, the entity: 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. 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
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.)			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). 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. 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. 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. 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.				
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 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] No harm is known to have occurred. 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.				
Mitigation			To mitigate this noncompliance, the entity: 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. 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
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.)

On May 24, 2018, the entity submitted two Self-Reports stating that, as a [redacted], it was in noncompliance with CIP-010-2 R4.

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.

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.

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.

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.

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).

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.

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.

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.

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 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.

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.

No harm is known to have 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
RFC2018019811	CIP-010-2	R4	[redacted]	[redacted]	1/24/2018	3/8/2018	Self-Report	Completed
			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.					
Mitigation			To mitigate this noncompliance, the entity: For the first instance: 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. For the second instance: 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. 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
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.)	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]. 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. 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]					
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 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. 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.					
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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. 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. 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. 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.
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 (BPS). 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. No harm is known to have occurred. Regional Entity determined that the entity's compliance history should not serve as a basis for applying a penalty.
Mitigation	To mitigate this noncompliance, the entity: 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.)	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. 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. 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.
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 (BPS). 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. Entity does not have a relevant compliance history. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, the entity: 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	[redacted]	[redacted]	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.)	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. 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. 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. The root cause of the first issue was ambiguous and incomplete instructions while the root cause of the second issue was human performance.
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 (BPS). 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. No harm is known to have occurred. Regional Entity determined that the entity does not have a relevant compliance history.
Mitigation	To mitigate this noncompliance, the entity: Issue 1: 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. Issue 2: 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.)	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. 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. 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.
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 (BPS). 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. No harm is known to have occurred. Regional Entity determined that the entity did not have a relevant compliance history.
Mitigation	To mitigate this noncompliance, the entity: 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	[redacted]	[redacted]	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.)	On December 22, 2017, [redacted] (the entity) self-reported that as a [redacted]), it had a possible instance of noncompliance for CIP-010-2, R2.1. 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. 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. 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. There were no baseline configuration changes to the asset between March 28, 2017 and June 5, 2017. 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.						
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 (BPS). 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. No harm is known to have occurred. The entity has no relevant compliance history.						
Mitigation	To mitigate this noncompliance, the entity: 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.)	On January 24, 2018, [redacted] (the entity) self-reported that as a [redacted] it was in noncompliance with CIP-010-2 R1.2. 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. This noncompliance duration was 1 day. 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.
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 (BPS). 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. The entity does not have a relevant compliance history. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, the entity: 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.)	On December 22, 2017, [redacted] (the entity) as a [redacted]) self-reported two instances of noncompliance with CIP-010-2, R1.5. 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. 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. 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). 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.
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 (BPS). 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. 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. No harm is known to have occurred. Entity does not have a relevant compliance history.
Mitigation	To mitigate this noncompliance, the entity: Issue 1: 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. Issue 2: 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.)	On June 25, 2018, [redacted] (the entity) as a [redacted] self-reported a noncompliance with CIP-010-2 R1.1. 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. The root cause of this issue was ineffective verification and validation practices.						
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 (BPS). 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. Entity ran a full IP script to verify address on all CIP assets and did not identify any other discrepancies with CIP Assets. No harm is known to have occurred. Entity does not have a relevant compliance history.							
Mitigation	To mitigate this noncompliance, the entity: 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.							

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
WECC2018019139	CIP-004-6	R5	[redacted]	[redacted]	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.)	During a Compliance Audit [redacted] WECC determined the entity, as a [redacted] had a potential noncompliance with CIP-004-6 R5 Parts 5.1 and 5.2. 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. 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. 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. 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.
Risk Assessment	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. 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. The entity has no compliance history for this Standard and Requirement.
Mitigation	To remediate and mitigate this issue, the entity has: a. completed physical access revocations for the contractors and employee in scope; b. 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; c. 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 d. 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. 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
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.)	During a Compliance Audit [redacted], WECC determined the entity, as a [redacted], had a potential noncompliance with CIP-005-5 R1 Part 1.3. 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. 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. 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. 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.
Risk Assessment	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. 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. The entity has no compliance history for this Standard and Requirement.
Mitigation	To remediate and mitigate this issue, the entity has: 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: 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. WECC 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
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.)	On January 10, 2019, the entity submitted a Self-Report stating, as a [redacted] it was in noncompliance with CIP-006-6 R1. 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. 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. 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. 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.
Risk Assessment	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. 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. 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.
Mitigation	To remediate and mitigate this issue, the entity has: 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. WECC verified the entity's mitigating activities.

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.)	On February 10, 2018, the entity submitted a Self-Report stating, as a [redacted] it was in noncompliance with CIP-006-6 R2. 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. 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. 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. 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.
Risk Assessment	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. 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. 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.
Mitigation	To remediate and mitigate this issue, the entity: 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. WECC verified the entity's mitigating activities.

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.)	On January 19, 2018, the entity submitted a Self-Report stating, as a [redacted] it was in noncompliance with CIP-007-6 R2. 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. 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. 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. 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.						
Risk Assessment	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. 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. The entity does not have any relevant previous violations of this or similar Standards and Requirements.						
Mitigation	To remediate and mitigate this issue, the entity: 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. WECC verified the entity's mitigating activities.						

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	[redacted]	[redacted]	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.)	On Jun 20, 2018, the entity submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-007-6 R2. 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. 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. 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. 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.						
Risk Assessment	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. 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. The entity does not have any relevant previous violations of this or similar Standards and Requirements.						
Mitigation	To remediate and mitigate this issue, the entity: a. deployed the software security patch to the two EACMS; b. 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; c. 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 d. sent an email to all personnel notifying them of the procedure was updated. WECC verified the entity's mitigating activities.						

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.)	On August 16, 2018, the entity submitted a Self-Report stating, as a [redacted] it was in noncompliance with CIP-010-2 R1. 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. 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. 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. 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.						
Risk Assessment	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. 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. The entity does not have any relevant previous violations of this or similar Standards and Requirements.						
Mitigation	To remediate and mitigate this issue, the entity: 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. WECC verified the entity's mitigating activities.						

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	[redacted]	[redacted]	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.)	On December 29, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in noncompliance with CIP-010-2 R2. 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. 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. 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. 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.
Risk Assessment	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. 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. The entity does not have any relevant previous violations of this or similar Standards and Requirements.
Mitigation	To remediate and mitigate this issue, the entity: a. completed baseline configuration reviews for the BCAs in scope; b. 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 c. created a Compliance Dashboard to track and identify the baseline configurations that have a monitoring task due. WECC verified the entity's mitigating activities.

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.)	On July 19, 2018, the entity submitted a Self-Report stating, as a [redacted] it was in noncompliance with CIP-010-2 R3. 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] 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. 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. 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.
Risk Assessment	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. 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. The entity does not have any relevant previous violations of this or similar Standards and Requirements.
Mitigation	To remediate and mitigate this issue, the entity: 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: 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. WECC verified the entity's mitigating activities.

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
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

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.)

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.

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.

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 managem

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.

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 (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.

[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.

WECC determined that [redacted] has no relevant compliance history for this noncompliance.

Mitigation

To mitigate this noncompliance, [redacted]

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.

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
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.)	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. 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. 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. The root cause of the issue was an incorrect processing of the contractor's identity by the human resources department of the employment firm. 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.
Risk Assessment	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. 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. WECC determined that [redacted] has no relevant compliance history for this noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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. 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
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.)	On February 28, 2018, [redacted] submitted a Self-Certification stating that as a [redacted]), it was in noncompliance with CIP-002-5.1 R1. 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. 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. 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. 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.
Risk Assessment	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. 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. WECC determined that [redacted] has no relevant compliance history for this noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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. 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
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.)	On February 26, 2018, [redacted] submitted a Self-Certification stating that, as a [redacted], it was in noncompliance with CIP-002-5.1 R2. 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. 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. 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. 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.
Risk Assessment	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. [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. WECC determined that [redacted] has no relevant compliance history for this noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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. WECC verified completion of mitigating activities.

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
WECC2018019341	CIP-007-6	R5	[redacted]	[redacted]	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.)	On March 1, 2018, [redacted] submitted a Self-Certification stating that, as a [redacted] it was in noncompliance with CIP-007-6 R5. 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. 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. 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. 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.
Risk Assessment	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. [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. WECC determined that [redacted] has no relevant compliance history for this noncompliance."
Mitigation	To mitigate this noncompliance, [redacted] 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. WECC has verified the completion of all mitigation activity.

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.	[redacted] ("the Entity")	[redacted]	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.)	On January 18, 2019, the Entity submitted a Self-Report stating that, [redacted], 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. 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. 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. 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. [redacted]. The script performed as designed and upgraded the firmware of all iLOs in that corporate subnet, including NERC iLO device. Therefore, this device was upgraded without the prior authorization and documentation that is required for applicable devices. An extent of condition review was performed by the Entity and revealed no additional occurrences. 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.
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 (BPS). 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. 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. 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.
Mitigation	To mitigate this noncompliance, the Entity: 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.

