

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	MRO2019020984			Yes	Yes	Yes			Yes	Yes				Category 2 – 12: 2 years
2	MRO2019020985	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
3	MRO2019022636	Yes		Yes	Yes	Yes				Yes				Category 1: 3 years; Category 2 – 12: 2 years
4	MRO2019021713	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
5	MRO2019022632	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
6	MRO2019022427	Yes		Yes	Yes	Yes								Category 1: 3 years; Category 2 – 12: 2 years
7	MRO2020022823			Yes	Yes									Category 2 – 12: 2 years
8	MRO2020022827	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
9	MRO2019022125			Yes	Yes					Yes				Category 2 – 12: 2 years
10	MRO2019022130	Yes	Yes	Yes	Yes	Yes	Yes							Category 1: 3 years; Category 2 – 12: 2 years
11	MRO2019022641	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
12	MRO2019022053	Yes		Yes	Yes	Yes					Yes			Category 1: 3 years; Category 2 – 12: 2 years
13	NPCC2019022283	Yes		Yes	Yes				Yes					Category 1: 3 years Categories 3 – 4: 2 years Category 8: 2 years
14	NPCC2019022284	Yes		Yes	Yes									Category 1: 3 years Categories 3 – 4: 2 years
15	NPCC2019021988	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years Categories 3 – 4: 2 years Categories 8 – 9: 2 years
16	NPCC2019022390	Yes		Yes	Yes				Yes					Category 1: 3 years Categories 3 – 4: 2 years Category 8: 2 years
17	NPCC2019021173			Yes	Yes				Yes		Yes			Categories 3 – 4: 2 years Category 8: 2 years Category 10: 2 years
18	NPCC2019021175			Yes	Yes						Yes			Categories 3 – 4: 2 years Category 10: 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)
19	NPCC2019021176	Yes		Yes	Yes						Yes			Category 1: 3 years Categories 3 – 4: 2 years Category 10: 2 years
20	NPCC2019021177			Yes	Yes						Yes			Categories 3 – 4: 2 years Category 10: 3 years
21	NPCC2019021619			Yes	Yes									Categories 3 – 4: 2 years
22	NPCC2019022285	Yes		Yes	Yes				Yes					Category 1: 3 years Categories 3 – 4: 2 years Category 8: 2 years
23	NPCC2018019453			Yes	Yes						Yes			Categories 3 – 4: 2 years Category 10: 2 years
24	RFC2019021806	Yes		Yes	Yes		Yes							Category 1: 3 years Category 2 – 12: 2 years
25	RFC2019022148	Yes	Yes	Yes	Yes		Yes		Yes				Yes	Category 1: 3 years Category 2 – 12: 2 years
26	RFC2019022255	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
27	RFC2019022440	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
28	RFC2019022021	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
29	RFC2019021805	Yes		Yes	Yes		Yes							Category 1: 3 years Category 2 – 12: 2 years
30	RFC2019022197			Yes	Yes									Category 2 – 12: 2 years
31	RFC2019021728	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 years
32	SERC2018018946		Yes	Yes						Yes				Category 2 – 12: 2 year
33	SERC2018019343			Yes	Yes						Yes			Category 2 – 12: 2 year
34	SERC2019022119	Yes		Yes	Yes			Yes	Yes					Category 2 – 12: 2 year
35	SERC2019022135			Yes	Yes					Yes				Category 2 – 12: 2 year
36	SERC2018020883			Yes	Yes			Yes	Yes		Yes			Category 2 – 12: 2 year
37	SERC2018020884			Yes	Yes			Yes	Yes		Yes			Category 2 – 12: 2 year
38	TRE2019022005	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
39	TRE2019022454	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)
40	WECC2018020714			Yes	Yes									Category 2 – 12: 2 years
41	WECC2020022820			Yes	Yes					Yes				Category 2 – 12: 2 years
42	WECC2020022982	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
43	WECC2019021791			Yes	Yes									Category 2- 12: 2 years
44	WECC2019021696	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
45	WECC2019021697	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
46	WECC2020022962			Yes	Yes									Category 2 – 12: 2 years
47	WECC2020023383			Yes	Yes									Category 2 – 12: 2 year
48	WECC2020022990			Yes	Yes					Yes				Category 2 – 12: 2 years
49	WECC2017018855	Yes		Yes	Yes					Yes				Category 1 (3 years) and 2 - 12: (2 years)

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019020984	CIP-006-6	R2	[REDACTED] (the Entity)	[REDACTED]	02/14/2018	02/14/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 18, 2019, the Entity submitted a Self-Report stating that [REDACTED], it was in noncompliance with CIP-006-6 R2. [REDACTED]</p> <p>The Entity reported that a supervisor provided their badge to a subordinate, who was authorized but did not have provisioned unescorted physical access to a Physical Security Perimeter (PSP), in order to escort external personnel into the PSP.</p> <p>The cause of the noncompliance was that Entity's failure to follow its process to ensure adherence to its documented Visitor Control Program.</p> <p>The noncompliance began on February 14, 2018, when the Entity failed to provide continuous escorted access to the individual of issue, and ended on February 14, 2018, when the individual exited the PSP.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the issue was limited to a single occurrence at [REDACTED] with a total duration that was less than ten minutes. The escorting individual accompanied the third party contractor for the duration of the visit, had a valid Personnel Risk Assessment (PRA), and was up to date on the Entity's required CIP cyber security training. Additionally, the Entity determined that the escorting individual had a legitimate need to receive unescorted physical access provisioning, but was lacking the management order granting the access privilege. No harm is known to have occurred.</p> <p>The Entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) escorted the third party from the PSP; 2) reiterated to the involved individuals its visitor program requirements prohibiting the sharing of badges; 3) sent an email to all supervisors at the affected facility reiterating its visitor program requirements. The supervisors also reviewed the policy with their employees; and 3) discussed access policy requirements, focusing on procedures for entering substations, at a company-wide [REDACTED] meeting. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Mitigation Completion Date
MRO2019020985	CIP-007-6	R3	[REDACTED] (the Entity)	[REDACTED]	7/1/2016	2/22/2018	Self- Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.)			<p>On January 18, 2019, the Entity submitted a Self-Report stating that [REDACTED], it was in noncompliance with CIP-007-6 R3. [REDACTED]</p> <p>The Entity reported that [REDACTED] Cyber Assets (servers) protected by antivirus (AV) software were not receiving antivirus signature updates. After the Self-Report was submitted, the Entity discovered that one server was receiving signature updates, and that the initial noncompliant determination for that asset was a false positive related to server communications. Therefore, the issue was limited to [REDACTED]</p> <p>The noncompliance began on July 1, 2016, when the standard became enforceable, and ended on February 22, 2018, when the AV software on the affected Windows server was reinstalled and the Entity confirmed receipt of signature updates.</p> <p>The cause of the noncompliance was that the Entity’s process for updating the antivirus signatures was deficient as it did not ensure the devices were setup in the appropriate group and reporting to the antivirus management software properly to receive updates.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity’s Control Center contains [REDACTED], monitors [REDACTED] containing [REDACTED], and monitors [REDACTED] that contain [REDACTED], which inherently limits the impact to the BES. The issue was limited to [REDACTED] Electronic Access Control or Monitoring System (EACMS) associated with [REDACTED]. Software was installed and had a signature file from the time of install, so it was still providing protection from malware known at least to that time. Additionally, the EACMS was protected by firewalls that filtered both incoming and outgoing traffic, which would have limited the network exposure of potential malware. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) reinstalled the antivirus software on the affected server and confirmed the machine is receiving antivirus signatures; and 2) established a monthly reporting process for its EMS support administrators to review the Configuration Management Databases and ensure applicable assets are in the appropriate groups and reporting properly to mitigate for reoccurrence. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022636	CIP-010-2	R3	[REDACTED] (the Entity)	[REDACTED]	09/01/2019	09/25/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 11, 2019, the Entity submitted a Self-Report stating that [REDACTED], it was in noncompliance with CIP-010-2 R3. [REDACTED]</p> <p>The Entity discovered that they failed to conduct a paper or active Vulnerability Assessment (VA) at least once every 15 calendar months.</p> <p>The cause of the noncompliance was that the Entity's controls were inadequate in that they failed to ensure that the company contracted to perform the VA would adhere to the required 15 calendar month interval.</p> <p>The noncompliance began on September 1, 2019, 15 calendar months after the completion of the previous assessment, and ended on September 25, 2019, when the Entity completed a new VA.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the Entity had a valid VA from the previous 15 calendar month interval, and the duration of the missed interval was limited to under one month. The Entity [REDACTED], and the Entity's [REDACTED] contain only [REDACTED] which are not applicable under CIP-010-2 R3 Part 3.1. Therefore, no BES Cyber Systems associated with the Entity's Control Centers were affected by the delayed VA. Additionally, there were no significant outputs or changes identified or implemented as a result of the updated VA. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) performed a new VA; 2) modified its third party contracts to explicitly include the requirement that VAs be performed within 15 calendar months; and 3) designated an individual responsible for ensuring the contractor meets the contractual dates. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021713	CIP-002-5.1a	R2	██████████ (the Entity)	██████████	10/31/2017	04/22/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On June 3, 2019, the Entity submitted a Self-Certification stating that, ██████████, it was in noncompliance with CIP-002-5.1a R2.</p> <p>The Entity reported that it did not review and approve the identifications from CIP-002-5.1a Requirement R1 within the required 15 calendar month interval specified in Requirement R2.</p> <p>The cause of the noncompliance was that the Entity identified that it was lacking internal controls to track and ensure that reviews were conducted per the required timing intervals of CIP-002-5.1a R2.</p> <p>The noncompliance began on October 31, 2017, the last day of the month 15 calendar months following the prior review, and ended on April 22, 2019, when the Entity reviewed and approved the identifications.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity determined that its assets only contain ██████████; therefore, the issue was limited to the review and approval for ██████████ associated specifically to CIP-002-5.1a R1.3. Also, the Entity determined that after subsequent review and approval, there were no changes to its identifications performed under requirement CIP-002-5.1a R1; therefore the risk was limited to a documentation issue only. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) reviewed and had its CIP Senior Manager or delegate approve the identifications; and 2) established new controls requiring an annual review and approval of its CIP-002 documentation which also require additional reviews and approval for changes made to the standard, Entity documentation, or its system outside of the normal annual review cycle. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022632	CIP-011-2	R1	[REDACTED] (the Entity)	[REDACTED]	10/09/2017	07/25/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, [REDACTED], it was in noncompliance with CIP-011-2 R1.</p> <p>The Entity reported that during an internal meeting, it discovered that it failed to enable encryption software for [REDACTED] as per CIP-011-2 requirement R1, Part 1.2.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for protecting and securely handling BCSI during transit and use.</p> <p>The noncompliance began on October 9, 2017, the day in which encryption was disabled, and ended on July 25, 2019, when full use of the encryption software event log encryption was enabled.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the Control Center contains [REDACTED] and the Control Center only controls and monitors assets that contain [REDACTED], which inherently limits the impact to the BES. The back end connection between the Entity and the software exchange services was encrypted via [REDACTED] during the period of issue, thereby protecting the emails containing BCSI while in transit between the Entity and software vendor. The cyber security events such as successful and failed login attempts, malicious code detection, and other cyber security related events are emailed to staff on a real-time basis. The relative risk for emailing these Cyber Security events is less than it would be for data including information which would provide information about the Entity's BCSI [REDACTED]. The software vendor has made publically available [REDACTED] audit reports [REDACTED] that describe cyber security adequacies for the core software product. These [REDACTED] audit assertions, which represents the audit work of others, indicate that there are no known inadequacies related to the software underlay. The risks posed by data in use, and data at rest in the software environment underlay are therefore limited. The software vendor has a data location declaration page that identifies exchange data at rest as being located within the United States (US) for US entities. This assertion limits the risk of BCSI data residing outside the jurisdictional control of the entity and of the ERO Enterprise. The software exchange service within the software vendor is primarily a data store with email processing capabilities, and the risks posed by the data in use and data at rest states would be limited. No harm is known to have occurred.</p> <p>The Entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) resumed full use of encryption program; 2) provided remedial training on internal policy regarding encryption to [REDACTED]; and 3) updated process where [REDACTED] will consult with a [REDACTED] for any further actions on encryption subscription service; 4) instructed the Entity's NERC team to periodically check the event log encryption; and 5) designated responsibility to the Entity's [REDACTED] for updating the encryption software subscription in a timely manner. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022427	CIP-006-6	R2	<div style="background-color: black; width: 100%; height: 1em; margin-bottom: 2px;"></div> (The Entity)	<div style="background-color: black; width: 100%; height: 1em;"></div>	02/08/2019	02/08/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, [REDACTED], it was in noncompliance with CIP-006-6 R2.</p> <p>The Entity reported that it discovered that two visitors were unescorted within a Physical Security Perimeter (PSP) at [REDACTED] containing [REDACTED]. The two visitors went into a separate office, within the PSP, while the escorts were in the main control room.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for escorting visitors at its generating plant.</p> <p>The noncompliance began on February 8, 2019, when the individuals entered the separate office, and ended five minutes later on February 8, 2019, when the individuals left the PSP.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the duration of the issue was limited to five minutes and was limited to one PSP. Also, the issue was limited to two individuals who were employees of the Entity, had completed required cyber security training, and had updated Personnel Risk Assessments on file. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) determined that the two unescorted individuals left the PSP; and 2) reinforced through additional communication its procedure to not allow visitors in the PSP at [REDACTED] unless it is possible for the authorized employees to escort the visitors properly. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2020022823	CIP-004-6	R5	[REDACTED] (the Entity)	[REDACTED]	05/02/2019	05/04/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 17, 2020, the Entity submitted a Self-Log stating that, [REDACTED], it was in noncompliance with CIP-004-6 R5.</p> <p>The Entity reported that a contractor termination request was entered into its access management system, and due to an error in the system, the termination action was marked complete prior to all actions being completed. As a result, the contractor's access to a BES Cyber System Information (BCSI) repository was not revoked until three days after it was required by the standard.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process due to a failure in its automated system.</p> <p>The noncompliance began on May 2, 2019, which was one day after the end of the day following the termination date, and ended on May 4, 2019, when the contractor's access was revoked, and had a duration of three days.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was minimal because the issue was limited to a single contractor and the duration was three days. Also, the contractor of issue was terminated due to completion of the project, rather than for cause, and this contractor had been current on personnel risk assessments and NERC CIP training. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked the contractor's access to the BCSI repository; 2) implemented a temporary manual process to ensure terminations completed the necessary tasks, including revocation of BCSI repository access; and 3) implemented the permanent automated 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
MRO2020022827	CIP-010-2	R2	[REDACTED] (the Entity)	[REDACTED]	05/13/2019	06/12/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 17, 2020, the Entity submitted a Self-Log stating that, [REDACTED], it was in noncompliance with CIP-010-2 R2.</p> <p>The Entity reported that it failed to monitor [REDACTED] device(s) associated with a [REDACTED] for changes at least once every 35 calendar days.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for monitoring baselines when an individual failed to review the baseline documentation for [REDACTED] baselines.</p> <p>The noncompliance began on May 13, 2019, which was 36 days after the previous baseline review, and ended on June 12, 2019, when the Entity reviewed the [REDACTED] baseline.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue was limited to [REDACTED] EACMS and only to ports and not the other four baseline attributes (operating system/firmware, commercially available/open-source applications, custom software, and security patches). Further, the affected [REDACTED], which would have limited the ability to exploit an unauthorized port, had one been opened during the period of issue. Lastly, the duration of the issue was limited to 31 days. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) restored monitoring of the [REDACTED] of issue by reviewing the [REDACTED] baseline; and 2) changed its monitoring process for that device type to include a peer review of the ports baseline documentation. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022125	CIP-005-5	R1	[REDACTED] (the Entity)	[REDACTED]	10/11/2018	08/19/2019	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit [REDACTED], MRO determined that the Entity [REDACTED], was in noncompliance with CIP-005-5 R1. [REDACTED]</p> <p>The Entity failed to update network drawings that had been identified as an Area of Concern (AOC) during the previous audit. The drawings were previously identified as an AOC because they showed the firewall containing Electronic Access Points (EAPs) inside the Electronic Security Perimeter (ESP) and not identified as Protected Cyber Assets (PCAs). Using these drawings, the Entity incorrectly reclassified its firewalls as BES Cyber Assets (BCAs), which put the firewalls on the boundary of the ESP and not fully enclosed within the ESP.</p> <p>The cause of the noncompliance was that Entity failed to accurately represent its network in its CIP-005-5 R1 drawings which led it to misclassify its firewalls as BES Cyber Assets.</p> <p>The noncompliance began on October 11, 2018, when the Entity incorrectly reclassified its firewalls as BCAs, and ended on August 19, 2019, when the firewalls were correctly classified as Electronic Access Control or Monitoring Systems (EACMS).</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal as it was documentation in-nature and was resolved through the reclassification of the asset, rather than implementation of a change to the system. No harm is known to have occurred.</p> <p>The Entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) correctly reclassified its impacted firewalls as EACMS; and 2) updated its network diagram to properly show the firewalls outside 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