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
MRO2017016816	CIP-004-6	R5	[redacted]	[redacted]	08/01/2016	10/14/2016	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.)	During a Compliance Audit conducted from [redacted] MRO determined that [redacted], was in noncompliance with CIP-004-6 R5. [redacted] 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. 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). 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, [redacted]: 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.)			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. 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. 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.					
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 [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.					
Mitigation			To mitigate this noncompliance, [redacted]: 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	[redacted]	[redacted]	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.)	On July 10, 2018, [redacted], submitted a self-log stating that it was in noncompliance with CIP-007-6 R5. [redacted]. The self-log identified two instances of noncompliance. The noncompliance occurred in [redacted]. In the first instance of noncompliance, [redacted] 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 [redacted] 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. In the second instance of noncompliance, [redacted] 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; [redacted] 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. 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.
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 risk associated with the first instance is minimal because per [redacted], 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, [redacted] 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 [redacted] the device [redacted]. Additionally, [redacted] 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.
Mitigation	To mitigate this noncompliance, [redacted]: To mitigate the first instance, [redacted]: 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. To mitigate the second instance, [redacted]: 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.)	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]. [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. 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. The noncompliance began on October 25, 2017 when the construction project was completed, and ended on July 17, 2018 when the opening was closed.
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 [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.
Mitigation	To mitigate this noncompliance, [redacted]: 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.)	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]. [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. The cause of the noncompliance was that [redacted] did not follow its documented process to update the device inventory during deployment. The noncompliance began on May 3, 2018, 36 days after the last evaluation, and ended on June 14, 2018, when the patches were assessed.
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 [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.
Mitigation	To mitigate this noncompliance, [redacted]: 1) assessed the patches and applied the applicable patches; 2) added the BES Cyber Assets to the device inventory; 3) sent an email to all CIP SMEs reinforcing the two-step process for replacement of an existing device; and 4) updated the process to replace/retire Cyber Assets.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020833	CIP-010-2	R1	[redacted]	[redacted]	12/14/17	1/18/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			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. The cause of the noncompliance was that the task became stalled in the Change Management Process. 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.					
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 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. [redacted] does not have any relevant history of noncompliance.					
Mitigation			To mitigate this noncompliance, [redacted] 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.)	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. 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. 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.					
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 [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. 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.					
Mitigation	To mitigate this noncompliance, [redacted] 1) changed the passwords; 2) provided reinforcement training to the applicable SME; 3) had the team responsible for managing passwords implement a peer-review process as part of the annual password change campaign; and 4) had the compliance and quality control teams perform quality check reviews as part of the annual password change campaign.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019581	CIP-007-6	R4	[redacted]	[redacted]	07/01/2016	01/22/2018	Self-Log	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	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. 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. 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.
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. [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.
Mitigation	To mitigate this noncompliance, [redacted] 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.)	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. 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. 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. 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. 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. The cause of the noncompliance was that [redacted] did not follow its process to identify patch source or install patches after evaluation. 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.
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 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.
Mitigation	To mitigate this noncompliance, [redacted]: 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.

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
MRO2017017597	CIP-007-6	R4	[redacted]	[redacted]	2/22/2017	3/9/2018	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.)

On [redacted] submitted a self-log to MRO stating that, as a [redacted], it was in noncompliance with CIP-007-6 R2. [redacted] Subsequently, during a Compliance Audit that occurred between [redacted], MRO determined that there were two additional instances of noncompliance with CIP-007-6 R4. MRO later determined that the description in the self-log did not constitute noncompliance.

For the first instance of noncompliance, during the Compliance Audit, two of ten sampled Cyber Assets (PCAs) were unable to provide evidence (logs) of successful and unsuccessful logins as required by P4.1. A post-audit extent of conditions analysis discovered an additional [redacted] Cyber Assets [redacted] EACMS, [redacted] PCAs) that could not provide evidence of successful and unsuccessful logins. The noncompliance impacted devices that were associated with [redacted]. The cause of the noncompliance was that [redacted] failed to follow its documented process related to configuring logging. The noncompliance began on February 22, 2017 when an error was made during the Active Directory reconfiguration, and ended on March 9, 2018 when it confirmed the authentication events were being logged.

For the second instance of noncompliance, during the Compliance Audit, [redacted] of 28 sampled Cyber Assets were unable to provide evidence that a sample of logs were reviewed at least every 15 days as required by P4.4. MRO determined that the review of logs were all missed for all Cyber Assets within the same period of time. The noncompliance impacted devices that were associated within the [redacted]. The cause of the noncompliance was that [redacted] failed to assign personnel to handle this review during the planned absence of applicable staff. The noncompliance began on March 19, 2017 when the logs of the Cyber Assets were not reviewed at least every 15 days, and ended on March 24, 2017 when a sample of logs were reviewed.

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.

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 first instance of noncompliance was minimal because per [redacted] the Cyber Assets were still logging for detected malicious code (P4.1.3) and [redacted] The second instance was minimal because MRO determined that all the Cyber Assets were reviewed within 20 days. Additionally, per [redacted] this represented a single incident out of 200 review periods. Finally, [redacted] states that a [redacted]. No harm is known to have occurred.

Mitigation

To mitigate this noncompliance, [redacted]

To mitigate the first instance of noncompliance, [redacted]
1) conducted an extent of conditions analysis;
2) resolved the Active Directory configuration error to enable logging on the [redacted] Cyber Assets;
3) reviewed procedures for changing and testing group policy changes; and
4) emphasized the importance of security monitoring to the relevant team.
To mitigate the second instance of noncompliance, [redacted]
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.)			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. 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. 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.					
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 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.					
Mitigation			To mitigate the noncompliance, [redacted]: 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. The mitigating activities [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
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.)			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] 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. 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. 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.				
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. [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.					
Mitigation			To mitigate the noncompliance, [redacted]: 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.					

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
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.)	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]. 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. 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. 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.
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. [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.
Mitigation	To mitigate this noncompliance, [redacted] 1) updated the Cyber Assets' baselines; and 2) realigned the process to ensure that proper communications take place.

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
MRO2018020537	CIP-004-6	R5	[redacted]	[redacted]	04/12/2018	08/16/2018	Self-Log	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)

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.

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] 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.

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.

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.

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.

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 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.

The second issue was minimal risk because pe[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.

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.

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			To mitigate this noncompliance, [redacted]: To mitigate the first issue of noncompliance, [redacted]: 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. To mitigate the second issue of noncompliance, [redacted]: 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]. To mitigate the third issue of noncompliance, [redacted]: 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.)	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]. 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. The noncompliance was caused by incorrect one-line drawings that did not accurately identify the joint ownership of the Facility 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.
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 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.
Mitigation	To mitigate this noncompliance, [redacted]: 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. Mitigation was limited to 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
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.)	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]. [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. The cause of the noncompliance was that the contractor with authorized access failed to follow [redacted] documented process regarding continuous escort. 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.
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. [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.
Mitigation	To mitigate the noncompliance, [redacted]: 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. The mitigating activities [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
MRO2018020513	CIP-004-6	R3	[redacted]	[redacted]	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.)	On October 5, 2018, [redacted] submitted a self-log stating that it was in noncompliance with CIP-004-6 R3. Specifically, [redacted] failed to ensure that an individual with authorized unescorted physical access had a personnel risk assessment completed (PRA) within the last seven years. Per [redacted], the PRA expired and [redacted] discovered the noncompliance through a bi-weekly access report review. The cause of the noncompliance was that [redacted] did not follow its process to renew existing PRAs. The noncompliance began on August 2, 2018, when the individual's PRA expired, and ended on August 3, 2018, when the access was disabled.
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. [redacted] states the employee did not have electronic access to a BES Cyber System. Additionally, [redacted] stated that the employee did not access a PSP during the period of noncompliance. Finally, [redacted] reports that the employee is in good standing and that [redacted] re-granted the access after a successful PRA update. No harm is known to have occurred. While the mitigation is ongoing, [redacted] will reduce the risk by continuing to utilize the access report review, a detective control that detected this instance of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted]: 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. To mitigate this noncompliance, [redacted] will complete the following mitigation activity by April 1, 2019. 1) create an additional email notification outside of the bi-weekly report that will identify upcoming PRAs that are close to expiration. The reason for the duration of the mitigating activities is due to personnel changes in the group responsible for implementing the activities.

Midwest Reliability Organization (MRO) | Compliance Exception | CIP

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020147	CIP-004-6	R5	[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.)	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. 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. 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.
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. [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.
Mitigation	To mitigate this noncompliance, [redacted] 1) revoked the employee's access; and 2) implemented a compliance software tool workflow to codify its process for granting/changing access.