MRO2019022130	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	05/31/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 10, 2019, the Entity submitted a Self-Log stating that, [REDACTED], it was in noncompliance with CIP-007-6 R2. The Self-Log contained two instances of noncompliance.</p> <p>In the first instance of noncompliance, the Entity discovered during a patch review that a patch [REDACTED] was installed on a device that is part of the Entity's [REDACTED]. The patch on the software [REDACTED] had not been updated since the device's initial baseline was established because, although the software [REDACTED] had been tracked in the Entity's patch management process, it was not documented as being installed on this particular device. As a result, the version of the patch on the software [REDACTED] installed on the asset [REDACTED] was out of date.</p> <p>This noncompliance began on July 1, 2016, when the standard became enforceable, and ended on March 4, 2019, when the Entity added the patch that should have been applied on the software [REDACTED] to a security patch mitigation plan and began tracking [REDACTED] versions.</p> <p>In the second instance of noncompliance, the Entity discovered, while updating change log information for patches that had been applied, that two patches, [REDACTED], had been assessed as being applicable but had not been installed, nor had they been included in a security patch mitigation plan. The affected BES Cyber Assets (BCAs) were one patch that was applicable to [REDACTED] switches located in substations and [REDACTED] switches located in the Entity's [REDACTED] and a second patch that was applicable to [REDACTED] located in the Entity's [REDACTED].</p> <p>This noncompliance began on May 31, 2019, which was one day after the 35-day window and, ended on the same day, May 31, 2019, when the Entity created two security patch mitigation plans; to address the patches that were not installed.</p> <p>The cause of both instances of noncompliance was a deficiency in the Entity's patch management process. Specifically, for instance one, the Entity's patch management process was deficient in that it did not record sufficient information about the presence of certain software [REDACTED] and the identification of a patch source on all BCAs where the patch was installed. The cause in instance two was the deficiency was the lack of a formalized process for tracking action items following the Entity's security patch review meetings.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk for the first instance was minimal because the software where the patch was to be applied, [REDACTED] was not being used on the device and was therefore "not running". [REDACTED] Also, the device is protected within a Physical Security Perimeter (PSP) and an Electronic Security Perimeter (ESP); access to devices within the ESP requires two-factor authentication, limiting opportunity to access the device where the software had not been updated. The risk for the second instance was minimal because of the Entity's configuration of the affected devices. All services affected by the patches were not used and had been disabled prior to the occurrence of this noncompliance. As a result, any vulnerabilities were inaccessible to an attacker. Also, all affected devices reside inside the Entity's PSPs and are protected by firewalls require two-factor authentication. No harm is known to have occurred.</p> <p>The Entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) added the missing software [REDACTED] to an existing security patch mitigation plan and began tracking it; 2) determined that the device at issue was unable to support (the upgraded version) of the software [REDACTED] and decommissioned the device; and 3) modified the spreadsheet used to track patches to clearly indicate which software resides on [REDACTED]. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) created two security patch mitigation plans, one each for [REDACTED] and [REDACTED]; and 2) developed a method for tracking security patch mitigation plan action items. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Mitigation Completion Date
MRO2019022641	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	5/30/2019	7/09/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, [REDACTED], it was in noncompliance with CIP-010-2 R1.</p> <p>The Entity reported that while performing a review of a [REDACTED] Change Management Document as part of an unrelated request for information from MRO, it discovered that baseline information related to the specific firmware version (R1 Part 1.1.1.) had been deleted from the baseline document. The baseline firmware information was missing for [REDACTED].</p> <p>The noncompliance began on May 30, 2019, when an employee unintentionally deleted the firmware version column, and ended on July 9, 2019, when the baseline document was updated to reflect the firmware version.</p> <p>The cause of the noncompliance was the Entity's process was deficient as it did not include any controls in place to prevent unintentional deletion of the firmware version column.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the resolution of the issue was limited to baseline updating, and the deletion that occurred was limited to the firmware version column; all other necessary baseline information was available. The Entity identified that it had a routine change management process which included an automated review and a manual review of the baseline to trigger change control and configuration management procedures to mitigate the risk to BES. The duration of the noncompliance was limited to 41 days. No harm is known to have occurred.</p> <p>The Entity has compliance history associated with missing baseline updates due to training. However, MRO did not consider this as a factor to elevate the disposition of the instant issue of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the baseline document with correct firmware version; 2) locked firmware version column cells on baseline spreadsheets; and 3) formatted the baseline document to show red cells when the firmware version column cells are blank. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022053	CIP-005-5	R2	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	03/31/2020	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], MRO determined that the Entity, [REDACTED], it was in noncompliance with CIP-005-5 R2.</p> <p>The Entity discovered that for all Interactive Remote Access (IRA) sessions, the Entity failed to implement bi-directional encryption for sessions with the Intermediate System (IS). The Entity's remote access client was implemented to provide encryption from the Cyber Asset initiating IRA to the IS but not implemented to provide encryption from the IS back to the Cyber Asset initiating IRA.</p> <p>The cause of the noncompliance was that the Entity failed to implement its CIP-005-5 R2 process completely by failing to have encryption utilized in both directions for IRA sessions to the IS.</p> <p>The noncompliance began on July 1, 2016, when the CIP Version 5 standards became enforceable, and ended on March 31, 2020, when the Entity updated its authentication agent to enforce encryption in both directions.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the Entity's [REDACTED] only contains [REDACTED] and is only responsible for [REDACTED], which inherently limits the impact to the BES. Encryption was implemented to the ISs, limiting the issue to encryption of data leaving the ISs. Additionally, Virtual Private Network (VPN) connection that is encrypted and uses multi-factor authentication was implemented when initiating an IRA session from the internet limiting the exposure of unencrypted information to the Entity's internal network. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <p>1) updated its authentication agent to allow encryption in both directions for IRA sessions.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019022283	CIP-006-6	R1.	[REDACTED]	[REDACTED]	04/27/2019	04/27/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 30, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it was in noncompliance with CIP-006-6 R1. The entity failed to properly secure a substation vehicle double gate and therefore failed to implement the entity's physical security plan.</p> <p>The substation houses a Medium Impact Physical Security Perimeter (PSP). All BES Cyber Assets at the substation are located in [REDACTED] to gain entry and/or [REDACTED] to gain entry.</p> <p>The noncompliance occurred on April 27, 2019 when a security guard assigned to the entity's substation's vehicle double gate ended his shift and left his post without properly securing the gate. The gate was left unattended and unlocked for approximately four minutes until it was discovered by a [REDACTED]. The [REDACTED] was then alerted about the open entry point and the vehicle double gate was then secured with a station lock, ending the noncompliance.</p> <p>The root cause of this noncompliance was an individual failure of a security guard to adhere to the entity's physical security plan.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not adhering to the [REDACTED] documented physical security plan, which entailed properly securing the vehicle double gate, an unauthorized person or persons could enter the substation via the open gate either on foot or with a vehicle in an attempt to compromise BES Cyber Assets within the substation, which could lead to misoperation or instability.</p> <p>However, the risk was reduced through design and layout of the substation because the vehicle double gate access point is [REDACTED] of the substation's BES Cyber Assets. The substation BES Cyber Assets reside [REDACTED]. The relay houses can only be entered [REDACTED] and control rooms can only be entered [REDACTED].</p> <p>The risk was further reduced because the entity kept continual surveillance on the access point. Video surveillance records indicate no unauthorized access to or from the substation occurred via the unsecured vehicle double gate during the period of noncompliance.</p> <p>The risk was also limited by the short duration of the noncompliance. A total of six minutes elapsed: four minutes passed until the entity's employee discovered the unlocked gate and an additional two minutes until the gate was secured.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and did not determine it to be an aggravating factor.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) secured the gate with a station lock; 2) removed the guard, who failed to properly secure the gate, from the entity's approved personnel list; 3) removed the guard company's dispatcher who failed to escalate the incident to upper management and failed to dispatch relief to the site; 4) underwent a review of guard post duties with the substitute guard dispatched to the site, where the [REDACTED] Security and the Station Operator emphasized the security of the entity's facilities to the new guard; and 5) conducted a safety and security session with every working group in the substation, facilitated by [REDACTED] Security, and held a team discussion reviewing security policies and procedures. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019022284	CIP-011-2	R1.	[REDACTED]	[REDACTED]	11/15/2018	04/16/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>On September 30, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it discovered through an internal compliance investigation that it was in noncompliance with CIP-011-2 R1. (1.2.). The entity failed to implement their procedure for protecting and securely handling Bulk Electric System (BES) Cyber System information (BCSI) in the course of transmission to an external party.</p> <p>The internal compliance investigation was conducted from May 13, 2019 through July 9, 2019 and found two separate instances of this noncompliance involving the same external party receiving an [REDACTED] of information containing BCSI, for the purpose of completing an upgrade project at one of the entity's control centers.</p> <p>This noncompliance started on November 15, 2018 when a contractor's expeditor, working on behalf of the entity, first provided BCSI to an external party and failed to handle the BCSI in a manner consistent with the entity's documented Information Protection Program (IPP). Specifically, the contractor's expeditor granted the external party, consisting of non-entity personnel, access to BCSI without having the external party sign a nondisclosure agreement (NDA) stipulating legal ramifications if the disclosed information was not kept confidential. In the first instance, the external party was granted access to BCSI on November 15, 2018 and had access until December 17, 2018. In the second instance, the external party was granted access to BCSI on March 28, 2019 and had access until April 16, 2019.</p> <p>The BCSI information in both instances consisted of [REDACTED]. The noncompliance ended on April 16, 2019 when the external party returned the BCSI to the contractor's expeditor.</p> <p>The root cause of this noncompliance was inadequate training on the requirements of the entity's documented IPP.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not adhering to the documented IPP, which provided instruction on protecting and securely handling BCSI, the BCSI could be viewed or accessed by malicious actors and used to exploit vulnerabilities.</p> <p>However, the entity reduced the risk of malicious actors utilizing the BCSI. The external party in receipt of the BCSI is a known government agency with a robust program to control access to BCSI while in their possession. The BCSI is [REDACTED]. The entity confirmed access to the BCSI was limited to two individuals from the external party, and the two individuals kept no copies of the BCSI after it was returned to the entity.</p> <p>The BCSI did not include IP addresses or specific locations of the entity's BES Cyber Assets.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and did not determine it to be an aggravating factor.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) performed an extent of condition which consisted of reviewing a list to confirm the two instances of this noncompliance was the only occurrence; 2) confirmed the external party returned and did not keep copies of the BCSI; 3) trained relevant internal personnel on BCSI protection and handling practices; 4) established a procedure to redact BCSI [REDACTED] prior to distribution to external parties; and 5) updated the IPP to clarify BCSI handling requirements when dealing with government agencies. 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021988	CIP-007-6	R5.	[REDACTED]	[REDACTED]	07/01/2016	06/04/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 23, 2019, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it had discovered it was in noncompliance with CIP-007-6 R5 (5.4 and 5.5.2). Specifically, the entity failed to change default passwords and it failed to technically enforce the required minimum password complexity.</p> <p>On March 25, 2019, during a gathering of security evidence (change control evidence) for a failed serial-to-ethernet converter replacement, the entity discovered that the associated account had a default password. The serial-to-ethernet converter’s password was not changed when five serial-to-ethernet converters were installed on September 20, 2016 and the passwords were not added to the password change document. The entity responded with a review of all entity assets for compliance with CIP-007-6 R5.4. The investigation discovered [REDACTED] Cyber Assets that failed to comply. Of this group, [REDACTED] of the assets were BES Cyber Assets and [REDACTED] were Protected Cyber Assets.</p> <p>The investigation also discovered that the entity was in noncompliance with CIP-007-6 R5.5.2. The entity discovered that [REDACTED] assets did not meet the minimum password complexity that is the lesser of three or more different types of characters. The [REDACTED] assets were BES Cyber Assets. There is no overlap between the assets that had passwords that did not meet the minimum complexity requirements and the ones that did not have default passwords changed.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable. The noncompliance ended on June 4, 2019, when the entity changed all the default passwords and enforced the appropriate complexity.</p> <p>The root cause of this noncompliance was a lack of training and awareness. Field personnel interpreted the standard such that changing a first level password was sufficient to protect the other associated password levels.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to change default passwords malicious actors could potentially utilize default passwords to gain access. However, there were multiple layers of defense, both physical and cyber to protect BES Cyber Systems (all Medium Impact) and their associated PCAs. Each of the substations that houses the BES Cyber Assets and PCAs has physical security in the form of a [REDACTED]. There is also a [REDACTED]. The entity monitored for unauthorized access and kept logs of anyone entering the [REDACTED] and had alarms in place to respond to any unauthorized access detected. Additionally, the BCAs and PCAs were included on the asset inventory and being monitored appropriately.</p> <p>For all but [REDACTED] of the assets involved, the risk was reduced by layers of password protection. Prior to reaching the access level where default passwords were left in place for these assets, users were required to provide authentication with an [REDACTED]. Also, for all stations but one, the assets had no external routable connectivity (ERC), mitigating the impact of possible inappropriate access through a default password to any single asset. The BES Cyber System with ERC has [REDACTED], and access requires the use of an [REDACTED].</p> <p>To access the serial-to-ethernet converter, a user must [REDACTED]. Once inside the [REDACTED]. A user must first [REDACTED]. The converter is [REDACTED] Cyber Assets with its own password controls.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity’s compliance history and determined that the entity has relevant compliance history. However, NPCC did not consider the entity’s compliance history as an aggravating factor because the prior noncompliance involved different assets and the mitigation would not have prevented this noncompliance. Additionally, both the prior noncompliance and the current instances of noncompliance were promptly self-reported upon discovery and mitigated.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) changed known default passwords, per Cyber Asset capability on all affected cyber assets; 2) updated change control document to include the serial-to-ethernet converter as part of the password changes; 					

	3) reviewed CIP-007-6 R5 requirements with [REDACTED] managers, supervisors, and contractors; and 4) changed the default passwords to include minimum password complexity on all affected 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
NPCC2019022390	CIP-004-6	R2.	[REDACTED]	[REDACTED]	02/01/2018	07/17/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>On October 17, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it was in noncompliance with CIP-004-6 R2 (2.3). The entity failed to require completion of a cyber security training program appropriate to individual roles, functions, or responsibilities at least once every 15 calendar months.</p> <p>The entity discovered the noncompliance on July 16, 2019 while conducting a monthly training date verification. There are two training modules required for employees with NERC CIP cyber access and unescorted physical access, Module 1 and Module 2. The modules together cover the training topics set forth in CIP-004-6 R2.1.1 through R2.1.9. This noncompliance started on February 1, 2018 when five of the entity's employees exceeded the 15-month period to complete NERC CIP Training (Module 2).</p> <p>The five individuals initially completed both Module 1 and Module 2 training. This granted the five individuals NERC CIP cyber access and unescorted physical access to Medium Impact BES Cyber Assets (BCAs) and authorized administrative access to BCAs and Protected Cyber Assets (PCAs), which included [REDACTED]. The entity reviewed the individuals' training as part of the incident analysis and found that while all five individuals went on to meet the 15-month re-training requirement for Module 1, they did not meet this requirement for Module 2. The five employees' access privileges continued after they failed to complete the Module 2 training. The noncompliance ended on July 17, 2019 when the entity had the employees complete the lapsed Module 2 training.</p> <p>The root cause of this noncompliance was deficient internal controls to verify that individuals had the training required for their access privileges. The entity verified employees' completion of Module 1 and Module 2 training through receipt of a workbook consisting of five sheets. One sheet of the workbook was supposed to list all users but had not been updated and therefore was not accurate. Two other sheets of the workbook, one sheet listing two groups of users, should have been combined and/or read as one sheet but instructions were not conveyed to the entity.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. An entity's failure to complete the required training of Part 2.1 at least once every 15 calendar months creates the risk of personnel having access to the BES Cyber Systems without full understanding of the responsibilities and risks associated with their access privileges.</p> <p>The entity reduced the risk of mishandling information leading to compromise of the BES because the employees did have initial training on handling such information. Although the employees' authorized access required two training modules and they were only current on Module 1, the five individuals had taken both Module 1 and Module 2 prior to receiving their authorized access and had re-taken training within every 15 month calendar year period up until the period of noncompliance. All the employees were in good standing and did not delay in taking the Module 2 training upon notification by the entity.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and did not determine it to be an aggravating factor.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed a review of the five employees' training; 2) had the five employees complete the Module 2 training; 3) changed its cyber access report so that all users will be compiled into a single spreadsheet; 4) ensured a standard form was created by [REDACTED]; 5) provided the standard form to [REDACTED] to complete and submit with a current list of all individuals with authorized cyber 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
NPCC2019021173	CIP-003-3	R1.	[REDACTED]	[REDACTED]	04/05/2014	11/03/2017	On-site Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED] NPCC determined that [REDACTED] (the entity), as a [REDACTED] was in noncompliance with CIP-003-3 R1 (R1.3). The entity failed to complete an annual review and approval of its cyber security policies by its CIP Senior Manager.</p> <p>This noncompliance stretched across multiple versions of the CIP-003 Reliability Standard. This noncompliance started on April 5, 2014, under CIP-003-3, when the entity first failed to have authorized staff signing the approval of cyber security policies. This noncompliance ended on November 3, 2017, under CIP-003-6, when the CIP Senior Manager reviewed and approved the cyber security policies.</p> <p>NPCC determined that during the period of noncompliance, the entity had many different senior managers and delegates. During the effective period of CIP Version 3 (April 2014 through June 2016), the entity had several different assigned senior managers and two senior manager delegates. For the effective audit period of CIP Version 5 ([REDACTED]), the entity had four individuals designated as CIP Senior Manager delegates.</p> <p>The entity was unable to demonstrate that the assigned senior managers (for CIP-003-3) or the CIP Senior Managers (for CIP-003-6), or any of the designated delegates, approved the 19 cyber security policy documents that addressed CIP-003-3 R1.3. Each of the policy documents listed various authors, reviewers, and approvers that were not assigned senior managers or CIP Senior Managers. The [REDACTED] signed off on each of the supporting documents instead.</p> <p>The root cause of this noncompliance was a misunderstanding of the requirements of the standard. The entity erroneously believed that the CIP Senior Manager only had to sign off on the overarching Cyber Security Policy.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, failure to have a senior manager, or CIP Senior Manager, approve of cyber security policies could result in inadequate or non-existent cyber security controls increasing the likelihood of a deficient security posture.</p> <p>However, the risk was reduced because the entity was reviewing the cyber security policies but only had CIP Senior Managers providing reviews on the overarching policies, not the supporting documents. The wrong personnel (the [REDACTED]) signed off on supporting documents and the documents appear to have gone through multiple reviews. Although the [REDACTED] is not the required personnel to provide review and approval, their signature provides evidence of executive level managerial review and responsibility.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no relevant prior instance of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) obtained CIP Senior Manager approval of CIP-003-6 R1 policies; and 2) updated the documentation to explicitly list the CIP Senior Manager as part of the annual review in the Cyber Security Policies. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021175	CIP-010-2	R1.	[REDACTED]	[REDACTED]	07/01/2016	05/23/2018	On-site Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>During a Compliance Audit conducted from [REDACTED] NPCC determined that [REDACTED] (the entity), as a [REDACTED] it was in noncompliance with CIP-010-2 R1 (1.1.4). Specifically, the entity failed to include logical network accessible ports within the baseline configuration.</p> <p>NPCC initially discovered five Electronic Access Control and Monitoring (EACMS) devices without logical network accessible ports within the baseline configuration. The entity reviewed all EACMS devices as an extent of condition and discovered that in total, 17 EACMS devices were lacking the logical network accessible ports in their baseline configurations. The 17 EACMS devices are associated with High Impact BES Cyber Systems.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable. The noncompliance ended on May 23, 2018, when baseline configuration monitoring software was changed to document all logical network accessible port numbers.</p> <p>The root cause of this noncompliance was a failure to configure the baseline monitoring software. It was configured to capture running services but did not provide the ports associated with the service.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The failure to maintain a complete configuration baseline has the potential to affect the reliability of the BPS by providing an opportunity for unauthorized and undetected modifications to be made to applicable Bulk Electric System (BES) Cyber Systems, which could introduce system instability or affect the functionality of such systems.</p> <p>The entity reduced the risk by ensuring only appropriate ports were enabled. Security checks performed by the monitoring software verified that only authorized ports and services were enabled on the 17 EACMS. All EACMS devices had rules for inbound and outbound traffic to protect the Electronic Security Perimeter (ESP). Passwords had been changed from defaults and met length and complexity requirements, and, despite the failure to document network accessible ports, the baseline configurations were still monitored by the EACMS and would alert personnel of any changes.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there was no prior relevant history.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) configured the monitoring software to document any logical network accessible ports for all 17 devices; and 2) updated the CIP-007 R1 and CIP-010 R1 documentation. 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021176	CIP-010-2	R1.	[REDACTED]	[REDACTED]	11/18/2016	06/26/2017	On-site Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED] NPCC determined that [REDACTED] (the entity), as a [REDACTED] was in noncompliance with CIP-010-2 R1. (1.1.1). The entity failed to develop baselines configuration that included device firmware.</p> <p>During a data request associated with the audit, the entity discovered that a spreadsheet used to track the baselines of two Physical Access Controls Systems (PACS) security panels did not contain the devices’ firmware. These PACS are associated with High Impact BES Cyber Systems.</p> <p>This noncompliance began on November 18, 2016, when the entity installed new security panels and failed to create a baseline document that included device firmware. The noncompliance ended on June 26, 2017, when the security panel baseline spreadsheet was updated with the current firmware version.</p> <p>The root cause of this noncompliance was a gap in the change control checklist. Specifically, change control has a checklist to update documentation but did not specifically include a requirement for actual verification of the baseline configuration.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to develop baseline configurations with firmware included could have created difficulties monitoring changes to the device firmware.</p> <p>However, the entity reduced the risk because all PACS are installed within a PSP and any unescorted access to the PSP requires CIP training, Personnel Risk Assessments (PRAs) and authorization. The PACS [REDACTED]. The [REDACTED] to the PACS server. There is no [REDACTED].</p> <p>The firmware version of the two security panels has not changed since the security panels were installed.</p> <p>Finally, the default passwords on the security panels have been changed and the passwords on the panel are changed at least every 15 months. Before being granted an account to access the panels, staff must complete a PRA, CIP training and be granted authorization.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the baseline configuration spreadsheet with the current firmware version; 2) completed an extent of condition on all PACS security panels and found no other issues; 3) set up a periodic control to review security panel baseline configurations on a monthly basis; and 4) updated security test plan to include a signoff of CIP-010-2 R1.1 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
NPCC2019021177	CIP-010-2	R3.	[REDACTED]	[REDACTED]	07/19/2016	10/20/2017	On-site Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>During a Compliance Audit conducted from [REDACTED] NPCC determined that [REDACTED] (the entity), as a [REDACTED] was in noncompliance with CIP-010-2 R3 (3.3). The entity failed to perform an active vulnerability assessment of one new Protected Cyber Asset (PCA) prior to adding it to a High Impact BES Cyber System.</p> <p>NPCC discovered that a PCA was added on July 1, 2016 as part of the CIP Version 5 transition. This PCA provides additional vulnerability scanning capabilities for the Energy Management System (EMS) network. The PCA is a device profiler and when the entity installed the device profiler, other device profilers were already in place on the EMS network. The entity believed an active vulnerability assessment for the new profiler was not required because other device profilers were already on the network. The device profiler was not a like replacement of the same type of Cyber Asset and required an active vulnerability assessment.</p> <p>This noncompliance started on July 19, 2016, when the entity activated the PCA without performing an active vulnerability assessment. The noncompliance ended on October 20, 2017, when the entity performed the active vulnerability assessment.</p> <p>The root cause of this noncompliance was a misinterpretation of the Reliability Standard and an insufficient procedure. The entity believed that a vulnerability assessment was not required because other similar assets were already on the network and the change control process in place did not explicitly require assessments for all replacement devices.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The potential risk to placing a PCA in production prior to performing a cyber-vulnerability assessment is that an entity may unknowingly place a vulnerable PCA into a protected environment and the PCA or other connected Cyber Assets could be compromised.</p> <p>The risk was reduced through electronic and physical controls. The PCA is a vulnerability scanning appliance that discovers and assesses assets installed on the EMS network. The PCA does not have access to make changes to BES Cyber Assets or their associated EACMS/PCAs. Personnel with either physical or cyber access were authorized and physical security controls were in place for those without authorization. Passwords for the PCA met length and complexity requirements and were changed from defaults. Finally, the PCA was monitored for any changes through documented baseline configurations.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed an extent of condition; 2) completed the missed active vulnerability assessment for the device profiler; and 3) revised the change control process to require an active vulnerability assessment for new and replacement devices. 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021619	CIP-004-6	R2.	[REDACTED]	[REDACTED]	4/1/2019	04/08/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>On May 24, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] it was in noncompliance with CIP-004-6 R2 (2.3). The entity failed to complete the required NERC CIP Training within 15 calendar months for one employee.</p> <p>On April 8, 2019, during a monthly training date verification, the entity discovered one employee had failed to complete their required NERC CIP Training within the required 15-month timeframe. Upon discovery of the issue, access was immediately revoked.</p> <p>This noncompliance started on April 1, 2019, when the employee failed to complete training within the required 15 months, and ended on April 8, 2019, when the entity provided the mandatory training to the employee.</p> <p>The root cause of this noncompliance was an insufficient procedure and weak internal controls to ensure training was completed on time.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, failing to complete mandatory NERC CIP training could result in the individual mishandling information or failing to follow an entity's current documented processes when utilizing electronic or physical access.</p> <p>However, the risk was limited because the employee still has a legitimate business need to access the NERC CIP Physical Security Perimeter (PSPs) and the employee had a current Personnel Risk Assessment (PRA). The duration of the noncompliance was short indicating other effective controls operated as intended, such as the monthly training date verification. The noncompliance lasted 8 days before being discovered and promptly mitigated.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) revoked access until training was completed; 2) had the employee complete the required training and access was restored; and 3) updated the CIP Training and PRA Access procedure to set up calendar alerts to revoke access "1-2 weeks" prior to the expiration of the training dates, if they are not already completed and to ensure mandatory training is completed within the required timeframe. 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019022285	CIP-007-6	R2.	[REDACTED]	[REDACTED]	05/27/2019	05/29/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 30, 2019, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-007-6 R2. (2.2.) The entity failed to evaluate a security patch within 35 days.</p> <p>The entity discovered the issue during a weekly [REDACTED]. The overdue patch was discovered through a patching reconciliation report that identifies all security patches that need to be evaluated.</p> <p>On April 22, 2019, the entity's authoritative patching source detected that a newer [REDACTED] version was available on the backup and recovery software of seven servers, which is treated by the entity as a patch. The entity did not document that it had evaluated the patch for applicability on the affected devices within 35 calendar days of being released from the source. It was discovered that, when the patch was released, an individual had determined that it could not be applied because the newer [REDACTED] version was not supported by the backup and recovery software. However, the individual did not open a patch ticket to document this evaluation as required until it was flagged in a [REDACTED] weekly meeting on May 29, 2019, 37 days after the patch was released.</p> <p>This noncompliance started on May 27, 2019 when the entity failed to evaluate a security patch within 35 calendar days. The noncompliance ended two days later, on May 29, 2019, when the entity discovered the issue and evaluated the patch.</p> <p>The root cause of this noncompliance was a failure by the individual who evaluated the patch to document and record their assessment. The individual failed to create a patch ticket at that time, intending to accomplish the task later. The entity's patching program requires a 'patch ticket' to be opened to document the evaluation.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The failure to evaluate and apply patches in a timely manner can expose BES Cyber Systems to cyber security vulnerabilities such as the introduction of malicious code.</p> <p>However, the patch that was released and was not evaluated for 37 days was not supported by the backup and recovery software and therefore could not be applied. Additionally, the entity had layers of varying controls in place that reduced the overall risk and ultimately discovered the noncompliance. These controls included an automated scanning tool that identifies available security patches for review and the reconciliation report that identifies security patches that still need to be evaluated, and the [REDACTED] which reviews outstanding patches and discovered the noncompliance.</p> <p>The risk was further reduced because of the short duration of the noncompliance. The noncompliance lasted two days and the quick discovery is evidence of the entity's strong internal controls that quickly identified and mitigated the issue.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined the entity has relevant compliance history. NPCC determined the entity's compliance history is not aggravating because of different underlying causes and improvements to internal controls that strengthened their procedures.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) verified the scope of the noncompliance was limited to a single patch; 2) evaluated the missed security patch; 3) reinforced expectations for [REDACTED] members at weekly meetings, including the timely assessment of patches; and 4) changed its weekly meeting to specifically review any item on the reconciliation report that has been released for more than 10 days. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019453	CIP-009-6	R3.	[REDACTED]	[REDACTED]	06/01/2017	1/3/2019	On-site Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>During a Compliance Audit conducted from [REDACTED] NPCC determined that [REDACTED] (the entity), as a [REDACTED] was in noncompliance with CIP-009-6 R3 (3.1). The entity failed to document lessons learned, or the absence of lessons learned, within 90 days of a test of its recovery plan.</p> <p>The entity performed a test of its recovery plan per CIP-009-6 R2.1 on March 1, 2017. The entity did not have any lessons learned from that recovery plan test, but failed to document the absence of any lessons learned.</p> <p>This noncompliance began on June 1, 2017, when the entity failed to document the absence of any lessons learned from a test of its recovery plan. The noncompliance ended on January 3, 2019, when the entity updated its procedures to include explicit instructions regarding the documentation of lessons learned including the absence of any lessons learned.</p> <p>The root cause of this noncompliance was a misunderstanding of the Reliability Standard and Requirement and the need to document the absence of lessons learned.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, failing to document lessons learned could lead to repeated mistakes or resulted in the entity not having recovery procedures that reflected all steps necessary to restore operations.</p> <p>However, the risk was reduced because of the lack of any lessons learned from this particular recovery test. The test did not produce any lessons learned and the entity failed to document the absence of lessons learned at the time of the recovery test, or within the subsequent 90 days. This noncompliance can be regarded as one of documentation only. In this case, the failure to annotate the lack of any lessons learned. The failure to document these occurrences did not impact any recovery plans or actual recoveries of Cyber Assets.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no prior relevant instances of noncompliance.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated their procedures to explicitly state that lessons learned must be documented within 90 days of a recovery (test, paper, or actual) including documenting if there are no lessons learned; and 2) added boxes to the end of their server and workstation recovery checklists to record lessons learned even when recording the absence of lessons 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