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
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.)	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. The noncompliance was caused by a lack of detail in the process for updating passwords. 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.
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. [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.
Mitigation	To mitigate this noncompliance, [redacted] 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	[redacted]	[redacted]	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.)	On October 10, 2018, [redacted] submitted a self-log stating that, as a [redacted], it was in noncompliance with CIP-004-6 R4. [redacted] states that during the cyber vulnerability assessment it identified that a user group had unauthorized local login access to CIP workstations. The user group pre-dated the CIP workstations and inherited local login access when the workstations were added to the domain. The cause of the noncompliance was [redacted] 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. 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.
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. [redacted] 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. [redacted] also states that all 13 users in the group had valid and up to date personnel risk assessments (PRA) and CIP training. Further, [redacted] 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.
Mitigation	To mitigate this noncompliance, [redacted] 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	[redacted]	[redacted]	7/1/2018	7/18/2018	self-log	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On October 10, 2018, [redacted] submitted a self-log stating that, as a [redacted], it was in noncompliance with CIP-009-6 R2. Specifically, [redacted] failed to test its recovery plan at least once every 36 months as required by P2.3. [redacted] states that it discovered the noncompliance on July 2, 2018 during an annual internal standard review. The cause of the noncompliance was a failure to follow its process; the process was not followed due to a schedule setting error, [redacted] entered the process reminders for 2019 instead of 2018. 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.
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. [redacted] promptly detected the noncompliance, which limited the duration of the noncompliance to less than 20 days. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, [redacted] 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	[redacted]	[redacted]	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.)	On November 17, 2017, [redacted] submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-004-6 R4. Specifically, [redacted] 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. 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. 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.
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. [redacted] states that when the late review was performed, all required authorization records were found to be correct. No harm is known to have occurred. MRO considered [redacted] relevant compliance history. [redacted] CIP-004-6 R4 compliance history includes noncompliance with CIP-004-1 R4 [redacted] 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 [redacted] 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.
Mitigation	To mitigate this noncompliance, [redacted] 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 [redacted] 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.)	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. The cause of the noncompliance is that [redacted] did not understand its responsibilities under the standard. 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.
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. [redacted] jointly owns a single BES substation and has no supervisory control over any BES Cyber Systems. No harm is known to have occurred. [redacted] has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted]: 1) drafted the necessary procedures; and 2) provided training on the procedures so that it could implement its cyber security plans. MRO verified completion of the mitigation.

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.)	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. The cause of the noncompliance is that [redacted] did not understand its responsibilities under the standard. 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.					
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. [redacted] jointly owns a single BES substation and has no supervisory control over any BES Cyber Systems. No harm is known to have occurred. [redacted] has no relevant history of noncompliance.							
Mitigation	To mitigate this noncompliance, [redacted]: 1) created the cyber security policies required by P1.2; and 2) had it CIP Senior Manager approve the policies. MRO verified the completion of the mitigation.							

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020802	CIP-010-2	R1	[redacted]	[redacted]	3/27/2017	9/27/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	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. The noncompliance was caused by a deficiency in [redacted] process of evaluating and identifying open ports during commissioning. 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.						
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 [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.							
Mitigation	To mitigate this noncompliance, [redacted] 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.							

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
SPP2018019315	CIP-004-6	R4	[redacted]	[redacted]	7/31/2017	2/2/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	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. 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. 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. 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.
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. 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. [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.
Mitigation	To mitigate this noncompliance, [redacted] 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. MRO verified the completion of the mitigating activities.

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.)			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] 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. The cause of the noncompliance was a lack of clarity in the process, which led to confusion on the part of the SME. 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.					
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 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.					
Mitigation			To mitigate this noncompliance, [redacted] 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.					

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
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.)	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. 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. 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.
Risk Assessment	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. [redacted] has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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.

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
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.)	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). [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). The cause of the noncompliance is that [redacted] failed to follow its documented processes. 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.
Risk Assessment	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.
Mitigation	To mitigate this noncompliance, [redacted] 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.

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
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.)	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. 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. 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.
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. 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.
Mitigation	To mitigate this noncompliance, [redacted] 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.)	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. 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. 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. 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). 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. 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. 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. The root cause of this noncompliance was the failure of two of the individuals to abide by the entity's physical security policy.
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. 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. 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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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.)			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. 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. The root cause of this noncompliance was a misclassification of the EACMS. The devices were originally classified as an information repository.					
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. 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. 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. 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.					
Mitigation			To mitigate this noncompliance, the entity: 1. Performed a review of authorization records for individuals with active electronic access or unescorted physical access to the EACMS in scope. To prevent future occurrences, the entity: 1. Performed a review of all High Impact BES Cyber Assets and their certification status to ensure no other discrepancies existed. 2. 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.)	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. 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. 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. The root cause of this noncompliance was lack of a control to require completion of the training specified in CIP-004-6 R2.1.
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. 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. 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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1. Addressed the non-compliance with training frequency for the twenty-one (21) identified employees: 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 To prevent recurrence, the entity: 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.)	On [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. 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. 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.
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. 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. The entity reduced the risk of an attacker gaining unauthorized access to the devices and brute force password attacks going unnoticed. [redacted] No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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.)			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. 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. 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.				
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. 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. 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] 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. No harm is known to have occurred as a result of this noncompliance. NPCC considered the entity's compliance history and determined there were no relevant underlying causes.				
Mitigation			To mitigate this noncompliance, the entity: 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 To prevent recurrence, the entity: 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.)	On July 25, 2018, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R2. 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. 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. 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. 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.
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 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. No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity will complete the following mitigation activities by April 30, 2019: 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. Prior to completion of the Mitigation Plan, entity SMEs have implemented measures to verify that all intended patches were installed and deployed as expected. The entity needs additional time to be able to retrain all 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
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.)	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. 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. 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. 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. 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.
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. 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. Regional Entity determined that the entity's compliance history should not serve as a basis for applying a penalty.
Mitigation	To mitigate this noncompliance, the entity: 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	[redacted]	[redacted]	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.)	On June 25, 2018, [redacted] (the entity) submitted a Self-Report stating that, as a [redacted] and [redacted], it was in noncompliance with CIP-004-6, R5.3. 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. 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.
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 (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. No harm is known to have occurred. Regional Entity determined that the entity's compliance history should not serve as a basis for applying a penalty.
Mitigation	To mitigate this noncompliance, the entity: 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	[redacted]	[redacted]	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.)	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. 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. The noncompliance duration was less than 8 hours. 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. The noncompliance duration was less than 30 minutes.
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 (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. 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 Regional Entity determined that the entity's compliance history should not serve as a basis for applying a penalty.
Mitigation	To mitigate this noncompliance the entity: In the first instance: 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. In the second instance: 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.)	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. 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. 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. 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. 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. The root cause was of this noncompliance was a lack of proper training and guidelines for properly escorting visitors within a PSP.
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 (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. Regional Entity determined that the entity's compliance history should not serve as a basis for applying a penalty.
Mitigation	To mitigate this noncompliance the entity: 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.)	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. 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. 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. 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. 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. 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.
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. 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] 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. No harm is known to have occurred. Texas RE considered [redacted] compliance history and determined there were no relevant instances of noncompliance.
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
			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. Texas RE 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
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.)	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. 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. 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. 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.
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. [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. No harm is known to have occurred. Texas RE considered [redacted] and its affiliate's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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. Texas RE verified the completion of all mitigation activity.

Texas Reliability Entity (Texas RE) | 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
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.)	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. 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. 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. 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.
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 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] No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, [redacted] 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.	[redacted]	[redacted]	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.)			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. [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. 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. 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.				
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. 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. No harm is known to have occurred. Texas RE considered [redacted] compliance history and determined there were no relevant instances of noncompliance.				
Mitigation			To mitigate this noncompliance, [redacted] 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. Texas RE has verified the completion of all mitigation activity.				

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

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

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

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

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2018020007	CIP-005-5	R2. (2.1.)	[redacted] ("the Entity")	[redacted]	7/1/2016	6/28/2018	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.)	During a Compliance Audit conducted from [redacted], the Region determined that the Entity, as a [redacted], was in noncompliance with CIP-005-5 R2. This noncompliance started on July 1, 2016, when the Standard became effective and the Entity had not properly secured Interactive Remote Access; and ended on June 28, 2018, when the Entity moved the Cyber Assets used to initiate Interactive Remote Access into the Electronic Security Perimeter (ESP) and removed firewall rules that allowed Interactive Remote Access. Specifically, the Entity allowed Interactive Remote Access to BES Cyber Systems from seven (7) engineering workstations. These workstations were within an isolated protected network with no remote electronic access available and inside a Physical Security Perimeter (PSP). Electronic access to the workstations was limited to authorized support personnel, who first had to gain access to the PSP with two-factor authentication protections. Additionally, the Entity did not implement its documented processes that included the utilization of an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable BES Cyber Asset. The cause for this noncompliance was due to the Entity's lack of correct understanding of the definition of Interactive Remote Access.
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's failure to properly use an Intermediate System for Interactive Remote Access allowed direct connection to BES Cyber Assets that could have introduced unwanted virus or data transfer. [redacted] FRCC determined that the Entity's compliance history should not serve as a basis for applying a penalty. The previous violations of CIP-005-1 R2 are of different facts and circumstances (i.e., access control models and access point ports and services) and were not related to Interactive Remote Access. The Region did not consider the instant noncompliance a repeat. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance the Entity: 1) moved the required workstations to inside the ESP with all paperwork and checklists complete; 2) removed all firewall rules that allowed access to the ESP; and 3) updated standard operating procedures 27 & 31, to elaborate further on the meaning of user-initiated remote access, better explaining the definition of Interactive Remote Access and providing procedural language to properly evaluate remote access risk mitigation for current and future support 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
FRCC2018020777	CIP-007-6	R3. 3.3.	[redacted] ("the Entity")	[redacted]	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.)	On December 6, 2018, the Entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R3 Part 3.3. 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. 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 [redacted] 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. 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. 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.
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 (BPS). 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. The risk was reduced as the PACS do not directly control BPS Facilities, nor interact with Cyber Assets that do. 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. FRCC determined the Entity's compliance history should not serve as a basis for applying a penalty.
Mitigation	To mitigate this noncompliance, the Entity: 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.

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.	[redacted] ("the Entity")	[redacted]	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.)	On November 20, 2018, the Entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-010-2 R1 Part 1.2. 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. 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. 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. 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.						
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 (BPS). 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. 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. 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. FRCC determined the Entity's compliance history should not serve as a basis for applying a penalty. No harm is known to have occurred.						
Mitigation	To mitigate this noncompliance, the Entity: 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.						

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.	[redacted] ("the Entity")	[redacted]	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.)	On November 19, 2018, the Entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-010-2 R2. 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. 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. 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. 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.
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. 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. 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. FRCC determined the Entity's compliance history should not serves as a basis for applying a penalty. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, the Entity: 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

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	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] identified two instances of noncompliance with CIP-007-6 R5. 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. 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] 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. 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.
Risk Assessment	The noncompliance poses 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 [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. 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.
Mitigation	To mitigate this noncompliance, [redacted] To mitigate the first instance of noncompliance [redacted] 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. To mitigate the second instance of noncompliance [redacted] 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.)	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]. [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 accidently 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. The cause of the noncompliance was that [redacted] failed to implement its manual process for documenting baselines. The noncompliance began on July 1, 2016 when the Standard became enforceable, and ended on June 12, 2018 when the baseline was updated.
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 (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.
Mitigation	To mitigate this noncompliance, [redacted] 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.)	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]. 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). 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. 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.
Risk Assessment	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. [redacted] has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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	[redacted]	[redacted]	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.)	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. The cause of the noncompliance was that [redacted] software development deployment process was flawed and allowed improper changes to be deployed to production. 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.
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 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. [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.
Mitigation	To mitigate this noncompliance, [redacted] 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.)			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. The cause of the noncompliance was a lack of controls to monitor the functionality of the threat detection system. 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.					
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 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. [redacted] has no relevant history of noncompliance.					
Mitigation			To mitigate this noncompliance, [redacted] 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.					

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
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.)	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). The cause of the noncompliance was that the employee failed to follow [redacted] escort policies. 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.
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. [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. [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.
Mitigation	To mitigate this noncompliance, [redacted] 1) had the contractor leave the PSP; and 2) reinforced the escort policy with the employee that left the contractor unescorted.

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
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.)	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. The cause of the noncompliance was that [redacted] failed to follow its Transient Cyber Asset policy. 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.
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. [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. [redacted] has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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.)	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. The cause of the noncompliance is that [redacted] failed to execute its process for implementing security patches. 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.
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 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.
Mitigation	To mitigate this noncompliance, [redacted] 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.)	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. The cause of the noncompliance was that [redacted] failed to follow its written procedures for work orders associated with BES CSI. 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.
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. [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.
Mitigation	To mitigate this noncompliance, [redacted] 1) revised the work orders; and 2) reviewed and reinforced written BES CSI procedures with applicable IT staff.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019580	CIP-004-6	R5	[redacted]	[redacted]	9/24/2016	2/16/2018	Self-Log	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	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. 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. 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. 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. [redacted] The cause of the noncompliance is that [redacted] relied upon a manual process to remove an individual from the EMS application. 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.
Risk Assessment	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.
Mitigation	To mitigate this noncompliance, [redacted] 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.)	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). 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. 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.
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 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. [redacted] has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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.)	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] 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. The cause of the noncompliance was that [redacted] processes lacked sufficient detail to ensure that UDP ports were included in baselines. 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.
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 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.
Mitigation	To mitigate this noncompliance, [redacted] 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.)	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. 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. 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. 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. 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.
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 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. 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. 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.
Mitigation	To mitigate this noncompliance, [redacted] 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. 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. 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.

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.)			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. 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. 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.				
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. [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.				
Mitigation			To mitigate this noncompliance, [redacted] 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.)	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. The cause of the noncompliance was that [redacted] process for identifying additional systems or devices impacted when performing changes lacked sufficient detail. 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.
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. [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.
Mitigation	To mitigate this noncompliance, [redacted] 1) authorized the software change and updated the baselines; 2) improved the process that applies to firewalls by updating its firewall change management process to require the review of the firewall software management tool to identify any Cyber Assets that the firewall software was installed on; and 3) augmented its compliance management software to issue a notification (prior to the 30-day timeframe) when a Cyber Asset's baseline has a difference that has not been addressed.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018018951	CIP-007-6	R2	[redacted]	[redacted]	8/6/2016	7/26/2017	Self-Log	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On October 16, 2017, [redacted] submitted a self-log to MRO stating that, as a [redacted] it was in noncompliance with CIP-007-6 R2. [redacted] (hereafter referred to [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. 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]. 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. 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. 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.
Risk Assessment	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. 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. 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.
Mitigation	To mitigate the first instance of potential noncompliance, [redacted] 1) evaluated and applied the patches; and 2) implemented a monthly patch management coordination meeting. To mitigate the second instance of potential noncompliance, [redacted] 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.)	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. 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. 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.
Risk Assessment	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.
Mitigation	To mitigate this noncompliance, [redacted] 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.)			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] The cause of the noncompliance was that [redacted] failed to follow its process to manually re-enable [redacted] following maintenance activities. 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].					
Risk Assessment			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.					
Mitigation			To mitigate this noncompliance, [redacted] 1) [redacted]; 2) worked with its vendor to implement a solution where [redacted]; and 3) sent a reminder to applicable staff to manually re-enable [redacted] every time a PACS panel is reallocated or power-cycled.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019023	CIP-004-6	R4	[redacted]	[redacted]	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.)	On January 8, 2018, [redacted] submitted a Self-Report stating that as a [redacted] it was in noncompliance with CIP-004-6 R4. Specifically in August 2017, during a periodic review, [redacted] 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 [redacted] buildings, including its substations, [redacted]. [redacted] stated that the employee's access badge did not provide access to the Primary Control Center. [redacted] 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. The cause of the noncompliance was that [redacted] 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. The noncompliance began on July 1, 2016 when the Standard and Requirement became enforceable, and ended on August 2, 2017.
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. [redacted] stated that the unauthorized access was limited to the BUCC and that the employee did not have access to the Primary Control Center. Additionally, [redacted] reports that the individual did not have electronic access to BES Cyber Systems. Further, [redacted] 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. [redacted] 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. [redacted] has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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. To mitigate this noncompliance, [redacted] will complete the following mitigation activities by February 28, 2019: 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. The length of time to complete the remaining mitigating activities is the result of [redacted] investigating different solutions and securing funding for the solution in the 2019 budget.

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
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.)	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. 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. 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.
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 noncompliance was minimal because per [redacted]. No harm is known to have occurred. [redacted] has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 1) corrected the categorization of the four switches, changing them from EACMS to BES Cyber Assets; and 2) an information verification step was added to the assessment process, which requires that System and Network Administrators must verify accuracy of the asset information prior to the review.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2018019320	CIP-003-6	R1	[redacted]	[redacted]	7/1/2017	2/21/2018	Self-Certification	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	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. The noncompliance was caused by [redacted] failure to follow its process. 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.
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 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. [redacted] has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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.

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
SPP2017016900	CIP-007-6	R2	[redacted]	[redacted]	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.)			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. The cause of the noncompliance was that [redacted] processes lacked detail to ensure timely action was taken by applicable staff. The noncompliance began on November 22, 2016, 36 days after the patch was evaluated, and ended later that day when the patch was applied.				
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. [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. [redacted] has no relevant history of noncompliance.				
Mitigation			To mitigate this noncompliance, [redacted] 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.)			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. 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. 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. 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.					
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. 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. 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. No harm is known to have occurred as a result of this noncompliance. 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.					
Mitigation			To mitigate this noncompliance, the entity: 1) Changed the password for the devices in scope. To prevent future recurrence the entity: 1) updated documents for tracking BESCA to include: a) devices with TFE; b) devices that should be remotely manageable; c) device Risk Profile; and 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.					

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.)	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. 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. The root cause of this noncompliance was lack of a control to ensure password age checks were performed before the entity was in noncompliance.						
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. 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. No harm is known to have occurred as a result of this noncompliance.						
Mitigation	To mitigate this noncompliance, the entity: 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
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.)	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. 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. 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. 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.					
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. 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. No harm is known to have occurred as a result of this noncompliance.					
Mitigation	To mitigate this noncompliance, the entity: 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.)	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.). 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. 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. 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. 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.
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. 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. 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. No harm is known to have occurred as a result of this noncompliance. NPCC considered the entity's compliance history and determined there were no relevant underlying causes.
Mitigation	To mitigate this noncompliance, the entity: 1) revised ESP Drawing and Asset List, Identify ESPs; and 2) reviewed NERC Glossary of Terms with Staff. To mitigate this noncompliance, the entity will complete the following mitigation activities by February 28, 2019: 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.