RFC2019021806	CIP-004-6	R4	[REDACTED]	[REDACTED]	2/15/2019	2/18/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 8, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4.</p> <p>The entity periodically reviews account access and verifies the existence of corresponding authorization records. On March 11, 2019, while completing such a review, the entity discovered an unauthorized test account. The account was on a [REDACTED] that is used to centrally manage [REDACTED] and has routability to all [REDACTED] within the entity's [REDACTED].</p> <p>The entity discovered that the test account was created by an employee who already had administrative rights to the asset. The employee needed to perform a test that would simulate a user with read-only privileges to the system. The employee was unaware that she was required to receive authorization prior to creating the test account.</p> <p>The root cause of this noncompliance is the employee's lack of awareness of the need to receive authorization prior to creating the test account due to ineffective training or controls. This noncompliance involves the management practice of workforce management. Effective workforce management includes, in part, promoting awareness and providing training to staff in support of their roles in maintaining Bulk Electric System reliability and resilience.</p> <p>This noncompliance started on February 15, 2019, when an employee created the unauthorized test account and ended on February 18, 2019, when the entity deleted the test account.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. There is an increased risk of an individual obtaining improper access, misusing access, or failing to adhere to security practices when an entity fails to follow a process to authorize access. Here, the risk was minimized based upon the following facts. The employee who created (and had access to) the test account had previously been authorized to have (and retained) administrator access to the affected system. And, the employee had previously completed the entity's cyber security training. Further, the test account had read-only privileges to the system meaning no changes could be made, and the test did not involve any modification to production data or configurations. There were no impacts to baselines. Lastly, this violation was short in duration (i.e., 4 days) because the test account was deleted shortly after completion of the test. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances involve different causes and issues.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the test account; and 2) developed a new policy for test accounts and coordinated with personnel to ensure awareness and training on the new policy. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022148	CIP-004-6	R3	[REDACTED]	[REDACTED]	6/8/2018	1/13/2020	Self-Report	7/22/2020
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On August 26, 2019, the entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R3.</p> <p>On May 7, 2019, as a result of reviewing a separate incident, the entity discovered that three entity employees had expired Personnel Risk Assessments (PRAs) but still had [REDACTED]. This included authorized unescorted physical access to [REDACTED]. The entity revoked all three employees' access on May 7, 2019. All three incidents involved employees transferring from job positions requiring authorized unescorted physical access and valid PRAs on file at the time of their transfers.</p> <p>The entity uses a set of special requirement values [REDACTED] to trigger PRA renewals every seven years to meet CIP-004-6 R3.5. Employees in a job position with an active [REDACTED] have their PRA expiration dates actively monitored in [REDACTED]. If an individual's PRA is approaching its expiration, [REDACTED] automatically generates a request for a PRA renewal to be initiated by [REDACTED] and upon completion, the PRA completion date is updated in [REDACTED].</p> <p>The first employee transferred from a job position with its [REDACTED] active to a new job position with its [REDACTED] incorrectly set as inactive on July 15, 2017. The manager had worked with a [REDACTED] representative to create the new job position and the [REDACTED] was inadvertently not activated. The new manager completed the entity's [REDACTED] process and elected to retain the employee's existing authorized unescorted physical access. However, the manager did not update the employee's job position [REDACTED] to align with retained authorized unescorted physical access rights in [REDACTED]. The employee's PRA expired on December 5, 2018 and their authorized physical access was revoked on May 7, 2019. As a result, the employee retained access for approximately 153 days with an outdated PRA. During this period, the employee entered the authorized [REDACTED] areas 16 times in the performance of his new job's responsibilities following the PRA's expiration date.</p> <p>The second employee transferred from a job position with its [REDACTED] active to a new job position with its [REDACTED] incorrectly set as inactive on April 22, 2017. The new manager completed [REDACTED] and elected to retain the employee's existing physical access. However, the manager did not update the employee's job position [REDACTED] to align with retained authorized unescorted physical access rights in [REDACTED]. The employee's PRA expired on June 8, 2018 and their authorized unescorted physical access was revoked on May 7, 2019. As a result, the employee retained access for approximately 333 days with an outdated PRA. During this period, the employee did not access or attempt to access any NERC CIP physical areas following the PRA's expiration date.</p> <p>The third employee transferred from a job position with its [REDACTED] active to a new job position with its [REDACTED] incorrectly set as inactive on January 8, 2017. The new manager completed [REDACTED] process and elected to retain the employee's existing physical access. However, the manager inadvertently failed to update the employee's job position [REDACTED] to align with retained physical access rights in [REDACTED]. The employee's PRA expired on February 26, 2019 and their authorized unescorted physical access was revoked on May 7, 2019. As a result, the employee retained access for approximately 70 days with an outdated PRA. During this period, the employee did not access or attempt to access any [REDACTED] areas following the PRA's expiration date.</p> <p>An extent of condition review conducted as part of the Mitigation Plan for this noncompliance identified a fourth entity employee having authorized unescorted physical access without having a valid PRA. The entity discovered this instance while performing an extent of condition review in January 2020 after it submitted the Self-Report on August 26, 2019 and disclosed it as part of its Mitigation Plan. This fourth employee transferred from a job position with its [REDACTED] active to a new job with its [REDACTED] incorrectly set as inactive on June 15, 2019. The manager had worked with an [REDACTED] representative to create the new job position and the [REDACTED] was inadvertently not activated. The new manager completed [REDACTED] process and elected to retain the employee's existing authorized unescorted physical access. However, the manager did not update the employee's job position [REDACTED] to align with retained authorized unescorted physical access rights in [REDACTED]. The employee's PRA expired on November 11, 2019 and their authorized physical access was revoked on January 13, 2020. As a result, the employee retained access for approximately 63 days with an outdated PRA. During this period, the employee entered the authorized [REDACTED] areas three times in the performance of his new job's responsibilities following the PRA's expiration date.</p> <p>This noncompliance involves the management practices of asset and configuration management and work management. The entity did not have an automated process or control to review physical access requirements (valid PRA and current NERC CIP Training) for employee transfers during this noncompliance. That lack of an automated process or control is the root cause of this noncompliance. The entity also did not have an effective control to review [REDACTED] for employees with PRAs that are approaching expiration. Another contributing factor for the third employee was that an employee took on a new position that did not have a [REDACTED] associated with that position and therefore a new PRA was not ordered when his current one expired.</p> <p>This noncompliance started on June 8, 2018, when the first employee's PRA expired and ended on January 13, 2020, when the entity finished revoking [REDACTED] for all four affected employees.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022148	CIP-004-6	R3	[REDACTED]	[REDACTED]	6/8/2018	1/13/2020	Self-Report	7/22/2020
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by allowing these four employees to access NERC CIP systems without up-to-date PRAs is that it provides the opportunity for unqualified individuals to physically or logically access and potentially misuse or compromise Bulk Electric System (BES) Cyber Systems. The risk is minimized because two of the four employees did not access CIP physical locations after their PRAs expired. The other two employees continued to need access after their PRAs expired and continued accessing CIP physical locations in line with their job functions. All four employees at issue had valid NERC CIP Trainings for the duration of the noncompliance. Lastly, all four employees had valid PRAs prior to and at the time of their job transfers. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) revoked physical access for the three employees at issue; 2) spoke with the three employees' respective managers regarding their job position's NERC CIP physical access requirements, their expired PRAs, and their responsibilities under CIP-004; 3) updated the first employee's job position and requested a PRA and authorized physical access; 4) developed a monthly preventative control [REDACTED] where the entity will verify that all personnel with authorized unescorted physical access to [REDACTED] have completed a PRA within the last 7 years, NERC CIP Training within 15 months, and their job position has the correct [REDACTED] setting; 5) reviewed and revised the entity's [REDACTED] and the [REDACTED] instructions; 6) reviewed and revised the entity's Supervisor Training for Managing Employees with [REDACTED]; 7) implemented the preventative control developed in Milestone 4 to verify those individuals have had a PRA within the last 7 years, have completed NERC CIP training within 15 months, and their job position has the correct [REDACTED] setting. The entity also completed an extent of condition for the entity's NERC BES [REDACTED] Impact BES Cyber Systems to identify other potential incidents. One additional instance was found; 8) implemented a new feature in its [REDACTED] that will monitor all personnel with authorized unescorted physical access to its BES Facilities containing NERC BES [REDACTED] and [REDACTED] Impact BES Cyber Systems to verify those individuals had a PRA completed within the last seven years and completed NERC CIP Training within the last 15 months; 9) reviewed and revised its NERC CIP Management Standard for BES Cyber Systems CIP-004 R4, R5 Procedure; 10) implemented a preventative control to include all personnel with authorized NERC CIP unescorted physical access to all BES Facilities containing NERC BES [REDACTED] and [REDACTED] Impact BES Cyber Systems not monitored by [REDACTED] to verify those individuals had a PRA within the last 7 years, have completed NERC CIP training within 15 months, and their job position has the correct [REDACTED] setting; and 11) assigned updated supervisor training to all applicable managers and established a control to verify training completion. <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by July 22, 2020:</p> <ol style="list-style-type: none"> 12) will automate the preventative control developed and implemented as part of Milestones 4 and 7. <p>Additional time is needed to automate the preventative control developed in Milestone 4 and implemented in Milestone 7 because automating that extensive preventative control across this entity requires coordination of many departments and is a difficult and time consuming task.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022255	CIP-010-2	R1	[REDACTED]	[REDACTED]	4/30/2019	5/29/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On September 24, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1.</p> <p>On May 20, 2019, the entity performed a 35-day baseline review, and discovered this noncompliance. Specifically, the entity discovered that it had updated a [REDACTED] on a [REDACTED] classified as a [REDACTED] without a change request. The entity identified this during the review when it found an updated version of a [REDACTED] installed on the [REDACTED] that conflicted with the version on the baseline. The entity inadvertently implemented the change on April 30, 2019.</p> <p>As background, on April 16, 2019, the entity accidentally removed the [REDACTED] from the [REDACTED]. An entity employee was retiring other devices and inadvertently selected the workstation for removal. The [REDACTED] has a [REDACTED] configured to check, on an hourly basis, the status of devices with the [REDACTED] agent installed. As the workstation still had the [REDACTED], it checked-in with the [REDACTED], at which point the [REDACTED] added the [REDACTED] to a [REDACTED]. The [REDACTED] is primarily used as a staging area for [REDACTED] not currently in production until they are assigned a different folder and added to production.</p> <p>On April 30, 2019, the entity ran an [REDACTED] on the [REDACTED] to push out an update to the [REDACTED] to all devices in the folder. While this update was planned for the [REDACTED], the entity installed the update on the [REDACTED] without obtaining the required approvals and before performing the required security testing.</p> <p>The root cause of this noncompliance was a lack of sufficient controls and procedures surrounding the handling of the [REDACTED] within [REDACTED]. Specifically, in this instance the [REDACTED] was accidentally moved from the [REDACTED] to the [REDACTED]. The entity uses the [REDACTED] for [REDACTED]. Since they are [REDACTED], the entity pushes new versions (in this case the new [REDACTED] to the [REDACTED] without the required approvals and security testing the entity uses for [REDACTED]. Therefore, the [REDACTED] incorrectly received the new [REDACTED] without a change request and proper security testing.</p> <p>This noncompliance involves the management practices of asset and configuration management and verification. Asset and configuration management is involved because the entity did not have a control in place to assure that production and non-production assets were properly distinguished and tracked. Verification management is involved because the entity did not have a process to assure that there was a change request prior to implementing an update to the [REDACTED].</p> <p>This noncompliance started on April 30, 2019, when the entity updated the [REDACTED] without a change ticket or required security testing and ended on May 29, 2019, when the entity created and executed the relevant change request with the required security testing.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The potential risk posed by failing to properly authorize a change to a [REDACTED] is that it could introduce potential vulnerabilities into the BPS. The risk here is minimal because both the [REDACTED] and the appropriate [REDACTED] have the same antivirus and scanning security settings which reduces the likelihood that potential vulnerabilities could be introduced because of the unauthorized change to a [REDACTED]. Additionally, the entity identified the noncompliance through an effective internal baseline review. ReliabilityFirst also notes that the change did not adversely impact security controls. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the change control process as it relates to the [REDACTED] which was the affected device in this noncompliance; 2) held a meeting with relevant working groups to identify controls necessary to lower the probability of recurrence; 3) implemented the control identified in the second milestone. Specifically, the entity determined that no tasks were to be assigned at the [REDACTED], to avoid the potential circumstances resulting in this noncompliance; and 4) added a peer review to their change management process for assets which utilize [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
RFC2019022440	CIP-010-2	R1	[REDACTED]	[REDACTED]	8/12/2019	8/30/2019	Self-Report	September 30, 2020
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 30, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1.</p> <p>On August 19, 2019, as a result of a [REDACTED] the entity discovered that eight assets [REDACTED] had a baseline deviation. When the entity compared the deviations to the change request, the entity discovered that the deviations occurred without their change requests being approved. These [REDACTED] are all classified as [REDACTED].</p> <p>Upon further investigation, the entity determined that between August 12, 2019 and August 15, 2019, an entity [REDACTED] put eight assets into production without an approved change request. The [REDACTED] put these assets into production while life-cycling [REDACTED].</p> <p>The commissioning tasks in the entity's [REDACTED] alerts are currently sent to a range of roles in the [REDACTED]. The [REDACTED] usually only receives alerts for the [REDACTED]. When the change tickets for these eight assets were created, the [REDACTED] received the [REDACTED], assumed they were the [REDACTED] and proceeded with implementation. The [REDACTED] is the first task in the [REDACTED] process and is followed by the [REDACTED], then the [REDACTED].</p> <p>This noncompliance involves the management practices of work management and reliability quality management. The root cause of this noncompliance was a lack of procedural controls to ensure that BES Cyber Systems were not placed into the production environment without an approved change request form. Specifically, the workflow within the [REDACTED] ([REDACTED]) assigned the [REDACTED] to an overly broad audience and that created confusion among the [REDACTED].</p> <p>This noncompliance started on August 12, 2019, when the entity placed all eight [REDACTED] into production without completing a change request and ended on August 30, 2019, when the entity completed the change request process.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is making unapproved changes when installing a Cyber Asset, which could introduce vulnerabilities, cause misconfiguration, cause system-to-system miscommunication, and provide a greater threat landscape. The risk here is minimal because the entity completed numerous commissioning tasks prior to the mistaken implementation including commissioning evidence, a [REDACTED], and baselining. The entity's performance of these commissioning tasks reduces the likelihood that these unapproved changes would introduce vulnerabilities, cause misconfiguration, or cause system-to-system miscommunication. ReliabilityFirst also notes that the assets acted as intended when introduced into the production environment. No harm is known to have occurred.</p> <p>Although the current noncompliance involves conduct that is arguably similar to the previous noncompliances, the current noncompliance continues to qualify for compliance exception treatment as it involves high-frequency conduct for which the entity has demonstrated an ability to identify and correct noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) obtained approval for the Change Requests; 2) modified system build procedures and checklist for each [REDACTED] to verify all approvals have occurred in the change request prior to proceeding with implementation. This modification ensures that the [REDACTED] cannot proceed with implementation until after the [REDACTED] and [REDACTED] are completed which will help prevent recurrence. Transmission communicated this change in process via the entity's [REDACTED] meeting, quarterly [REDACTED] Q1, 2020 as well as emails to applicable employees with the updated information; and 3) conducted an extent of condition, where the [REDACTED] reviewed the [REDACTED] within the change management system of record [REDACTED] for on-boarding new assets (completed between 12/1/2018 thru 12/15/2019) to determine if any deviations from the process occurred. Where a deviation is detected an evaluation would be completed to determine if adherence to the process has been met. The entity found no deviations as part of its extent of condition review. <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by September 30, 2020:</p> <ol style="list-style-type: none"> 4) will create a [REDACTED] board that will display approval status for those changes being tracked; and 5) will work with the [REDACTED] to update the process flow so that [REDACTED] are assigned to the [REDACTED] only. They will also update the wording in the email alerts from the creation of [REDACTED] to draw more attention to whom the task is assigned and the purpose of the task. The [REDACTED] will send an awareness email about the modifications to the [REDACTED] process for the commissioning task to applicable employees. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022440	CIP-010-2	R1	[REDACTED]	[REDACTED]	8/12/2019	8/30/2019	Self-Report	September 30, 2020
The entity requires additional time to complete updating the process flow given the number of changes required.								