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.)	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.). 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. 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. 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.
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. 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. No harm is known to have occurred as a result of this noncompliance. NPCC considered the entity's compliance history and determined there were no relevant underlying causes.
Mitigation	To mitigate this noncompliance, the entity: 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.)	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.). 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. [redacted] The root cause of this noncompliance was lack of vendor documentation and periodic review.
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. 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] No harm is known to have occurred as a result of this noncompliance. NPCC considered the entity's compliance history and determined there were no relevant underlying causes.
Mitigation	To mitigate this noncompliance, the entity: 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. To mitigate this noncompliance, the entity will complete the following mitigation activities by May 1, 2019: 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.)	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. 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. 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. The root cause of this noncompliance was a failure to include the media player in the security patch tracking spreadsheet.						
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 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. No harm is known to have occurred as a result of this noncompliance. NPCC considered the entity's compliance history and determined there were no relevant underlying causes.						
Mitigation	To mitigate this noncompliance, the entity: 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.						

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.)	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. 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. The root cause of this noncompliance was inadequate contractor training prior to the April 1, 2017 effective date for CIP-010-2 R4.
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. 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. 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. 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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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.)	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. 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. 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.
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. 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. 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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1) the entity's CIP Senior Manager approved the identification of the BES Cyber System [redacted] To prevent future recurrence, the entity: 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]

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.)			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]. 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. 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.					
Risk Assessment			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. No harm is known to have occurred as a result of this noncompliance.					
Mitigation			To mitigate this noncompliance, the entity: 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
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.)	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. 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. 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. The root cause of this noncompliance was due to lack of oversight and miscommunication during deployment of new assets.						
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. 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. 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. No harm is known to have occurred as a result of this noncompliance.						
Mitigation	To mitigate this noncompliance, the entity: 1) created ports and services documentation for the two Protected Cyber Assets (time servers). To prevent future recurrence, the entity: 1) amended its change control process and checklist to require checkoff/signoff of CIP-007 R1 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
NPCC2017018101	CIP-005-5	R1.	[redacted]	[redacted]	7/1/2016	7/17/2017	Self-Log	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	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. 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. [redacted] 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.
Risk Assessment	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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this issue, the entity: 1) removed the firewall connection between the [redacted] facility and the [redacted] substation.

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.)	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]. 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. 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. 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.
Risk Assessment	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. 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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1) created baseline for PACS equipment in scope. To prevent future recurrence, the entity: 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.

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.)	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]. 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. 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.							
Risk Assessment	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. No harm is known to have occurred as a result of this noncompliance.							
Mitigation	To mitigate this noncompliance, the entity: 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.)	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]. 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. [redacted] The root cause of this noncompliance was failure to comply with their password guidelines/procedures.
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. 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]. No harm is known to have occurred as a result of this issue of non-compliance.
Mitigation	To mitigate this noncompliance, the entity: 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.)	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. 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. The root cause of the noncompliance was due to not following procedure. 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. 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. 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. 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.
Risk Assessment	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In each instance all users had valid Personal Risk Assessments and Cyber Security Training certifications in accordance with the NERC CIP Standards. 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. 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. 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. No harm is known to have occurred as a result of these issues of non-compliance.
Mitigation	To mitigate this issue for Instance 1, the entity: 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. To mitigate this issue for Instance 2, the entity:

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

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.

To mitigate this issue for Instance 3, the entity:

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.

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.)	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. 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. 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. 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.
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. 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. [redacted] No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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.)	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. 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. 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). The root cause of this noncompliance was lack of a control to ensure timely termination notifications from vendors.
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. 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. 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. 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. 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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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.

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.)	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. 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. 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. 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.
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. 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. 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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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
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.)	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]. 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. 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.						
Risk Assessment	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. No harm is known to have occurred as a result of this noncompliance.							
Mitigation	To mitigate this noncompliance, the entity: 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
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.)	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. 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. 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: 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 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.
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. 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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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.

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.)	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. 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. The root cause is due to a misunderstanding in how the equipment was being used to monitor and control the BES.
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. 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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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.

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.)	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. 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. 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. 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.
Risk Assessment	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. No harm is known to have occurred as a result of this issue of non-compliance.
Mitigation	To mitigate this issue, the entity: 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; 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.

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.)	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. 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. 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.
Risk Assessment	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. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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.)	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). 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. [redacted] The root cause of the noncompliance was determined to be incomplete design documentation.
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. 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] No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018432	CIP-007-6	R4.	[redacted]	[redacted]	7/1/2016	9/22/2017	Audit	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	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. 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. 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. 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.
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. 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. No harm is known to have occurred as a result of this noncompliance. 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.
Mitigation	To mitigate this noncompliance, the entity: 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
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.)	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. 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. The root cause of this noncompliance was lack of a control to ensure password age checks were performed before the entity was in noncompliance.						
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. 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. No harm is known to have occurred as a result of this noncompliance.						
Mitigation	To mitigate this noncompliance, the entity: 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.						

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.)	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. 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. 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. 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.					
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. 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. No harm is known to have occurred as a result of this noncompliance.					
Mitigation	To mitigate this noncompliance, the entity: 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
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.)	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. 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. The root cause of this noncompliance was a lack of a control to ensure reviews were performed prior to the compliance due date.
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. 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. 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. 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	To mitigate this noncompliance, the entity: 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.)	On February 12, 2018, [redacted] submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R4. This noncompliance involves three instances. 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. 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. 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.
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 (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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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.)	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. 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. 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. 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. 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. 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.
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 (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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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.)	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. 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. 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. 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]t 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. 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. 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.
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 (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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
RFC2016015835	CIP-003-3	R6	[redacted]	[redacted]	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.)	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. 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. 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. 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. The entity verified that no security controls were impacted by the unauthorized changes. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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). ReliabilityFirst 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
RFC2016016354	CIP-005-5	R1	[redacted]	[redacted]	7/1/2016	9/9/2016	Audit	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On [redacted] ReliabilityFirst determined that [redacted] as a [redacted] and [redacted] was in violation of CIP-005-5 R1. ReliabilityFirst identified the violation during a Compliance Audit conducted from [redacted]. Seven of the entity's Bulk Electric System (BES) Cyber Systems that the entity identified as Protected Cyber Assets (PCA) were connected via a routable protocol to a network, but did not reside within a defined Electronic Security Perimeter (ESP) and network traffic to and from these BES Cyber Systems was not through an identified Electronic Access Point (EAP). These BES Cyber Systems bridged both ESP and non-ESP network segments. This occurred because a former ESP was declassified and these PCAs were overlooked during the decommissioning of the former ESP. As such, the entity continued to classify these systems as PCAs and the assets continued to be monitored and protected by [redacted]. Upon identification at audit, the entity exercised an emergency shutdown on all assets. 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. 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.
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 based on the following factors. The potential risk was the possibility of unwanted network traffic into the ESP. The risk here is mitigated because the entity continued to classify these assets as PCA and thus, except for CIP-005-5 R1, Parts 1.1 and 1.2, the assets were protected pursuant to the CIP Standards. For example, the assets continued to be monitored for baseline changes, met the password requirements, and had updated antivirus. Also, the assets were not directly accessible from the user network. [redacted] No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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. 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. Twelve instances related to four Electronic Access Control or Monitoring systems (EACMS) and one instance related to four Bulk Electric System Cyber Assets. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
RFC2017018652	CIP-007-6	R2	[redacted]	[redacted]	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.)	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. 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. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
RFC2017017733	CIP-010-2	R2	[redacted]	[redacted]	7/1/2016	6/20/2017	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.)	On June 5, 2017, [redacted] submitted a Self-Report to ReliabilityFirst stating that, as a [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. 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. 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. 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. 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. 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.
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 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. ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 1) removed the BCSI from the twelve drawings. The entity created twelve new drawings and the BSCI was place 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. ReliabilityFirst 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
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.)	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. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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. 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. 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. 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.						
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 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. 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.						
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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. 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] [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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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] [redacted] and [redacted] accounts for each area of responsibility: [redacted], [redacted] and [redacted] 3) compared Shared Accounts from [redacted] [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] [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. ReliabilityFirst 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
RFC2017018479	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.)	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. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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] 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]. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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] 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. 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] 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. 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.
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 (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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
RFC2017018863	CIP-007-6	R3	[redacted]	[redacted]	10/13/2017	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.)	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] 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. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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. 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. 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. 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.
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 (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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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. 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). 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. 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.
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 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. No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity: 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). 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. ReliabilityFirst 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
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.)	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. 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. 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.
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 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. ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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.) 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. 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. 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.
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 (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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
RFC2017018710	CIP-011-2	R1	[redacted]	[redacted]	7/1/2016	9/26/2017	Self-Report	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	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] 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. 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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]. ReliabilityFirst 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
RFC2017018770	CIP-007-6	R4	[redacted]	[redacted]	9/23/2017	9/24/2017	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.)	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. 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. This noncompliance started on September 23, 2017, when the entity first lost logs, and ended on September 24, 2017, when logging was restored.
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 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] 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	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] 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. 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.
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 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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
RFC2018019117	CIP-010-2	R2	[redacted]	[redacted]	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.)	On January 30, 2018, [redacted] submitted a Self-Report stating that, as a [redacted] and [redacted] it was in noncompliance with CIP-010-2 R2. The entity failed to monitor for changes to the baseline configuration at least once every 35 calendar days as required by CIP-010-2 R2 for two vulnerability scanner servers, which are Protected Cyber Assets (PCAs). They were not monitored because they were offline and thus the monitoring tool could not read the devices. The first asset's baseline was not monitored from August 12, 2017 through October 9, 2017 (58 calendar days) and the second asset's baseline was not monitored from August 29, 2017 through October 9, 2017 (41 calendar days). On October 6, 2017, the entity discovered both issues during a daily baseline monitoring reconciliation, and then resolved the issues on October 9, 2017. As additional background, for the first server, on August 13, 2017, during daily baseline monitoring, the entity identified a "modified" baseline for the server. "Modified" as it relates to the reporting status for the entity's monitoring tool means the configuration baseline scan shows a variance between current and last baseline (due to configuration baseline change or scanning error; or, as in this case, the reported "modification" was because the server was off-line). The entity failed to document the modification, which led to a delay in identifying the issue. Regarding the second server, on August 30, 2017, during daily baseline monitoring, the entity identified a modified baseline (again, due to the server being offline). The entity could not reconcile the change because there was not an associated change ticket. An analyst observed that the current baseline from that day matched a prior current baseline (actually the August 30, 2017 modification) and promoted the modification in [redacted] in error. This resulted in the entity incorrectly identifying the change as an approved change (and thus not investigating the change). 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. 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. 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.
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 (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. ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1) documented and investigated the deviations for the affected assets as required by the entity's configuration management and baseline monitoring process; 2) conducted a meeting to identify the root causes; 3) configured [redacted] to automatically monitor configuration baselines for the affected assets; 4) trained teams on the method of communication between teams and escalation of un-reconcilable baseline modifications to the owner of the baseline monitoring process; 5) counseled responsible entity analysts on the requirements of the documented configuration management and baseline monitoring process, test procedures process, and change management process including the importance of following procedures; and 6) added a new procedural control requiring a peer review prior to manually promoting baselines within [redacted] and defining escalation path and timelines, and trained staff on the above. ReliabilityFirst 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
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.)	On March 23, 2018, [redacted] submitted a Self-Report stating that, as a [redacted] and [redacted] it was in noncompliance with CIP-010-2 R1. On December 1, 2017, a baseline change inadvertently occurred on a Physical Access Control System (PACS) client workstation without an associated change ticket, which would have alerted entity staff to perform pre-change test procedures on the asset. The baseline changes were ultimately detected by a routine [redacted] scan on December 5, 2017. The entity thereafter tested the security controls and confirmed that they were not adversely affected by the change. The inadvertent software installation occurred because an entity analyst updated the entity's Electronic Security Perimeter-[redacted] infrastructure to a new version. [redacted] 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. 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.
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 (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. 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.
Mitigation	To mitigate this noncompliance, the entity: 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." ReliabilityFirst 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
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.)	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. 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. 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. 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. 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. 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.
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 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. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, the entity: 1) initiated the recovery plan for the impacted Physical Security Perimeter, including posting a guard; and 2) restored normal function of the PACS for the impacted Physical Security Perimeter.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020408	CIP-004-6	R4; P4.2	[redacted]	[redacted]	1/1/2018	6/19/2018	Self-Log	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	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. 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. 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. 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. 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. 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.
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 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. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, the entity: 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.)	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. 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. 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. 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. 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. 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.
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 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] 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. No harm is known to have occurred.