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022021	CIP-006-6	R1	[REDACTED]	[REDACTED]	6/22/2019	6/22/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 31, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-006-6 R1. More specifically, the entity failed to retain physical access logs for approximately seven hours on June 22, 2019, due to a storage space issue.</p> <p>The entity typically retains logs [REDACTED]</p> <p>On June 22, 2019, at 6:10 a.m., security personnel informed access management personnel that there were issues logging into the entity's Physical Access Control Systems (PACS) application. Personnel at separate locations reported the same issue. During the investigation, the entity discovered that physical access logs were not being stored due to [REDACTED]. The [REDACTED]</p> <p>[REDACTED] In total, the entity lost logs from 2:05 a.m. to 9:02 a.m. on June 22, 2019, for [REDACTED] PACS devices. During this period, the Physical Security Perimeter (PSP) doors and controls remained functional (i.e., only authorized personnel were allowed to enter).</p> <p>The root cause of this noncompliance was [REDACTED]. A contributing factor to the noncompliance was the entity's failure to monitor, and generate alerts for, [REDACTED]. This noncompliance implicates the management practices of asset and configuration management and implementation. Effectively managing and maintaining asset configurations can have a positive impact on the reliability and resilience of the Bulk Electric System (BES). When an entity decides to implement a change, it is important for the organization to invoke internal processes and procedures to ensure that modifications do not compromise the reliability and resilience of the BES.</p> <p>This noncompliance started on June 22, 2019, at 2:05 a.m. when the entity failed to retain physical access logs and ended on June 22, 2019, at 9:02 a.m. when the log retention issue was resolved.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. A failure to retain physical access logs could hinder an entity's ability to investigate and recover from an incident due to a lack of awareness of who was physically present at the time of the incident. Here, the risk was minimized based upon the following facts. First, this noncompliance was short in duration; the entity only lost approximately seven hours of physical access logs. Second, due to the questioning nature of security (and other) personnel, the entity quickly identified, investigated, and resolved the issue. Third, there was a reduced likelihood of an incident during the period of this noncompliance because the entity's PACS system and PSP doors and controls otherwise remained functional. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior violations involved distinct and separate issues and/or different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity completed the following activities. In order to correct the issue, the entity recovered [REDACTED]. In order to prevent recurrence, the entity: (1) reactivated an application [REDACTED]; (2) investigated the need to have [REDACTED]; (3) implemented a [REDACTED]; and (4) [REDACTED].</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021805	CIP-004-6	R4	[REDACTED]	[REDACTED]	2/15/2019	2/18/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 9, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4.</p> <p>The entity periodically reviews account access and verifies the existence of corresponding authorization records. On March 11, 2019, while completing such a review, the entity discovered an unauthorized test account. The account was on a [REDACTED] that is used to centrally manage [REDACTED] and has routability to all [REDACTED] within the entity's [REDACTED].</p> <p>The entity discovered that the test account was created by an employee who already had administrative rights to the asset. The employee needed to perform a test that would simulate a user with read-only privileges to the system. The employee was unaware that she was required to receive authorization prior to creating the test account.</p> <p>The root cause of this noncompliance is the employee's lack of awareness of the need to receive authorization prior to creating the test account, due to ineffective training or controls. This noncompliance involves the management practice of workforce management. Effective workforce management includes, in part, promoting awareness and providing training to staff in support of their roles in maintaining Bulk Electric System reliability and resilience.</p> <p>This noncompliance started on February 15, 2019, when an employee created the unauthorized test account and ended on February 18, 2019, when the entity deleted the test account.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. There is an increased risk of an individual obtaining improper access, misusing access, or failing to adhere to security practices when an entity fails to follow a process to authorize access. Here, the risk was minimized based upon the following facts. The employee who created (and had access to) the test account had previously been authorized to have (and retained) administrator access to the system. And, the employee had previously completed the entity's cyber security training. Further, the test account had read-only privileges to the system meaning it could make no changes, and the test did not involve any modification to production data or configurations. Lastly, this violation was short in duration (i.e., 4 days) because the test account was deleted shortly after completion of the test. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the test account; and 2) developed a new policy for test accounts and coordinated with personnel to ensure awareness and training on the new policy. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022197	CIP-003-6	R1			4/1/2017	4/3/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On September 6, 2019, the entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-003-6 R1. In late July 2019, the entity conducted an internal review of its compliance program with the assistance of a third-party contractor. During this review, the entity discovered that its CIP Senior Manager signed its cyber security policy two days late. The entity determined that the approval was due on April 1, 2017. However, that was a Saturday, and the CIP Senior Manager signed and approved it the next business day, April 3, 2017.</p> <p>The root cause of this noncompliance was the fact that the entity's procedure did not build in extra time for situations where due dates fall on non-business days. This root cause involves the management practice of work management.</p> <p>This noncompliance started on April 1, 2017, when the entity was required to have its CIP Senior Manager sign and approve its cyber security policy, and ended on April 3, 2017, when the CIP Senior Manager actually signed and approved it.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to review and approve of the cyber security policy every 15 calendar months is that the entity may deploy incorrect or outdated security practices. The risk was minimized in this case based on the following factors. First, the CIP Senior Manager signed and approved the cyber security policy only two days late, minimizing the amount of time that any harm could have been realized. Second, the entity identified the issue through an internal review of its compliance program, which demonstrates a commitment to compliance. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) signed and approved the cyber security policy (CIP Senior Manager); and 2) adjusted the expectation of when approvals should take place. Specifically, the entity required that all internal NERC policies and procedures be approved and executed prior to the enforcement date, with language specifying when the policy or procedure becomes effective. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021728	CIP-010-2	R2	[REDACTED]	[REDACTED]	3/14/2019	5/6/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On June 12, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R2. Following an upgrade to address a licensing issue, the baseline-monitoring tool was configured to use an incorrect [REDACTED]. The baseline-monitoring tool was directed to [REDACTED]. As a result, the tool was only capturing the baseline for [REDACTED]. The [REDACTED] was not monitored from February 26, 2019, to May 6, 2019. The last baseline for [REDACTED] was completed on February 6, 2019.</p> <p>The root cause of this noncompliance was a misconfiguration after an upgrade to address a licensing issue. This noncompliance involves the management practice of asset and configuration management. Through effective asset and configuration management, including the implementation of processes, internal controls, and technology designed to minimize the frequency of configuration-related errors, an entity can systematically mitigate certain threats to Bulk Electric System reliability and resilience.</p> <p>This noncompliance started on March 14, 2019, after the entity failed to monitor [REDACTED] for changes to the baseline configuration during a 35-day interval and ended on May 6, 2019, when the entity restored monitoring [REDACTED].</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System based on the following factors. Failing to monitor assets for changes to baseline configurations reduces an entity's ability to prevent and detect unauthorized modifications to said assets. In this case, the risk was minimized based upon the following facts. This noncompliance involved [REDACTED] and was short in duration (i.e., 54 days). This was not a programmatic issue, and the noncompliance involved unique circumstances (i.e., a configuration error after an upgrade to address a licensing issue). Once the communication issue between the baseline-monitoring tool and [REDACTED] was corrected, the entity confirmed that all changes that occurred on the device had been authorized. The entity confirmed that no other assets had a similar issue. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty. The prior noncompliances involved separate and distinct issues as well as different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the [REDACTED] in the baseline monitoring tool with [REDACTED] and inspected the baseline; 2) conducted an extent of condition review [REDACTED] (note: no other issues were found); and 3) developed a process to inspect [REDACTED]. The process includes the method and frequency of inspections. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Mitigation Completion Date
SERC2018018946	CIP-010-2	R3, P3.1	██████████	██████████	7/1/2017	8/8/2017	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, alleged, or confirmed violation.)			<p>On January 4, 2018, the Entity submitted a Self-Report stating that, as a ██████████, it was in noncompliance with CIP-010-2 R3, P3.1. The Entity conducted a vulnerability assessment within the required 15-month timeline per P3.1, but omitted ██████ medium impact Bulk Electric (BES) Cyber Assets from the assessment.</p> <p>Pursuant to the CIP Version 5 Implementation Plan, entities were required to comply with CIP-010-2 R3 within 12 months of the effective date of July 1, 2016. On July 1, 2017, the Entity believed its 2017 paper vulnerability assessment was completed in accordance with the 12-months period. However, on July 18, 2017, while reviewing the 2017 vulnerability assessment results, as part of an established internal control, the Entity identified ██████████ classified as BES Cyber Assets that the Entity inadvertently omitted from the recently completed vulnerability assessment. The Entity overlooked the BCAs due to a clerical error that occurred when it migrated from one inventory management database to another in early 2017. On August 8, 2017, the Entity assessed and included the ██████ BCAs in the 2017 vulnerability assessment.</p> <p>The Entity performed an extent-of-condition review by comparing the CIP Version 5 migrated database’s inventory list with Electronic Security Perimeter drawings and change requests to ensure that it did not overlook any other assets during the 2017 inventory management database migration. The Entity determined this was an isolated incident. The scope of affected facilities included ██████████. Affected Cyber Assets included ██████ medium impact BES Cyber System without External Routable Connectivity and ██████ BES Cyber Assets.</p> <p>The cause of this noncompliance was management oversight for failing to implement an internal control, e.g., a secondary review, to verify all information, including assessment deadlines, associated with vulnerability assessments were properly transferred when the Entity migrated to a new inventory management database.</p> <p>This noncompliance started on July 1, 2017, when the Entity conducted a vulnerability assessment but excluded ██████ BCAs, and ended on August 8, 2017, when the Entity conducted a vulnerability assessment on the ██████ previously missed BCAs.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. By performing a vulnerability assessment of ██████ BCAs at 13 months rather than 12 months, there was a potential introduction of attack vector(s) for malicious threat agents. Malicious actors could deliver malware payload, conduct intelligence gathering or data exfiltration, all leading to adverse effects to the reliability of the BPS. However, in this instance, the vulnerability assessment revealed no new required actions. The ██████ BCAs did not have External Routable Connectivity or dial-up connectivity. Thus, provisioned physical access was required to exploit vulnerabilities. All other applicable CIP cyber security controls were in place. Finally, the Entity changed default passwords to the devices upon site commissioning as required. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined there were no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) performed an extent-of-condition to ensure all missing items had been identified; 2) added the ██████ missing cyber assets to the assessment and performed the vulnerability assessment for those assets; 3) updated its procedure to add a note that states anytime the Entity converts from one database to a new database, a validation will be required; and 4) performed training for applicable staff on the procedure change. 					

SERC Reliability Corporation (SERC)

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
SERC2018019343	CIP-002-5.1	R1	[REDACTED]	[REDACTED]	07/01/2016	03/31/2017	Audit	Complete
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], SERC determined that the Entity, as a [REDACTED], was in noncompliance with CIP-002-5.1 R1. The Entity failed to implement a documented process to identify applicable facilities (i through vi) and categorize them as either high, medium, or low impact Bulk Electric System (BES) Cyber Systems per P1.1 - 1.3.</p> <p>Requirement 1 requires the methodology the Entity used to categorize its identified BES Cyber Systems according to their impact. The Entity did not implement a documented process to identify and categorize its [REDACTED] applicable control center BES Cyber Systems. Instead, the Entity, believing it was not required to implement a documented process, informally identified its applicable facilities and categorized them as low impact BES Cyber Systems. On March 31, 2017, the Entity completed its BES Cyber System categorization with the appropriate approvals designating its [REDACTED] control centers as low impact. The Entity did not identify any BES Cyber Assets in either of the control centers.</p> <p>This noncompliance started on July 1, 2016, when the Entity failed to implement a documented process to identify and categorize its BES Cyber Systems, and ended on March 31, 2017, when the Entity implemented a documented process and completed its BES Cyber System categorization.</p> <p>The cause for this noncompliance was management oversight for failing to implement a practice or policy to ensure its staff properly interpreted the standard and gained familiarity to fully implement the standard. The Entity erroneously believed that it was not required to implement a documented process with the methodology used to categorize its identified BES Cyber Systems according to their impact.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Failure to ensure accurate identification and categorization of applicable BES Cyber Systems according to their impact could lead to a failure to identify, protect, and secure facility BES Cyber Systems, which could jeopardize BPS reliability by rendering the BES Cyber Systems vulnerable to misuse, degradation, or malicious attack. However, the risk was reduced because the Entity identified its applicable facilities and informally categorized them as low impact BES Cyber Systems, which was confirmed on March 31, 2017, when it applied its documented process. Accordingly, the Entity was not required to implement cyber security policies and controls until the subsequent implementation due date of CIP-003-6 R1.2 and R2 on April 1, 2017. No harm is known to have occurred.</p> <p>SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) developed and implemented a documented process for its BES Cyber System identification and categorization; and 2) communicated with all applicable staff on the new 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
SERC2019022119	CIP-004-6	R4	[REDACTED]	[REDACTED]	06/18/2019	09/5/2019	Self-Report	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On August 28, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED] it was in noncompliance with CIP-004-6 R4, P 4.1. The Entity failed to authorize access based on need for two different employees during two separate instances.</p> <p>The first instance occurred on June 18, 2019, when an employee, who was responsible for creating employee badges, granted oneself cardkey access to a Physical Access Control System (PACS) group that provided access to Physical Security Perimeters (PSPs), which housed the high impact Control Center and the Entity’s training center. The employee only had a business need to access the non-PSP areas of the training center and did not have a business need to access the PSP areas. The Entity’s CIP-004-6, R4 process [REDACTED] when requesting PSP level access. The [REDACTED]. The employee believed it was allowed to by-pass the [REDACTED] and grant oneself access to both the NERC PSP and the non-PSP areas because the employee completed the NERC cybersecurity training and the PRA for PSP access. The Entity discovered this instance on June 21, 2019 during a final review of a new quarterly access review report and removed the access that same day. The duration of this instance was three days.</p> <p>The Entity performed an extent-of-condition by reviewing the quarterly access review report for CIP-004 R4.2 and found no additional instances of missing access requests.</p> <p>This noncompliance started on June 18, 2019, when the employee granted oneself the cardkey access, without an approved request, and ended on June 21, 2019, when the Entity removed the cardkey access.</p> <p>The cause of this noncompliance was inadequate training (A6B1). The employee was responsible for creating badges, which allowed access to the system that is used to provision NERC physical access. The employee received training on the functionality of the Entity’s PACS system, however, the employee did not receive specific training on the entity’s CIP-004-6 R4 process, which included the need for a documented authorized approval.</p> <p>The second instance was submitted as a scope expansion on October 16, 2019. The Entity stated that it discovered, on September 5, 2019, that an employee had been provisioned access by an analyst, prior to formal approval, to a BES Cyber System Information (BCSI) storage location on August 19, 2019. The Entity’s process to gain access to the BCSI storage location required two steps [REDACTED]. The latter is required for an individual to receive the generated reports via email from the BCSI storage location application, but also provides direct access to the BCSI storage location when coupled with the [REDACTED] to the environment. The analyst that provisioned the access account believed that it was only providing access for the employee to receive the generated reports via email and did not realize that the employee had been provisioned [REDACTED] for other approved access and, therefore, was able to access the BCSI storage location. The Entity discovered this through a conversation between the manager and the analysts and the Entity removed the access on the same date of discovery. The duration of this instance was 17 days.</p> <p>The Entity performed an extent-of-condition by reviewing all Tripwire application access to ensure no additional accounts had been created and found no additional instances.</p> <p>This noncompliance started on August 19, 2019, when the Entity granted the employee access, without an approved request, and ended on September 5, 2019, when the Entity removed the access.</p> <p>The cause of this noncompliance was management oversight for failing to have adequate process documentation for granting access to the specified BCSI location, specifically, there was a lack of clarity in the Entity’s access management process to emphasize that all user accounts defined to NERC and BCSI assets must have authorization records regardless of usage.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In the first instance, failure to properly manage electronic access could have resulted in unauthorized physical access to a PSP that protected access to the high impact Bulk Electric System (BES) Cyber Systems located in its primary Control Center. However, the risk was reduced as the Entity had implemented [REDACTED] on the security software installed on the PACS and the employee was not provided the necessary personal identification number (PIN) required to gain access. The employee also made no access attempts. In the second instance, failure to properly authorize and manage access to BCSI, could have resulted in exposure of sensitive data or improper handling of the BCSI. While the Entity granted access without formal approval to a BCSI storage location, the employee in question was very low risk: a [REDACTED] that had a bona fide need for the access, a valid PRA, and NERC training. The employee did not access the BCSI storage location before receiving formal approval of the access. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the Entity:</p>					

- | | |
|--|---|
| | <ol style="list-style-type: none">1. removed the respective access for the individuals (instances 1 and 2);2. performed extent-of-condition review of PACS access and CIP-004 R4.2 report (instance 1) and of a report to identify all users that received application emailed reports and created access requests for any that didn't show up in the CIP-004 R4.4 report (instances 2);3. performed root cause analysis (instances 1 and 2);4. identified PACS users with capability to grant NERC access (instance 1);5. provided CIP-004 R4 process training on the roles and responsibilities for all PACS users with capability to grant NERC access (instance 1);6. communicated to all PACS users to submit all (corporate and NERC) access to request system (instance 1);7. provided coaching to [REDACTED] that reinforced the need to go through the formal approval process for granting/removing access to BCSI storage locations (instance 2);8. shared the lesson learned and reinforced the need to go through a formal approval process to all application administrators of physical and electronic NERC access and BCSI access (instance 2);9. updated and communicated the CIP-004 R4-R5 Access Management Process to emphasize that [REDACTED] (i.e., whether it is to facilitate automated reporting versus user interactive access) (instance 2); and10. updated and communicated the process documentation for granting access to the specified BCSI location to grant/remove user access to the BCSI application. |
|--|---|

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2019022135	CIP-007-6	R4, P4.4	[REDACTED]	[REDACTED]	06/26/2019	06/26/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 30, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-007-6 R4, P4.4. The Entity failed to review a sampling of logged events within the required 15 days to identify undetected Cyber Security Incidents for [REDACTED] Electronic Access Control or Monitoring Systems (EACMS) Cyber Assets and [REDACTED] BES Cyber Assets (BCAs).</p> <p>The Entity's practice requires an Analyst to review logged events on Monday mornings, every seven days. In the event the Analyst is out of the office, the Analyst is required to alert the backup subject matter expert (SME) to perform the review. On Monday, June 10, 2019, the Entity's Analyst conducted its review of the logs required for the [REDACTED] manually monitored EACMS and BCAs. Thereafter, the Analyst was out of the office for a number of days and forgot to notify the backup SME to perform the next log review while the Analyst was out of the office. As a result, the Entity did not complete the next review by June 25, 2019, as required. On June 26, 2019, the Analyst returned to work and realized the review was overdue and performed the review at 7:13 a.m. that same day. The review found zero undetected Cyber Security Incidents.</p> <p>The Entity performed an extent-of-condition review of the logs that were manually monitored, the [REDACTED] EACMS and the [REDACTED] BCAs, and found no other instances of noncompliance.</p> <p>This noncompliance started on June 26, 2019, the day after the Entity was required to have completed the required log review, and ended on June 26, 2019, when the Entity completed the required log review.</p> <p>The cause of this noncompliance was management oversight. Management failed to ensure that there was an adequate internal control for proper communication to take place regarding the secondary reviewer in the absence of the primary reviewer.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure to review logs for EACMS and BCAs, within the required timeframe, could allow cyber security events to go undetected increasing the risk of impact to the BCAs and the bulk electric system. The Entity reduced the risk with protective measures in place for gaining access to all of these EACMS and BCAs. For example, the Entity had [REDACTED]. The risk was further reduced as the duration of the noncompliance was under eight hours and the Entity found no undetected Cyber Security Incidents upon the completion of the review. No harm is known to have occurred.</p> <p>SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) reviewed the alert logs for the affected [REDACTED] devices; 2) performed extent-of-condition to determine if any prior reviews passed the 15-day period for the [REDACTED] manually reviewed devices; 3) performed root cause analysis; 4) created a preventative control in Outlook calendar with reminders to conduct log reviews for the primary and backup SMEs; 5) created a preventative control in Outlook calendar with reminders for the manager to help ensure log reviews were completed; and 6) performed a preventative control communication with the primary and backup SMEs about log review coverage. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018020883	CIP-002-5.1	R2, R2.2	[REDACTED]	[REDACTED]	07/01/2016	03/11/2020	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], SERC determined that the Entity, as a [REDACTED] was in noncompliance with CIP-002-5.1 R2.2. The Entity failed to have its [REDACTED] approve the identified and categorized BES Cyber Systems (BCSs) at least once every 15 calendar months.</p> <p>On February 11, 2019, in response to a Request for Information (RFI), the Entity confirmed that it did not have the [REDACTED] approve the identified and categorized BCSs as required by the Standard.</p> <p>This noncompliance started on July 1, 2016, when the Entity did not have the [REDACTED] approve the identified and categorized BCSs, and ended on March 11, 2020, when the [REDACTED] approved the updated list of BCSs</p> <p>The cause for this noncompliance was ineffective resource management for failing to establish a team dedicated to tracking and monitoring NERC compliance.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to obtain evidence of required review and approvals could have left unknown BES Cyber Assets, Physical Access Control Systems, and Electronic Access Control and/or Monitoring Systems undocumented and not properly protected providing potential impact to the reliability of the Bulk Electric System (BES). The Entity reduced this risk as it is required to meet [REDACTED] regulations for all information systems. The [REDACTED] requirements use the same National Institute of Standards and Technology Risk Management Framework that guide the CIP Standards and exceed the NERC requirements for low impact BCSs. The Cyber Assets associated with the Entity's facilities are covered by these [REDACTED] and, therefore, meet them in order to operate. The Cyber Systems at the affected locations all operate under an [REDACTED] obtained by achieving full compliance with this [REDACTED] process. This [REDACTED] process requires a third party validation of all Entity Cyber Systems. The results of this [REDACTED] third party review concludes with a final recommendation for the approval or denial of the [REDACTED] the Cyber Systems. Furthermore, the subsequent review and approval of the BES assets found that no changes had occurred from the initial asset determination. No harm is known to have occurred.</p> <p>SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) reorganized its technical manpower to establish a dedicated team to monitor and track NERC compliance and communicated this to Staff; 2) implemented a secure CIP-002-5 central repository for electronic documentation which it considered sensitive but not classified and communicated the central repository to Staff; 3) completed a review of its CIP-002-5 Assets and the associated Cyber Assets in accordance with its Asset Risk Determination Matrix; and 4) approved the updated list of Cyber Assets by its [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
SERC2018020884	CIP-003-6	R1, P1.2	[REDACTED]	[REDACTED]	04/01/2017	03/11/2020	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], SERC determined that the Entity, as a [REDACTED], and [REDACTED], was in noncompliance with CIP-003-6 R1.2. The Entity failed to obtain [REDACTED] approval at least once every 15 calendar months for its documented cyber security policies.</p> <p>On July 28, 2016, the Entity created the required cyber security policies for its low impact BES Cyber Systems (BCS) but did not obtain approval of the policies by the [REDACTED] within the required 15 months.</p> <p>This noncompliance started on April 1, 2017, when the Entity did not obtain the [REDACTED] approval for its low impact cyber security policies, and ended on March 11, 2020, when the Entity obtained the [REDACTED] approval for its low impact cyber security policies.</p> <p>The cause for this noncompliance was ineffective resource management for failing to establish a team dedicated to tracking and monitoring NERC compliance.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to obtain required approvals could have left the low impact BES Cyber Assets (BCAs) without documented cyber security policies with appropriate plans for properly protecting the Entity's BCAs. The Entity reduced this risk as it is required to meet [REDACTED] regulations for all information systems. The [REDACTED] use the same National Institute of Standards and Technology Risk Management Framework that guide the CIP Standards and exceed the NERC requirements for low impact BCSs. The Cyber Assets associated with the Entity's facilities are covered by these [REDACTED] and, therefore, meet them in order to operate. The Cyber Systems at the affected locations all operate under an [REDACTED] obtained by achieving full compliance with this [REDACTED] process. This [REDACTED] process requires a third party validation of all Entity Cyber Systems. The results of this [REDACTED] third-party review concludes with a final recommendation for the approval or denial of the [REDACTED] the Cyber Systems. Furthermore, the subsequent review and approval of the policies found no significant changes had occurred from the initial creation. No harm is known to have occurred.</p> <p>SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) reorganized its technical manpower to establish a dedicated team to monitor and track NERC compliance and communicated this to staff; 2) implemented a secure CIP-003-6 central repository for electronic documentation, which it considered sensitive but not classified, and communicated the central repository to Staff; 3) reviewed documented cyber security policies on June 20, 2019 and submitted these cyber security policies for approval by the Entity's Cyber [REDACTED]; and 4) approved cyber security policies by its [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
TRE2019022005	CIP-007-6	R3	[REDACTED] (the "Entity")	[REDACTED]	07/01/2016	05/13/2019	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit from [REDACTED] Texas RE determined that the Entity, as a [REDACTED] was in noncompliance with CIP-007-6 R3.3. Specifically, the Entity did not have a documented process for the update of signatures or patterns for the [REDACTED] Cyber Assets.</p> <p>The root cause of the noncompliance was that the Entity mistakenly did not realize that its [REDACTED] was in the scope of CIP version 5 because the responsible employees did not understand how it was configured, and therefore did not finalize the procedure for addressing [REDACTED] signature testing and installation.</p> <p>This noncompliance started on July 1, 2016, when the standard became effective, and ended on May 13, 2019, when the Entity finalized its procedure for testing and installing malicious communication signature updates for its [REDACTED] assets.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's lack of a documented process could have result in a failure to update its signatures on its [REDACTED], which would have increased potential for the execution of malicious code, unknown to the engine, thereby creating potential risk to the BPS. However, the risk was lessened by a few factors. To begin, the Entity provided evidence of updated signatures and patterns on their [REDACTED]; although the Entity did not have a finalized written procedure for [REDACTED] signature updates, the Entity had a draft procedure that its employees followed, and that procedure implemented an on-going practice to update all [REDACTED] signatures in accordance with scheduled update cycles. Additionally, the [REDACTED] would be a supporting method, as the applicable devices do have a method to cover Part 3.1 without the [REDACTED].</p> <p>This Entity [REDACTED]. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To end this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) finalized its procedure for testing and installing malicious communication signature updates for its [REDACTED] assets; and 2) updated its BCA and BCS Identification Methodology procedure to include two additional steps: one step for reviewing functional network diagrams, configurations, etc. with the workgroup responsible for installing, configuring and commissioning the Cyber Asset to determine if it meets any NERC definition for in-scope devices, and one step for the Regional Compliance Officer to perform a tool-assisted independent 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
TRE2019022454	CIP-004-6	R2; R2.1	[REDACTED] (the "Entity")	[REDACTED]	09/17/2019	09/30/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On November 6, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R2. In particular, the Entity reports that one employee was provisioned unescorted physical access into applicable Physical Security Perimeters (PSP) prior to the employee completing the Entity's Cyber Security Training program.</p> <p>The root cause of this noncompliance was a failure to follow documented procedures due to insufficient training or familiarity with documented processes. Access provisioning via the Entity's PACS is normally performed by members of the Entity's IT Compliance department. No members of this department were available and as such the provisioning was performed by the Entity's IT Operations Division Manager. The IT Operations Division Manager authorized and provisioned the access the individual would need without ensuring that the individual had completed all necessary steps in order to be authorized to be provisioned access.</p> <p>This noncompliance started on September 17, 2019, when the employee was provisioned access to the Entity's PSPs, and ended on September 30, 2019, when the employee completed cyber security training.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>Aggravating risk factors as they relate to the Entity:</p> <ul style="list-style-type: none"> • the Entity's system is primarily a [REDACTED]; • the Entity has at least [REDACTED]; • the Entity's [REDACTED]; • the Entity is responsible for independent actions coordinated with its Reliability Coordinator during system restoration; • the Entity owns [REDACTED]; and • the Entity owns or operates [REDACTED] to provide voltage control. <p>Mitigating risk factors as they relate to the Entity:</p> <ul style="list-style-type: none"> • the Entity is not planning on or currently building [REDACTED] in the next three years; • the Entity does not operate [REDACTED]; • the Entity is responsible for less than [REDACTED] and • less than 25% of the Entity's System Operators have less than 5 years of System Operator experience. <p>Mitigating risk factors as they relate to the issue:</p> <ul style="list-style-type: none"> • the duration of the noncompliance was short, lasting 13 days; • the employee was unaware that they had been provisioned access; • the employee did not access any PSPs during the period of noncompliance; and • the employee had a legitimate business need for the provisioned access. <p>No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity took the following actions:</p> <ol style="list-style-type: none"> 1) to end the noncompliance the Entity's employee completed the required training; and 2) to prevent reoccurrence of this noncompliance the Entity updated its access provisioning process to only allow IT Compliance personnel to grant access to PSPs. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020714	CIP-008-5	R3: P3.1.3; P3.2.2	[REDACTED]	[REDACTED]	06/13/2017	09/04/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On November 15, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] it was in potential noncompliance with CIP-008-5 R3.</p> <p>Specifically, between June and August of 2018, with the assistance of a third-party contractor hired to assess the entity's compliance with all applicable CIP Standards and Requirements, the entity discovered two issues related to its Cyber Security Incident response plan (CSIRP) used for all of its High, Medium, and Low Impact Bulk Electric System (BES) Cyber Systems. Regarding the first issue, the entity conducted a tabletop exercise of its CSIRP on March 24, 2017, which resulted in documented lessons learned but they were not communicated timely to persons or groups with an identified role or responsibility in the CSIRP as required by Part 3.1 subpart 3.1.3. Regarding the second issue, on April 13, 2017, the entity updated the roles and responsibilities in the CSIRP but did not communicate timely the update to the relevant personnel as required by Part 3.2 subpart 3.2.2. The first issue began on June 23, 2017, and the second issue began on June 13, 2017, the day after the timeframe to notify the relevant personnel expired, and for both issues ended on September 4, 2018, when the entity completed its 2018 CSIRP test exercise and made the necessary notifications.</p> <p>The root cause of these issues was attributed to an incomplete CSIRP. Specifically, the CSIRP addressed the requirement to make notifications per CIP-008-5 R3.1 and R3.2 however it did not contain sufficient detail to address the capturing of an evidence artifact to document the required notifications.</p>					
Risk Assessment			<p>These issues 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 notify each person or group with a defined role in the CSIRP of the updates based on lessons learned, as well as the changes to the roles or responsibilities in the CSIRP that the entity determined would impact the ability to execute the plan used for its High, Medium, and Low Impact BES Cyber Systems, as required by CIP-008-5 R3, Part 3.1, subpart 3.1.3 and Part 3.2, subpart 3.2.2.</p> <p>Such failure could have resulted in confusion and delays when responding to a Cyber Security Incident. This could have led to a less effective response, possible exacerbation of an event, or damage of evidence required for mitigation and recovery. The resulting response delays could have potentially allowed for the incident to spread to other locations or affect more Cyber Assets; thereby, having a greater overall impact on the entity and the operating BES environment. However, all relevant incident response personnel participated in the 2017 test and were aware of the updates and lessons learned. In addition, these issues were limited to documentation deficiencies because the CSIRP required the notifications to be made but did not address the need to document that the notifications were made. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) conducted a test of its CSIRP in 2018 and notified the identified response personnel of any updates or changes to the CSIRP; 2) updated the CSIRP to include instructions for the documentation of notifications; and 3) updated its notification tasks in its compliance management software with an express requirement to retain evidence that the notification was made. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2020022820	CIP-011-2	R2: P2.2	[REDACTED]	[REDACTED]	5/8/2019	7/17/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On January 24, 2020, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-011-2 R2.</p> <p>Specifically, in November 2019, during a review of BES Cyber Assets (BCAs) which had been removed from service, the entity discovered it had no disposal documentation for [REDACTED] BCA associated with a Medium Impact BES Cyber System (MIBCS) which had been retired during an upgrade at a substation. Upon further investigation, the entity determined that the password-protected BCA had been removed from service in May 2019 by a contract technician that did not follow the established procedure to wipe or reset the password to factory default before being powered down and removed for disposal. The only BES Cyber System Information (BCSI) on the BCA was the password. The BCA was sent off-site to be processed for disposal and was subsequently destroyed, however the BCSI password was not removed per the entity's documented procedures. This issue began on May 8, 2019, when a Cyber Asset was disposed without first removing its BCSI and ended on July 17, 2019, when the Cyber Asset was destroyed by the entity's recycling provider.</p> <p>The cause of the issue was attributed to the lack of a standard checklist for technicians to document the removal of BCSI prior to disposal of a Cyber Asset.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed, prior to disposal of [REDACTED] BCA that contained BCSI password, to take action to prevent the unauthorized retrieval of the BCSI from the BCA as required by CIP-011-2 R2 Part 2.2.</p> <p>Such failure could have resulted in a malicious actor obtaining the BCSI password of the affected BCA and using it to compromise the other Cyber Assets in that substation to affect the BES. However, as compensation, the entity [REDACTED] on the containers that contained the disposed Cyber Asset in route to the recycling facility. Shipments of the entity's scrap metal recycler were sent in [REDACTED], thus minimized the risk of an unauthorized person gaining access to the Cyber Asset prior to destruction. Additionally, each substation utilized a unique set of passwords, which prevented the use of a compromised password from being used on other substations Cyber Assets like the one at issue. Lastly, the entity utilized [REDACTED] to access the substation as verified during the entity's most recent Compliance Audit and a malicious actor would have to defeat [REDACTED] to effectively utilize a compromised relay password. No harm is known to have occurred</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To remediate and mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) verified the team responsible for demolition and removal of Cyber Assets have appropriate training and awareness materials; 2) verified that contracts for demolition and removal of Cyber Assets provide applicable checklists and instructions for BCSI handling; and 3) updated data [REDACTED] to incorporate internal controls to identify missing BCSI checklists. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2020022982	CIP-003-6	R1; P1.2.	[REDACTED]	[REDACTED]	10/01/2019	02/26/2020	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On February 20, 2020, the entity (Entity A) submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-003-6 R1.</p> <p>Specifically, Entity A did not review or obtain CIP Senior Manager approval of its Cyber Security Policy related to [REDACTED] low impact Bulk Electric System (BES) Cyber Systems (LIBCS) at least once every 15 calendar months. In October of 2019, Entity A had reached an agreement in principle between it and another entity (Entity B) to have Entity B assume the CIP-003 compliance obligation for its LIBCS. Since the agreement did not take effect until January 10, 2020, when the agreement was signed, Entity A was still responsible for complying with CIP-003-6 R1 Part1.2. This issue began on October 1, 2019 when the timeframe to review the Cyber Security Policy expired and ended on February 26, 2020, when Entity A's CIP Senior Manager reviewed and approved the Cyber Security Policy.</p> <p>The root cause of the issue was attributed to an individual justifying their actions based on biased evidence. Specifically, the CIP Senior Manager assumed that the agreement with Entity B was already effective because Entity B had knowledge of the agreement, but the agreement was not effective at that time compliance with CIP-003-6 R1, P1.2 was due.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to review and receive CIP Senior Manager approval at least once every 15 calendar months for its documented Cyber Security Policy for its LIBCS as required by CIP-003-6 R1 Part 1.2.</p> <p>Such failure could have resulted in an outdated Cyber Security Policy that did not address new vulnerabilities or risks not addressed in a previous version, which could have reduced Entity A's cyber security posture. Entity A did not have controls in place to detect or prevent this issue; however, this was a documentation deficiency, as Entity A had a Cyber Security Policy in place. Additionally, Entity A was inherently low risk and after transferring compliance responsibility to Entity B, Entity A no longer had assets applicable to CIP-003. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) reviewed and obtained CIP Senior Manager approval of the Cyber Security Policy; and 2) contracted with a private company to help ensure future compliance with applicable CIP Standards. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021791	CIP-003-6	R1: P1.2.			05/01/2018	06/04/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On July 3, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-003-6 R1.