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])	[redacted]	7/9/2018	7/11/2018	Self-Log	Completed
Mitigation			To mitigate this noncompliance, the entity: 1) initiated the recovery plan for the impacted Physical Security Perimeters; 2) restored normal function of the PACS for the impacted Physical Security Perimeters; 3) initiated the recovery plan for the impacted Physical Security Perimeters; 4) restored normal function of the PACS for the impacted Physical Security Perimeters; 5) discussed measures with [redacted] staff to enhance reporting of fire system activations to the entity [redacted] and coordination of system maintenance; and 6) implemented measures to enhance reporting of fire system activations to the entity [redacted] and coordination of system maintenance.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018020410	CIP-007-6	R5 P5.4	[redacted]	[redacted]	7/23/2018	7/26/2018	Self-Log	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	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. 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. 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. [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. 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. 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.
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 (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. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, the entity: 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.)	On February 23, 2018, [redacted] and [redacted] through [redacted] submitted a Self-Report stating that, as a [redacted] and [redacted] they were in noncompliance with CIP-004-6 R4. [redacted]. 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. 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. 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.
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 (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. No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	On February 23, 2018, [redacted] and [redacted] through [redacted] submitted a Self-Report stating that, as a [redacted] and [redacted] they were in noncompliance with CIP-006-6 R1. [redacted] On January 10, 2018, an entity senior IT infrastructure consultant (Infrastructure Consultant) on the [redacted] Team opened a secure Physical Security Perimeter (PSP) cabinet, and subsequently left the area without re-securing the cabinet. The cabinet is located inside a card-reader-protected server room inside a building that requires company identification to enter. Video records reveal that the PSP cabinet was left unattended for 16 minutes. 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). 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] isited the area and verified that all appropriate NERC CIP Physical Security Perimeter signage was in place.) 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. 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.
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 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. No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
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.)	On February 23, 2018, [redacted] submitted a Self-Report stating that, as a [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. 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. 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. 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. 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. 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.
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 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. No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
RFC2018019506	CIP-010-2	R1	[redacted]	[redacted]	1/5/2018	2/12/2018	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.)	On March 28, 2018, [redacted] and [redacted] through [redacted] submitted a Self-Report stating that, as a [redacted] and [redacted] they were in noncompliance with CIP-010-2 R1. [redacted] 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. 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. 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. 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] 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. 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. 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] to track the 30-day baseline update requirement. That failure to verify is a contributing cause of this noncompliance. 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.
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 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. No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity: 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;

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
			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 4) updated the procedure for tracking the baseline to ensure that any configuration exceptions which are not accepted into the baseline are clearly documented in an incident record whose target completion date is less than thirty days from the original "[redacted] before accepting any exceptions. The entity also reviewed a report of such incident records weekly at the same time the [redacted] is reviewed. ReliabilityFirst has verified the completion of all mitigation activity.					

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	[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.)	On February 23, 2018, [redacted] submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-004-6 R4. 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. 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. 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.
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 (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. No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
RFC2018019280	CIP-006-6	R1	[redacted]	[redacted]	1/10/2018	1/11/2018	Self-Report	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On February 23, 2018, [redacted] submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-006-6 R1. On January 10, 2018, an entity senior IT infrastructure consultant (Infrastructure Consultant) on the [redacted] Team opened a secure Physical Security Perimeter (PSP) cabinet, and subsequently left the area without re-securing the cabinet. The cabinet is located inside a card-reader-protected server room inside a building that requires company identification to enter. Video records reveal that the PSP cabinet was left unattended for 16 minutes. 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). 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.) 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. 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.
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 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. No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
RFC2018019279	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.)	On February 23, 2018, [redacted] submitted a Self-Report stating that, as a [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. 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] from detecting the related configuration baseline exceptions the morning after they were installed. This triggered an internal investigation into what prevented [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. 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. 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. 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.
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 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. No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity: 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. ReliabilityFirst 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
RFC2018019507	CIP-010-2	R1	[redacted]	[redacted]	1/5/2018	2/12/2018	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.)	On March 28, 2018, [redacted] submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-010-2 R1. 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. 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. 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. 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] 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. 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. 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] to track the 30-day baseline update requirement. That failure to verify is a contributing cause of this noncompliance. 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.
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 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. No harm is known to have occurred. 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.
Mitigation	To mitigate this noncompliance, the entity: 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; 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