</p> <p>Specifically, the entity did not retain evidence that its CIP Senior Manager reviewed and approved its Cyber Security Policy related to its low impact Bulk Electric System (BES) Cyber Systems (LIBCS) at least once every 15 calendar months. During a review conducted by the entity in 2018, the entity determined that its CIP Senior Manager had reviewed four policies associated with its LIBCS but could not locate its approved 2018 Cyber Security Policy. This issue began on May 1, 2018, when the timeframe to review the Cyber Security Policy had expired and ended on June 4, 2019, when the entity reviewed and obtained approval of its Cyber Security Policy from its CIP Senior Manager.</p> <p>The root cause of the issue was attributed to less than adequate internal controls. Specifically, the entity did not have a control in place to verify and document that each policy had been timely reviewed and approved.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to review and obtain CIP Senior Manager approval at least once every 15 calendar months of its Cyber Security Policy for its LIBCS as required by CIP-003-6 R1 Part 1.2.</p> <p>Such failure could have resulted in the entity operating under a Cyber Security Policy that was not guided by the entity's management structure and current operating conditions. This could result in a policy that did not adequately address entity-level risks known to management. Alternatively, the manager could have made decisions that were not aligned with the Cyber Security Policy. Without managerial oversight, the entity's security posture could have been reduced. The entity did not have internal controls in place to detect this issue timely; however, this was a documentation deficiency and the entity had a Cyber Security Plan in place per R2 of CIP-003-6 which conveyed the steps necessary to implement the cyber security controls. Additionally, each of the entity's policy documents, including the Cyber Security Policy, were approved by the CIP Senior Manager in 2017 and no changes were made to them in 2018. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) reviewed and obtained CIP Senior Manager approval of its Cyber Security Policy; 2) implemented a process to obtain CIP Senior Manager approval every 12 calendar months, instead of 15 calendar months; and 3) implemented a spot check to help ensure its policies are approved by its CIP Senior Manager prior to the expiration of the 15 calendar month timeframe. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021696	CIP-002-5.1	R1: P1.1; P1.2; P1.3	[REDACTED]	[REDACTED]	7/1/2016	9/30/2016	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 violation.)			<p>On June 12, 2019, the entity submitted a Self-Report stating that, as a [REDACTED] was in potential noncompliance with CIP-002-5.1 R1.</p> <p>Specifically, the entity (entity A) had a contractual agreement with another entity (entity B) to perform the entity's [REDACTED] and the compliance responsibilities for the associated BES Cyber System (BCS), from [REDACTED]. Due to entity A being [REDACTED], even though the BCS functions and compliance responsibilities were contractually provided by entity B, a potential noncompliance was identified against entity A.</p> <p>During the contractual agreement, entity B failed to implement its documented process to identify an appropriate impact rating for the BES Cyber System(s) [REDACTED] for entity A, located in entity B's Control Center, including backup Control Center and associated data centers, as prescribed by R1.i, for the purposes of Parts 1.1 through 1.3. This issue started on July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on September 30, 2016 when entity A performed the CIP-002-5.1 R1 identifications.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). At the time of the issue, entity B was contractually responsible for [REDACTED] for entity A, utilizing entity B's BCS. The failing of entity B to identify the impact rating of its BCS [REDACTED] resulted in entity B not appropriately implementing protective security measures, commensurate with their impact, which could have led to inadequate or non-existent cyber security controls (CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, and CIP-011-2) and resulted in the compromise or misuse of the BCS.</p> <p>However, as compensation the affected BCS operated by entity B, [REDACTED], would have been classified as a Low Impact BCS (LIBCS) from [REDACTED] during the time of noncompliance. Additionally, entity B implemented several best practices within its network architecture, specifically [REDACTED]. Lastly, the [REDACTED] LIBCS at the [REDACTED] utilized by entity A as the [REDACTED] were appropriately identified and protected, per the applicable CIP Standards and Requirements. No harm is known to have occurred.</p> <p>WECC determined entity A had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, entity A did the following:</p> <p>[REDACTED] re-certification by establishing and certifying its own Control Center to [REDACTED] and took direct and independent responsibility for compliance with all applicable Reliability Standards. All CIP Version 6 policies and procedures, including the entity's documented CIP-002-5.1 identification of the BES Cyber Systems in the entity's Control Center [REDACTED] were reviewed by the Certification team which found no issues. [REDACTED]</p> <p>Entity A continued with the transition to change the location of the Control Center until its completion on [REDACTED]. [REDACTED] No Cyber Assets used by entity B [REDACTED] to entity A, nor did entity A rely upon any entity B Cyber Assets or systems after September 30, 2016.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021697	CIP-002-5.1	R1: P1.1; P1.2; P1.3	[REDACTED]	[REDACTED]	7/1/2016	9/30/2016	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 violation.)			<p>On June 12, 2019, the entity submitted a Self-Report stating that, as a [REDACTED] it was in potential noncompliance with CIP-002-5.1 R1.</p> <p>Specifically, the entity (entity A) had a contractual agreement with another entity (entity B) to perform the entity's [REDACTED] and the compliance responsibilities for the associated BES Cyber System (BCS), from [REDACTED]. Due to entity A being [REDACTED] even though the BCS functions and compliance responsibilities were contractually provided by entity B, a potential noncompliance was identified against entity A.</p> <p>During the contractual agreement, entity B failed to implement its documented process to identify an appropriate impact rating for the BES Cyber System(s) [REDACTED] for entity A, located in entity B's Control Center, including backup Control Center and associated data centers, as prescribed by R1.i, for the purposes of Parts 1.1 through 1.3. This issue started on July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on September 30, 2016 when entity A performed the CIP-002-5.1 R1 identifications.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). At the time of the issue, entity B was contractually responsible for [REDACTED] for entity A, utilizing entity B's BCS. The failing of entity B to identify the impact rating of its BCS [REDACTED] resulted in entity B not appropriately implementing protective security measures, commensurate with their impact, which could have led to inadequate or non-existent cyber security controls (CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, and CIP-011-2) and resulted in the compromise or misuse of the BCS.</p> <p>However, as compensation the affected BCS operated by entity B, [REDACTED], would have been classified as a Low Impact BCS (LIBCS) from [REDACTED] during the time of noncompliance. Additionally, entity B implemented several best practices within its network architecture, specifically [REDACTED]. Lastly, the [REDACTED] LIBCS at the [REDACTED] utilized by entity A as the [REDACTED] were appropriately identified and protected, per the applicable CIP Standards and Requirements. No harm is known to have occurred.</p> <p>WECC determined entity A had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, entity A did the following:</p> <p>[REDACTED] re-certification by establishing and certifying its own Control Center to [REDACTED] and took direct and independent responsibility for compliance with all applicable Reliability Standards. All CIP Version 6 policies and procedures, including the entity's documented CIP-002-5.1 identification of the BES Cyber Systems in the entity's Control Center [REDACTED] were reviewed by the Certification team which found no issues. [REDACTED]</p> <p>Entity A continued with the transition to change the location of the Control Center until its completion on [REDACTED]. [REDACTED] No Cyber Assets used by entity B for the BA function were transferred to entity A, nor did entity A rely upon any entity B Cyber Assets or systems after September 30, 2016.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2020022962	CIP-007-6	R5: P5.6	[REDACTED]	[REDACTED]	3/20/2019	2/4/2020	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On February 25, 2020, the entity submitted a Self-Report stating that, as a [REDACTED] it was in potential noncompliance with CIP-007-6 R5.</p> <p>Specifically, during an annual review of its user and service account passwords, the entity discovered that passwords for [REDACTED] accounts had not been changed within the past 15-calendar months as required by CIP-007-6 R5 P5.6. This issue included [REDACTED] BES Cyber Asset domain account and [REDACTED] user accounts on Physical Access Control Systems (PACS) workstations associated with High Impact BES Cyber Systems (HIBCS) at the entity's Control Center. This issue began on March 20, 2019, when the 15-calendar month timeframe for changing passwords expired and ended on February 4, 2020, when the entity changed the passwords for the accounts at issue.</p> <p>The cause of the issue was attributed to a less than adequate process design. Specifically, the entity's documented system access control process required an annual review of user and service account passwords that had exceeded 365 calendar days. However, because the system-generated report only included accounts with passwords aged over 365 days, not all accounts with passwords that would expire prior to commencement of the next annual review were flagged for action. The issue was limited to the [REDACTED] accounts.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement a documented process to either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months for password-only authentication for interactive user access as required by CIP-007-6 R5 Part 5.6 for [REDACTED] passwords.</p> <p>Failure to change a password on PACS workstations could have resulted in a malicious actor using a brute force attack or other method to obtain the password and subsequently attempt to physically control doors to the Physical Security Perimeter at the entity's primary Control Center. A failure to change a password of the BES Cyber Asset domain account could have allowed a malicious actor to obtain the password to the account and process information regarding the entity's Energy Management System. However, none of the accounts were logged into after the passwords expired. Further, the had entity implemented an Electronic Security Perimeter (ESP) with more than one firewall between the ESP and the corporate network. Finally, the user accounts associated with the PACS were local accounts and provided access to a single host. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for aggravating the disposition treatment. Specifically, the prior instances of noncompliance had a distinct root cause and fact pattern, of which the mitigation activities would not have prevented this issue and are not indicative of a systemic or programmatic issue.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) updated the passwords of the user accounts at issue; 2) increased the frequency of its password review to quarterly and updated its documented process accordingly; 3) communicated updated procedural changes to relevant employees; and 4) implemented monthly reminders to change passwords as a preventative control. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2020023383	CIP-010-2	R1: P1.4, subpart 1.4.1.	[REDACTED]	[REDACTED]	10/6/2019	10/31/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On January 30, 2020, the entity submitted a Self-Log stating that, as a [REDACTED], it was in potential noncompliance with CIP-010-2 R1.</p> <p>Specifically, the entity did not determine the cyber security controls that could have been impacted prior to implementing a change to the existing baseline configuration as required by CIP-010-2 R1 Part 1.4, subpart 1.4.1. The entity updated its [REDACTED] for its virtual machines; the update to the [REDACTED] unexpectedly pushed a software update to [REDACTED] Electronic Access and Monitoring Systems (EACMS) associated with the entity's High Impact BES Cyber System (HIBCS) before the entity had determined if any of the cyber security controls in CIP-005 and CIP-007 would be affected by the baseline configuration change. This issue began on October 6, 2019, when the configuration change was implemented without determining if cyber security controls would be impacted and ended on October 31, 2019, when the entity confirmed that the security controls were not negatively impacted by the configuration change.</p> <p>The root cause of the issue was attributed to a knowledge-based error as the entity made an incorrect assumption that two or more facts did not correlate. At the time, the entity's centralized management utility system did not segment the corporate virtual machines from the EACMS associated with the HIBCS. When the entity updated its corporate servers, it did not anticipate the impact on its EACMS.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented configuration change management process for a change that deviated from the existing baseline configuration, to determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change prior to the change as required by CIP-010-2 R1 Part 1.4 subpart 1.4.1. for one configuration change on [REDACTED] EACMS.</p> <p>Failure to determine the impact a change could have had on the cyber security controls in CIP-005 and CIP-007 could have resulted in the entity's EACMS software change being incompatible or inoperable with other dependent systems, thereby potentially diminishing the functionality of the EACMS. However, the configuration change had been authorized, approved for installation, and all other change management procedures had been properly followed. Further, the entity conducted testing and determined that no cyber security controls were impacted because of the configuration change. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) conducted cyber security controls testing for the configuration change; 2) deployed a centralized management utility system to segment Cyber Assets associated with the HIBCS from corporate virtual machines; and 3) communicated the new system to relevant employees. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018855	CIP-009-3	R1	[REDACTED]	[REDACTED]	09/08/2015	08/31/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On December 18, 2017, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-009-3 R1. Specifically, at the time the potential noncompliance began, the entity was using a single recovery plan for [REDACTED] Cyber Assets. In this instance, the entity did not annually review its recovery plan applicable to those Cyber Assets. This issue began on September 8, 2015, when the annual review timeframe expired and ended on August 31, 2017, when a new recovery plan process document was created, reviewed and updated.</p> <p>The root cause of the issue was attributed to a lack of management oversight. Specifically, after the entity [REDACTED], the entity did not provide for management oversight to verify that the recovery plan was annually reviewed.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to annually review its recovery plan as required by CIP-009-3 R1.</p> <p>Such failure resulted in the recovery plan being out-of-date and inaccurate which could have resulted in slower recovery times for the [REDACTED] Cyber Assets or misinformation being disseminated between recovery personnel. However, as compensation, when the recovery plan was reviewed, the entity had a limited number of revisions. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) implemented a new series of recovery plans specific to certain Cyber Assets; 2) assigned responsibility for the annual review of the recovery plans to a single Vice President; and 3) provided CIP-009 training to its recovery personnel to include applicability, rationale, overview of conditions, and evidence retention. <p>WECC has verified the completion of all mitigation activity.</p>					

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	MRO2019022523			Yes	Yes					Yes				Category 2 – 12: 2 years
2	MRO2019022526			Yes	Yes					Yes				Category 2 – 12: 2 years
3	MRO2019022527			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
4	MRO2020022757			Yes	Yes					Yes				Category 2 – 12: 3 years
5	MRO2020022758			Yes	Yes									Category 2 – 12: 3 years
6	MRO2019022638	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
7	MRO2020022811			Yes	Yes									Category 2 – 12: 2 years
8	MRO2019022438	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
9	MRO2020022743			Yes	Yes					Yes				Category 2 – 12: 2 years
10	MRO2019022352		Yes	Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 3 years
11	MRO2019022616	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 years
12	NPCC2019021345	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
13	NPCC2019021414	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
14	RFC2019021720	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 years
15	RFC2019021927	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 years
16	RFC2019021784	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
17	RFC2016016472	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 years
18	RFC2018018928	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
19	RFC2017016727	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
20	RFC2017018251	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)
21	RFC2017018531	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 years
22	RFC2016016471	Yes		Yes	Yes	Yes	Yes							Category 1: 3 years; Category 2 – 12: 2 years
23	RFC2017017784	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
24	RFC2018019427	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 years
25	RFC2018019979	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 years
26	RFC2017017783	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 years
27	RFC2018019182	Yes		Yes	Yes		Yes	Yes		Yes				Category 1: 3 years; Category 2 – 12: 2 years
28	RFC2019021929	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
29	RFC2019021928			Yes	Yes									Category 2 – 12: 2 years
30	RFC2019021718	Yes	Yes	Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 years
31	RFC2019021808			Yes	Yes				Yes					Category 2 – 12: 2 years
32	RFC2019021197	Yes		Yes	Yes	Yes								Category 1: 3 years; Category 2 – 12: 2 years
33	RFC2019021194	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
34	SERC2018020880			Yes	Yes				Yes					Category 2 – 12: 2 years
35	SERC2018020881			Yes	Yes				Yes					Category 2 – 12: 2 years
36	SERC2019021386			Yes	Yes				Yes	Yes				Category 2 – 12: 2 years
37	SERC2019021387			Yes	Yes				Yes	Yes				Category 2 – 12: 2 years
38	SERC2019021471			Yes	Yes				Yes	Yes				Category 2 – 12: 2 years
39	SERC2019021518			Yes	Yes					Yes				Category 2 – 12: 2 years
40	SERC2018020051			Yes	Yes									Category 2 – 12: 2 years
41	SERC2019021419			Yes	Yes		Yes			Yes				Category 2 – 12: 2 years
42	SERC2018020333			Yes	Yes				Yes	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)
43	TRE2018020581			Yes	Yes	Yes			Yes					Category 1: 3 years; Category 2 – 12: 2 year
44	TRE2017018210			Yes	Yes	Yes				Yes				Category 1: 3 years; Category 2 – 12: 2 year
45	TRE2020022980			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
46	TRE2019022373			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
47	TRE2018020246	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
48	TRE2019022653	Yes		Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 year
49	WECC2018020731			Yes	Yes									Category 2 – 12: 2 years
50	WECC2019021190			Yes	Yes									Category 2 – 12: 2 years
51	WECC2020022801			Yes	Yes									Category 2 – 12: 2 years
52	WECC2020022802			Yes	Yes									Category 2 – 12: 2 years
53	WECC2020022800			Yes	Yes									Category 2 – 12: 2 years
54	WECC2020022892			Yes	Yes									Category 2 – 12: 2 years
55	WECC2018020568			Yes	Yes						Yes			Category 2 – 12: 2 years
56	WECC2019022141			Yes	Yes					Yes		Yes		Category 2 – 12: 2 years
57	WECC2019022142			Yes	Yes					Yes		Yes		Category 2 – 12: 2 years
58	WECC2019022455			Yes	Yes									Category 2 – 12: 2 years
59	WECC2019022643			Yes	Yes									Category 2 – 12: 2 years
60	WECC2019021133			Yes	Yes									Category 2 – 12: 2 years
61	WECC2017017628			Yes	Yes				Yes	Yes				Category 2 – 12: 2 years
62	WECC2018020637			Yes	Yes									Category 2 – 12: 2 years
63	WECC2019021121			Yes	Yes					Yes				Category 2 – 12: 2 years
64	WECC2019021122			Yes	Yes				Yes					Category 2 – 12: 2 years

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022523	CIP-010-2	R2	[REDACTED] (the Entity)	[REDACTED]	08/04/2016	05/28/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R2. [REDACTED] In this Self-Log, the Entity reported that there were two instances where it failed to monitor changes to the baseline configuration at least every 35 days as required by Part 2.1.</p> <p>In the first instance of noncompliance, the Entity reported that for [REDACTED] Protected Cyber Assets (PCA) associated with [REDACTED], it failed to monitor for changes to one port at least once every 35 calendar days.</p> <p>This noncompliance began on August 4, 2016, when the UDP port was not added to its automated baseline monitoring tool, and ended on May 28, 2019, when the UDP port was added to its automated baseline monitoring tool.</p> <p>In the second instance of noncompliance, the Entity reported that for [REDACTED] PCAs associated with [REDACTED], it failed to monitor for changes to one port at least once every 35 calendar days.</p> <p>This noncompliance began on July 30, 2018, when the automated baseline monitoring tool configuration was updated incorrectly, and ended on May 28, 2019, when the automated baseline monitoring tool was configured correctly.</p> <p>The cause of the noncompliance for both instances was that the Entity’s implementation of its baseline monitoring tool lacked rigor for implementing PCAs.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk for both instances was minimal because of the issue was resolved by updating documentation, rather than by making any changes to the PCAs of issue. The two ports of issue were determined to be needed and authorized to be enabled, and the capability of changing the ports on the PCAs of issue was restricted to [REDACTED] authorized individuals with administrative access. Additionally, the one port authorized, but not included in the baseline, was configured with read only access and non-default passwords. Lastly, the issue was limited to [REDACTED] PCAs that have limited functionality and do not contain BES Cyber System Information, and the Entity procedurally reviews unsuccessful login attempts weekly and documents the review for these PCAs. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate both instances of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) performed a review of the PCAs of issue active, enabled ports, and determined that all active ports were authorized and there was no deviations from the baseline; 2) added the detected one authorized port to its baseline monitoring tool; 3) created a scheduled task to network scan the PCAs of issue so that the scan results can be compared against the baseline in the baseline monitoring tool and reviewed as part of the weekly baseline configuration review; and 4) performed its weekly baseline configuration review process which included the updated network scan of the PCAs of issue against the baseline. 					