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

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016494	CIP-006-6	R2; P2.2	[redacted]	[redacted]	7/5/2016	11/2/2016	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.)	On November 8, 2016, [redacted] submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-006-6 R2, Part 2.2. The entity determined that it failed to require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter (PSP) that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances, on several different occasions. On November 2, 2016, a CIP subject matter expert (SME) observed missing log information while signing in a visitor and discovered a potential violation affecting the October 2016 manual visitor log for the primary control center. Later on the same date, the CIP SME notified the CIP Senior Manger via email of the identified noncompliance. The CIP Senior Manager then reviewed the visitor log for correctness and confirmed the SME's findings that there was missing required information as documented in the entity's visitor control program. A subsequent comprehensive review spanning July through October 2016 revealed that there were 20 log entry errors affecting 13 visitors for the primary control center and 2 log entry errors affecting 2 visitors for the data center, for a total of 22 logging error instances affecting 15 visitors. The logs indicate the name of the visitor for all 15 visitors with visitor log issues. However, for the associated 22 instances of logging oversights, there were 8 omissions of individual points of contact responsible for visitors, 3 omissions of time of initial entry, and 11 omissions of time of last exit. On November 7, 2016, the CIP Senior Manager held a meeting to review the potential noncompliance and annual training materials for any possible enhancements. The scope of affected Facilities included a primary control center and data center. Affected Cyber Assets included 1 medium impact Bulk Electric System (BES) Cyber System (the energy management system), 23 BES Cyber Assets, 5 Protected Cyber Assets, 10 Electronic Access Control or Monitoring Systems and 2 Physical Access Control Systems. The entity determined the extent-of-condition through a review of all manual visitor logs spanning July through October 2016. The root cause of the noncompliance was a workflow process in need of enhancement, and insufficient training related to situational awareness of visitor escort responsibilities. The monthly workflow tool did not specify to review the visitor log daily, and only required collection of the logs monthly. In addition, the workflow only required a review by the CIP Senior Manager on an annual basis, at the end of the calendar year. This noncompliance lasted from July 5, 2016, the date of the first noncompliant log entry, until November 2, 2016, the date the entity discovered the noncompliance.
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 (BPS). The entity's incomplete documentation of visitor access could have potentially permitted physical access to essential systems that could result in an adverse impact to the BPS. The entity's noncompliance with this requirement could hamper the investigation phase of an event due to not properly documenting physical access into a PSP. However, the log books included all visitor names and the entity continuously escorted all 15 visitors. Further, date and time-stamped CCTV video footage was available to enable identification of the visitors, of which 14 were the entity employees with currently in-force personnel risk assessments and cyber security training, and the last was a non-employee continuously escorted for purposes of fire suppression assessment. No harm is known to have occurred. SERC considered the entity's compliance history and determined that there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1) provided additional annual online training that covered visitor controls; 2) provided quarterly training of the Visitor Control procedure/process with emphasis on the responsibilities of the entity "Escort"; and 3) added a visitor log review prior to the end of the business day.

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	[redacted]	[redacted]	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.)	On June 29, 2017, [redacted] submitted a Self-Report to SERC stating that, [redacted] 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. 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. 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. 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. The entity determined the extent-of-condition by implementing the annual access review that led to discovery. The entity discovered no additional instances. The root cause of this noncompliance was determined to be oversights in activities associated with implementing compliance with CIP version 5. 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.
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. 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. SERC considered the entity's compliance history and determined that there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 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 [redacted] 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 [redacted] is responsible for ensuring that staff transfers, standard terminations, and terminations for cause are completed based upon this program's processes. The [redacted] 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

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.)	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. 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. 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.
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. 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. [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. 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.
Mitigation	To mitigate this noncompliance, [redacted]: 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
WECC2017017689	CIP-007-6	R1, P1.1	[redacted]	[redacted]	7/1/2016	7/31/2017	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.)

On May 31, 2017, [redacted] submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R1.

Specifically, [redacted] reported that on May 3, 2017, during an internal audit of its CIP program, it was unable to locate sufficient evidence that it enabled only ports and services for its Physical Access Control System (PACS) that were determined to have a business need. [redacted] PACS consisted of one desktop computer accessible inside the Control Center, one PACS server which controls and monitors the individual switches, and 13 PACS switches which control the physical security of 13 Physical Security Perimeters (PSP) for a total of 15 devices. [redacted] had implemented a process for system administrators to document and enable ports and services for applicable devices, however no controls were in place to maintain and validate that the process was applied to all of the applicable CIP devices when a SME left [redacted] employment and their compliance responsibilities transferred to a new employee.

After reviewing all relevant information, WECC determined that [redacted] failed to enable only logical network accessible ports that have been determined to be needed for its PACS, including port ranges or services where needed to handle dynamic ports, as required by CIP-007-6 R1 Part 1.1.

The root cause of the issue was due to management not having adequate processes or procedures for transitioning compliance job responsibilities prior to an employee leaving.

WECC determined that this issue began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable to [redacted] and the end date of this issue was July 31, 2017, when it met the requirements of the standard for the PACS, for a total of 396 days.

Risk Assessment

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 enable only logical network accessible ports that have been determined to be needed for its [redacted] including port ranges or services where needed to handle dynamic ports, as required by CIP-007-6 R1. Part 1.1. Such failure could create a situation where [redacted] could enable ports or services that were not part of the authorized baseline, thereby creating an opportunity for exploitation. Additionally, such failure could potentially affect [redacted] generation or interconnection should a threat actor be able to access and exploit the PACS on an unsecured port. This could enable the threat actor to modify the physical access controls of the facilities by either denial-of-service by locking out authorized individuals or by allowing unauthorized individuals to gain physical access to the facilities. [redacted] Therefore, WECC assessed the potential harm to the security and reliability of the BPS as intermediate.

However, the PACS were air-gapped from all other networks and did not have any external electronic access. All electronic access to the PACS must be performed while physically at the device. Additionally, [redacted] maintained documentation files for listening ports and configuration files of the host based firewalls as well as documentation of other device level mechanisms which identified the ports and services communication traffic which was approved and established based on the business need. 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.

WECC notes that [redacted] does not have any relevant previous violations of this or similar Standards and Requirements.

Mitigation

[redacted] completed mitigating activities to address this issue and WECC verified [redacted] mitigating activities.

To remediate and mitigate this issue, [redacted]
1.) Finalized procedures for transitioning of job responsibilities to include documentation and file location for documentation prior to an employee leaving a position;
2.) Validated and documented the business need for all enabled ports and services for the PACS;
3.) Modified device configurations for any ports and services that were enabled but do not have a documented business need;
4.) Created a current listing of configuration files for host-based firewalls or other device level mechanisms and validate the business need;
5.) Centralized its documentation location and retention for future review and use; and
6.) Provided training to all personnel on all new procedures and documentation required to comply with the CIP-007-6 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
WECC2016016415	CIP-007-6	R2, P2.2, 2.3	[redacted]	[redacted]	7/1/2016	2/16/2018	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.)

On October 26, 2016, [redacted] submitted a Self-Report stating that, as a [redacted] and a [redacted], it was in noncompliance with CIP-007-6 R2.

Specifically, [redacted] 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 [redacted] on June 30, 2016. The vendor was not able to achieve remote access into [redacted] patch management system due to improperly maintained password files by the Lead technician who was no longer at [redacted] 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, [redacted] 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 [redacted] on June 10, 2016. [redacted] 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.

After reviewing all relevant information WECC determined that [redacted] 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, [redacted] 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.

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.

WECC determined that the issues began July 1, 2016, when the Standard and Requirement became effective and ended on February 16, 2018 when [redacted] completed its security patch evaluations and installation of applicable patches for all devices in scope, for a total of 231 days.

Risk Assessment

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, [redacted] 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, [redacted] 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 [redacted] MIBCS to cause disruptions to its operating capabilities, potentially affecting [redacted] of generation and the interconnection of [redacted] and [redacted] ties to the BES. WECC assessed the potential harm to the security and reliability of the BPS as intermediate.

However, [redacted] 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, [redacted] 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.

No harm is known to have occurred.

[redacted] does not have any relevant previous violations of this or similar Standards and 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
WECC2016016415	CIP-007-6	R2, P2.2, 2.3	[redacted]	[redacted]	7/1/2016	2/16/2018	Self-Report	Completed

Mitigation	To remediate and mitigate this issue, [redacted] 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. 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
WECC2018018940	CIP-004-6	R4: P4.1.1.	[redacted]	[redacted]	12/12/2017	12/12/2017	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.)	On January 3, 2018, [redacted] submitted a Self-Report stating that, as a [redacted] and [redacted], it was in noncompliance with CIP-004-6 R2. Specifically, [redacted] reported that on December 19, 2017 during a weekly meeting, it discovered that on December 12, 2017, a subcontractor was given escorted physical access to a Physical Security Perimeter (PSP) for the purpose of replacing the Physical Access Control System (PACS) panel associated with the PSP door which protected [redacted] Medium Impact Bulk Electric System (BES) Cyber System (MIBCS) with External Routable Connectivity (ERC). As part of the process of replacing the PACS panel, the subcontractor needed electronic access to the PACS server in order to set up communications between the new panel and the server. A [redacted] technician, with authorized electronic access to the server, logged in with his credentials so that the subcontractor could access the server and complete his work. The subcontractor was on site from 9:15 AM to 4:30 PM and accessed the PACS server for approximately two hours throughout the day. Even though the [redacted] technician was physically present for the entire time the subcontractor was accessing the server, there is no Requirement in the Standard that allows for the escorting of electronic access. After reviewing all relevant information, WECC determined that [redacted] failed to appropriately implement its process to authorize electronic access to its PACS associated with the MIBCS with ERC based on need, as required by CIP-004-6 R4 Part 4.1 Sub-Part 4.1.1. [redacted] not did fail CIP-004-6 R2 as originally Self-Reported. The root cause of the issue was due to less than adequate processes or procedures. Specifically, [redacted] Access Management Program at the time did not clearly define the expectations for third-party electronic access to its CIP applicable systems. This noncompliance started on December 12, 2017, when an unauthorized individual gained electronic access to [redacted] PACS server, and ended that same day, when the unauthorized individual's electronic access was removed.
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 (BPS). In this instance, [redacted] failed to appropriately implement its process to authorize electronic access to its PACS associated with the MIBCS with ERC based on need, as required by CIP-004-6 R4 Part 4.1 Sub-Part 4.1.1. Such failure could allow a malicious actor to adjust the settings on the PACS such as turning off alarms, which would limit situational awareness, or allow unrestricted access to the MIBCS by adjusting or removing access rights. [redacted] owns and/or operates [redacted] of generating capacity with a peak load of [redacted] that was applicable to this issue. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as minor. However, [redacted] had weak controls in place to prevent this issue. The only compensating factor was the subcontractor being continuously escorted while in the PSP and on the server. Based on this, WECC determined that there was a moderate likelihood of causing minor harm to the BPS. No harm is known to have occurred. WECC considered [redacted] compliance history in its designation of this remediated issue as a CE. [redacted] prior compliance history with CIP-004-6 R4 includes NERC Violation IDs [redacted] and [redacted] WECC determined that [redacted] is not relevant compliance history as it deals with keeping the list updated when changes occur, which is different from this noncompliance. Additionally, WECC determined that while [redacted] is relevant compliance history, it is only one instance of previous noncompliance and should not serve as an aggravating factor to escalate the disposition.
Mitigation	To mitigate this noncompliance, [redacted] 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.)	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. 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. 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. 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. 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.
Risk Assessment	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. 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. WECC determined that [redacted] has no relevant compliance history for this noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 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.

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
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.)	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. 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 though 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. 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. 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. 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.
Risk Assessment	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. 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. No harm is known to have occurred. [redacted] does not have any relevant previous violations of this or similar Standards and Requirements.
Mitigation	To remediate and mitigate this issue, [redacted] 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

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])	[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	[redacted]	[redacted]	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.)	During a Compliance Audit conducted from [redacted], WECC auditors determined that [redacted] as a [redacted], and [redacted], had a potential noncompliance with CIP-014-2 R4 and R5. Specifically, [redacted] provided evidence that it completed R4 and R5 of CIP-014-2 on April 5, 2016, which was 189 days after it completed R2. After reviewing all the relevant information, WECC determined that [redacted] 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. The root cause of the noncompliance was [redacted] 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". [redacted] understood the "Not Later Than" date as the initial implementation date. WECC determined that these issues began on January 27, 2016, which was 120 days after [redacted] completed CIP-014-2 R2, and ended on April 5, 2016, when [redacted] completed R4 and R5, for a total of 69 days of noncompliance.
Risk Assessment	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, [redacted] 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. [redacted] transmission system consists of approximately [redacted] miles of transmission which includes [redacted] miles of [redacted] lines, [redacted] miles of [redacted] lines, and [redacted] miles of [redacted] lines. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as intermediate. However, [redacted] 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. WECC determined that [redacted] has no relevant compliance history for this noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 1) held a kick-off meeting for the next R1 Transmission Risk Assessment, at which time attendees discussed timelines; the audit finding; and recommendations received from the audit; 2) scheduled on-going status meetings to track progress and timelines and to facilitate communication between business areas; 3) added CIP-014-2 compliance activities and deadlines into its ServiceNow tracking system; and 4) adopted a date calculator to track the calculation of dates to ensure future dates are not missed.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018587	CIP-014-2	R5	[redacted]	[redacted]	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.)	During a Compliance Audit conducted from [redacted], WECC auditors determined that [redacted] as a [redacted], and [redacted], had a potential noncompliance with CIP-014-2 R4 and R5. Specifically, [redacted] provided evidence that it completed R4 and R5 of CIP-014-2 on April 5, 2016, which was 189 days after it completed R2. After reviewing all the relevant information, WECC determined that [redacted] 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. The root cause of the noncompliance was [redacted] 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". [redacted] understood the "Not Later Than" date as the initial implementation date. WECC determined that these issues began on January 27, 2016, which was 120 days after [redacted] completed CIP-014-2 R2, and ended on April 5, 2016, when [redacted] completed R4 and R5, for a total of 69 days of noncompliance.
Risk Assessment	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, [redacted] 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. [redacted] transmission system consists of approximately [redacted] miles of transmission which includes [redacted] miles of [redacted] lines, [redacted] miles of [redacted] lines, and [redacted] miles of [redacted] lines. Therefore, WECC assessed the potential harm to the security and reliability of the BPS as intermediate. However, [redacted] 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. WECC determined that [redacted] has no relevant compliance history for this noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 1) held a kick-off meeting for the next R1 Transmission Risk Assessment, at which time attendees discussed timelines; the audit finding; and recommendations received from the audit; 2) scheduled on-going status meetings to track progress and timelines and to facilitate communication between business areas; 3) added CIP-014-2 compliance activities and deadlines into its ServiceNow tracking system; and 4) adopted a date calculator to track the calculation of dates to ensure future dates are not missed.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017879	CIP-007-6	R4; P4.1; P4.3	[redacted]	[redacted]	7/1/2016	9/26/2016	Self-Report	Completed

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.)	On July 7, 2017, [redacted] submitted a Self-Report stating that, as a [redacted] and [redacted], it was in noncompliance with CIP-007-6 R4. Specifically, [redacted] reported that during a change control review conducted in September 2016, it identified an instance in which it failed to capture and retain 90 calendar days of security event logs for one Electronic Access Control or Monitoring System (EACMS) which did not have a Security Incident and Event Manager (SIEM) log collector installed, and two network switches which were improperly configured and did not have a firewall rule in place to enable log collection to the SIEM; all associated with a Medium Impact BES Cyber System (MIBCS). Additionally, [redacted] reported that during a Cyber Vulnerability Assessment (CVA) it identified one EACMS associated with a High Impact Bulk Electric System (BES) Cyber System (HIBCS) that was not capturing and retaining security event logs due to configuration errors on the SIEM device which caused a gap in logging. The SIEM was collecting and storing all logs sent to the device from other devices, but was not logging failed login attempts to itself. The SIEM was inadvertently disabled during a recent upgrade to the device. After reviewing all relevant information, WECC determined [redacted] failed to capture and retain security event logs, per BES Cyber Asset capability, for all cyber security events as required by CIP-007-6 R4 Part 4.1 Sub-Parts 4.1.1 and 4.1.2 and R4.3, for four Cyber Assets. The root cause of the noncompliance was insufficient manpower to support goals and objectives. Specifically, during the transition from CIP Version 3 to CIP Version 5, asset configuration changes were not tested or peer reviewed before implementation. WECC determined that events began when [redacted] failed to log and retain security event logs on July 1, 2016 and ended on September 26, 2016 when [redacted] started logging and retaining security event logs as required by CIP-007-6 R4, Part 4.1, Sub-Parts 4.1.1, 4.1.2, and Part 4.3, for a total of 88 days.
Risk Assessment	WECC determined that this noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, [redacted] failed to capture and retain security event logs, per BES Cyber Asset capability, for all cyber security events as required by CIP-007-6 R4 Part 4.1 Sub-Parts 4.1.1 and 4.1.2 and R4.3, for four Cyber Assets. Such failure could allow a malicious actor to login to the devices without [redacted] knowledge. A failure to retain ninety days of logs would prevent [redacted] from being able to review the security details for after-the-fact investigations. This could potentially cause a loss of remote access and SCADA data for series capacitors on one of the [redacted] lines which include [redacted]. A potential loss of other devices at a [redacted] substation could potentially cause a loss of remote access to meters, however data is still sent to Electronic Monitoring System (EMS) via serial cable at this location. [redacted] owns and operates [redacted] of [redacted] generation, and [redacted] of generation in their [redacted] footprint. [redacted] transmission system consists of approximately [redacted] miles of transmission which includes [redacted] miles of [redacted] lines, [redacted] miles of [redacted] lines, and [redacted] miles of [redacted] lines. WECC assessed the potential harm to the security and reliability of the BPS as intermediate. However, [redacted] Cyber Assets were physically secured as well as isolated from the internet and internal networks by utilizing network segmentation to include firewalls that deny access by default. In the event a system would have gone down or resource usage was abnormal, [redacted] Systems or Network and Telephone Services teams would have received notification and troubleshooting would have taken place to identify the root cause and any attack would have been identified as part of their troubleshooting. The primary physical monitoring of the BES Cyber System is performed in real-time at the Physical Security Command Center which is manned twenty-four hours a day. Based on this, WECC determined that there was a low likelihood of causing intermediate harm to the BPS. No harm is known to have occurred. WECC determined that [redacted] compliance history should not serve as a basis for applying a penalty. There was a different cause for the prior instances of noncompliance which was distinct and separate than the cause of this issue.
Mitigation	To mitigate this noncompliance, [redacted] 1) restarted the SIEM logging service to enable log collection and storage of logs; 2) installed the SIEM collector on applicable device; 3) added firewall rules to allow logs to send to the log collectors;

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.					