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
MRO2019022526	CIP-007-6	R1	██████████ (the Entity)	██████	07/01/2016	06/01/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, as a ██████████, it was in noncompliance with CIP-007-6 R1. ██████████</p> <p>The Entity reported that during an internal assessment, a SME discovered that for ██████ Intermediate Systems (IS) associated to ██████████, it failed to determine a range of ports that were determined to be needed. The Entity determined that the ports of issue are not actively enabled but may have the capability to be enabled under unique circumstances.</p> <p>The cause of the noncompliance was that the Entity’s process for determining needed enabled ports lacked detail for ports that may be enabled but are not active all the time.</p> <p>The noncompliance began on July 1, 2016, when CIP Version 5 became enforceable, and ended on June 1, 2019, when the needed port range was added to the baseline documentation.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the issue was documentation in nature and was resolved through the update of documentation, rather than implementation of a change to the system. Only those ports needed for authorized services were enabled, reducing the exposure of the vulnerability. Additionally, the Entity monitors and reviews configuration changes to the ISs of issue above the required CIP protections. No harm is known to have occurred.</p>					
Mitigation			<p>To this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated its baseline with the ports of issue including the determination of need; 2) updated and approved manual ports and service documents associated to the ISs of issue to include the extended range for the needed ports of issue; and 3) began using manual documentation of the need for logical network accessible ports as part of its change control management until its automated baseline monitoring tool can support the ISs of 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
MRO2019022527	CIP-005-5	R2	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	05/30/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-005-5 R2. [REDACTED]</p> <p>The Entity reported that for [REDACTED] Intermediate Systems (IS) associated to [REDACTED], it failed to enforce encryption for Interactive Remote Access (IRA) sessions. The Entity discovered that the ISs of issue had telnet enabled, which provided the capability of unencrypted remote access to the ISs.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for identifying IS and the associated protections when performing an IRA.</p> <p>The noncompliance began on July 1, 2016, when CIP V5 standard became enforceable, and ended on May 30, 2019, when the access method was disabled on the IS of issue.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the Entity’s implemented procedure for IRA administratively enforced the use of encrypted access to the IS of issue, and it logged access sessions at the IS to its Security Information and Event Management system, which limited the issue to the technical control for using encryption. Although the violation duration was almost three years, MRO still determined the risk to be minimal because multi-factor authentication was enabled for the telnet access and the multifactor authentication was configured with a time-changing authentication token that could only be used once which would have mitigated the risk posed by the PIN being transmitted unencrypted, which limited the capability of the exposure. Lastly, the telnet access was limited to its substation wide area network that is managed by and restricted to the Entity and does not traverse the internet. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) disabled the telnet access on all ISs of issue; 2) removed telnet as a port determined to be needed for the IS of issue; and 3) identified the IS of issue as Intermediate Systems in its configuration management database to provide clarity on the required protections. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2020022757	CIP-003-6	R1	██████████ (the Entity)	██████████	09/19/2019	12/11/2019	Self-Log	Expected 12/31/2020
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 8, 2020, the Entity submitted a Self-Log stating that as a ██████████, it was in noncompliance with CIP-003-6 R1.</p> <p>The Entity reported that it reviewed all the periodic tasks as a practice of detective internal control and determined that it failed to review and obtain CIP Senior Manager approval within 15 calendar months for ██████████ cyber security policy documentations as per Part 1.1. The Entity has ██████ cyber security policies, a board policy and an administrative policy. The administrative policy was rewritten/reformatted in July 2019 and approved by the CIP Senior Manager. During this process, the board policy was also marked as though the CIP Senior Manager review was complete in the Entity’s tracking tool. However, the CIP Senior Manager had not approved the Entity’s board policy.</p> <p>The cause of the noncompliance was that the Entity’s implementation of its process was deficient in ensuring both cyber security policies are reviewed and approved by the CIP Senior Manager.</p> <p>The noncompliance began on September 19, 2019, when the review and CIP Senior Manager approval was not completed within 15 calendar months, and ended on December 11, 2019 when the review and CIP Senior Manager approval was completed for the board policy.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the Entity utilizes internal controls which reduced the duration of the issue to 84 days. Additionally, upon completion of the review and approval, it was determined that no changes were made to the cyber security policy since the previous CIP Senior Manager approval. Lastly, the issue was limited to ██████████ policies. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <p>1) when CIP Senior Manager reviewed and approved the board policy; and</p> <p>To mitigate the noncompliance for reoccurrence, the Entity will complete the following mitigation activity by December 31, 2020:</p> <p>1) update its NERC compliance tasks tracking process by implementing a Compliance Management System which will include review and approval of policies. The amount of time required to complete this final mitigation activity is related to the time frame needed to implement a new system to track system changes.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2020022758	CIP-009-6	R3	[REDACTED] (the Entity)	[REDACTED]	10/01/2019	01/06/2020	Self-Log	Expected 12/31/2020
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 8, 2020, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-009-6 R3.</p> <p>The Entity reported that it reviewed all the periodic tasks as a practice of detective internal control and determined that it failed to notify each person or group, with a defined role, within 60 days of creating the recovery plan for a new asset class as per Part 3.2.2. The new asset class was created two months prior to the noncompliance date with a recovery plan, and was reclassified as a different asset class with a new recovery plan replacing the existing recovery plan which ended the noncompliance.</p> <p>The cause of the noncompliance was that the Entity’s process was deficient as it did not send alert notification to each person or group with a defined role within 60 days from creation of the new recovery plan.</p> <p>The noncompliance began on October 1, 2019, which was 60 days after the recovery plan was created for the new asset class, and ended on January 6, 2020, when the asset class was reclassified as a different asset class with a new recovery plan replacing the existing recovery plan, and when approved notification was sent to each person or group with a defined role in the new recovery plan.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the Entity utilizes internal controls to review and verify completion of periodic tasks which limited the duration of the issue to 98 days. The Entity had newer recovery plan information available in the recovery plan directory for the Subject Matter Experts (SMEs) to use in the event of recovery of the asset. Additionally, the issue was limited to the new asset class. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <p>1) sent notification to each person or group with a defined role within 60 days from creation of the new recovery plan;</p> <p>To mitigate this noncompliance for reoccurrence, the Entity will complete the following mitigation activities by December 31, 2020:</p> <p>1) update its NERC compliance tasks tracking process by implementing a Compliance Management System which will include review and sending alert notifications to each person or group with a defined role within 60 days from creation of the new recovery plan. The amount of time required to complete this final mitigation activity is related to the time frame needed to implement a new system to track system changes.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022638	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	10/03/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2.</p> <p>When using a new detective control (new version of baseline scan tool), the Entity discovered that [REDACTED] were not updated for [REDACTED] Physical Access Control Systems (PACS) devices and [REDACTED] Electronic Access Control and Monitoring Systems (EACMS) devices. These devices were associated with [REDACTED]. The Entity reviewed the patch history evidence and patch source document and determined that all other relevant operating systems and software patching had been reviewed and applied to the devices. Additionally, the Entity discovered that its baseline documentation did not include patch related information for the [REDACTED] devices. The review determined that [REDACTED] security related [REDACTED] updates were missed as a result of the documentation deficiency.</p> <p>The cause of the noncompliance was the entity failed to follow its processes to include [REDACTED] to patch source and patch tracking documentation for [REDACTED] PACS devices and [REDACTED] EACMS related to CIP-007-6 Parts 2.1.</p> <p>The noncompliance began on July 1, 2016, the date the standard became enforceable, and ended on October 3, 2019, when missed [REDACTED] were installed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because of the following. All the security patches related to [REDACTED] [REDACTED] were evaluated and applied. The issue was discovered by a new internal detective control to the patching program. The issue was limited to [REDACTED] PACS devices and [REDACTED] EACMS device associated with a [REDACTED]. The issue was limited to [REDACTED] updates from a single source. All the impacted Cyber Assets where either PACS or EACMS, and the issue did not affect the associated BCS. The BES Assets reside outside Electronic Security Perimeter (ESP), are protected with several layers of security infrastructure. The [REDACTED] only controls and monitors [REDACTED], which inherently limits the impact to the BES. Additionally, there have been no security events associated with any of the devices. Upon discovery of the issue, the review, approval, and mitigation was completed within eight days. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the current [REDACTED] for all the affected devices; 2) updated the patch source documentation with new [REDACTED] information for the affected devices; 3) updated the patch tracking documentation with new [REDACTED] information for the affected devices; and 4) performed extent of condition analysis on all the Assets and confirmed that [REDACTED] was being tracked on all other in scope assets. <p>MRO has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2020022811	CIP-004-6	R2	██████████ (the Entity)	██████████	05/01/2019	12/13/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 10, 2020, the Entity submitted a Self-Log stating that, as a ██████████, it was in noncompliance with CIP-004-6 R2.3.</p> <p>The Entity reported that while performing an internal detective control review, it determined that ██████ individuals had failed to complete CIP training once every 15 calendar months as specified in CIP-004-6 R2.1. The Entity’s implemented training tool used to support CIP-004-6 R2.3 was not configured to enforce a mandatory deadline. Thus, the training was present for individuals to complete but individuals were not notified that there was a mandatory date for completion.</p> <p>The cause of the noncompliance was that the Entity failed to implement its control process for ensuring individuals complete CIP training once every 15 calendar months.</p> <p>The noncompliance began on May 1, 2019, when the first of the individuals impacted did not complete the training within 15 months of the previous training, and ended on December 13, 2019, when the last of the individuals impacted completed the training.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because all impacted individuals had previously received the CIP training and were aware of the CIP cybersecurity rules and responsibilities. The Entity had implemented additional cybersecurity awareness controls such as signs at the entrance of its Physical Security Perimeter (PSP) reminding personnel of required processes, a notification warning when electronically accessing a protected network, and periodic cybersecurity best practice emails. Additionally, the issue was discovered by a detective control, limiting the noncompliance to less than one 15 calendar month training cycle. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed CIP training (all individuals of issue); 2) updated its training tool to enforce a mandatory due date for CIP Training and provide individuals with notifications of the due date; 3) implemented an automated weekly report by the tracking tool for time based CIP activities that is reviewed by Compliance Staff; and 4) updated the reoccurrence of the CIP training to be performed annually within the training tool. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022438	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	11/28/2018	07/11/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 8, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2. The Self-Log contained two instances of noncompliance.</p> <p>In the first instance of noncompliance, during an internal reorganization, the Entity reevaluated the patch sources for [REDACTED] and discovered that [REDACTED] security patch was not evaluated within 35 days of being released as required by part 2.2. The security patch was not evaluated for antivirus clients for Windows workstations and servers logically [REDACTED]. The patch was not evaluated due to misinterpretation of the Vendor’s applicability statements which did not address any cyber security vulnerabilities.</p> <p>This instance of noncompliance began on November 28, 2018, 36 days after the patch evaluation cycle began, and ended on July 11, 2019, when the patch was evaluated.</p> <p>In the second instance of noncompliance, during the same internal reorganization the Entity reevaluated the patch sources for [REDACTED] and discovered that another [REDACTED] security patch was not evaluated within 35 days of being released as required by part 2.2. The security patch was not evaluated for antivirus clients for Windows workstations and servers logically [REDACTED]. The patch was not evaluated due to misinterpretation of the vendor’s applicability statements which did not address any cyber security vulnerabilities.</p> <p>This instance of noncompliance began on April 15, 2019, 36 days after the patch evaluation cycle began, and ended on July 11, 2019, when the patch was evaluated.</p> <p>The cause of noncompliance for both instances was that the Entity did not follow its once every 35 calendar days patch evaluation process due to misinterpretation of vendor’s applicability statements.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal for both instances because the issues were limited to [REDACTED] administrative credential security patches. The patches were applied to the Assets on next scheduled patching cycle, and the Assets were behind a firewall that did not have direct exposure to internet; this limited the external connectivity. Additionally, the vulnerability of the risk was related to administrative credentials, and there was only [REDACTED] with administrative credentials at the time the issue occurred who had access to these Assets, which reduces the risk of malicious activity. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) evaluated the [REDACTED] security patches; 2) updated the patch implementation procedure to include the revised patch source; 3) applied evaluated patches to all applicable Assets; and 4) provided training on the updated procedures to all network engineers. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2020022743	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	10/14/2019	10/22/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 3, 2020, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1.</p> <p>The Entity reported that its Compliance Coordinator reviewed its patch status report (internal control) and found [REDACTED] was installed by the Subject Matter Expert (SME) without prior authorization. A change request was issued that included [REDACTED] other applicable security patches but did not include the security patch of issue for installation when the SME selected patches to be included in the change request.</p> <p>The cause of the noncompliance was that the Entity's process was deficient in that it did not ensure that authorized patches were selected for installing.</p> <p>This noncompliance began on October 14, 2019, when the SME installed the patch without authorization, and ended on October 22, 2019, when the change request was submitted and approved by the manager.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the Entity utilizes internal controls which reduced the duration of the issue to nine days. Additionally, the patch of issue was verified and ensured that no cyber security controls were adversely impacted prior to the installation of the security patch. The installed patch was planned and the Entity was intending to include the patch of issue in the authorization request, limiting the issue to the documentation of the authorization request. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) submitted a change a request to document the change that was subsequently authorized the same day; 2) updated process for viewing security patches to include for installation to use a new view to provide clarity to which patches should be included and which should not be included; and 3) updated process for selecting security patches with a new filter that excludes patches not applicable or were already assessed. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022352	CIP-005-5	R2	<div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> (the Entity)	<div style="background-color: black; width: 100%; height: 15px;"></div>	07/01/2016	06/19/2019	Compliance Audit	Expected 12/31/2020
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from <div style="background-color: black; width: 100%; height: 15px;"></div>, MRO determined that the Entity, as a <div style="background-color: black; width: 100%; height: 15px;"></div>, was in noncompliance with CIP-005-5 R2.</p> <p>It was discovered that the Entity allowed Interactive Remote Access (IRA) from <div style="background-color: black; width: 100%; height: 15px;"></div> users, located in corporate environment, to Cyber Assets within an Electronic Security Perimeter (ESP), which was not allowed per the Entity’s ESP policy.</p> <p>The cause of the noncompliance was that the Entity failed to follow its documented process to ensure that IRA is not available from <div style="background-color: black; width: 100%; height: 15px;"></div> users to Cyber Assets within ESP.</p> <p>The noncompliance began on July 1, 2016, when the CIP v5 applicable standard became enforceable <div style="background-color: black; width: 100%; height: 15px;"></div>, and ended on June 19, 2019 when it was determined that this read only access for the <div style="background-color: black; width: 100%; height: 15px;"></div> users is required to perform their job duties.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was minimal for the following reasons. First, the Entity did not allow vendor remote access into the ESP. The Entity had protections in place on the corporate network to deny any access to Supervisory Control and Data Acquisition (SCADA) system through Virtual Private Network (VPN). The Entity does not allow any ESP access from the internet. Only a small number of approved users were capable of initiating <div style="background-color: black; width: 100%; height: 15px;"></div> access. The users were current with their Personnel Risk Assessment (PRA). All login and logout attempts or transactions were recorded in the system alarm log for all the SCADA system authentication and the Entity did not find any unauthorized logins and the <div style="background-color: black; width: 100%; height: 15px;"></div> logins were limited to read-only access. On June 19, 2019, it was determined that the <div style="background-color: black; width: 100%; height: 15px;"></div> authenticated read-only access is required by the Entity’s employees to perform their job duties. The Entity’s Control Center contains <div style="background-color: black; width: 100%; height: 15px;"></div> This Control Center only controls and monitors assets that contain <div style="background-color: black; width: 100%; height: 15px;"></div> which inherently limits the impact to the BES. No harm is known to have occurred.</p> <p>The Entity has no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity will complete the following mitigation activities by December 31, 2020:</p> <ol style="list-style-type: none"> 1) scheduled an upgrade of SCADA system with its vendor; and 2) discussed the issue with the SCADA vendor; the vendor ensured that this issue will be resolved with the upgrade. <p>The amount of time required to complete this mitigation activity is related to the vendor availability.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022616	CIP-004-6	R4	[REDACTED] (the Entity)	[REDACTED]	04/01/2019	06/07/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 29, 2019, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-004-6 R4, P4.3. [REDACTED]</p> <p>The Entity reported that during a security compliance specialist’s annual review of CIP-004-6 P4.3, the security compliance specialist discovered that it did not verify user account groups and role access once every 15 calendar months as required by CIP-004-6 P4.3. The Entity had completed its previous 15 calendar month evaluation. The Entity periodically evaluated its quarterly access review as required by P4.2 but did not verify P4.3. The annual review process reminder email was sent to the newly hired [REDACTED], and no additional email or outlook reminders were sent after the initial email. Due to high volume of emails received, this individual, missed the 15 calendar month notification. The regional supervisors are more familiar with the access roles and have more familiarity and capability to complete the review process; however, they were unaware that it was due and were not assigned as the reviewers.</p> <p>The cause of the noncompliance was that the Entity’s process was inadequate as it did not ensure that the responsibilities and duties were assigned to the appropriate personnel for review as needed to follow the Entity’s process to perform the necessary once every 15 calendar months evaluation.</p> <p>The noncompliance began on April 1, 2019, the day after the last day of 15 month evaluation date, and it ended on June 7, 2019, when a thorough review of all user account groups and role access were completed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the quarterly reviews, required by P4.2, were completed by managers who understood who should have authorized access. No improper privileges of individuals, user account groups, or user role categories resulted from this issue. The initial access to the SCADA system requires both supervisor and role owner approval, and a separate individual who provisions the access, which provided multiple level of checking and scrutinizing the access level provision. Inappropriate access or authorization would have triggered a review of the individual’s entire access. No other CIP requirements were at risk of noncompliance as a result of this issue. Additionally, the noncompliance was discovered during an internal annual evaluation, limiting the duration of the noncompliance to 68 days. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed the review of all user accounts for the SCADA system; 2) reviewed the individual of issue's associate privileges and determined they were correct and necessary; and 3) reassigned reviewer role to the user’s closest manager to conduct both quarterly and annual role 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
NPCC2019021345	CIP-002-5.1	R1.	[REDACTED]	[REDACTED]	07/01/2016	12/05/2017	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>During a Self-Certification conducted from March 1, 2019 through April 24, 2019, NPCC determined that [REDACTED] (the entity), as a [REDACTED], was in noncompliance with CIP-002-5.1 R1. The entity failed to implement a process that identified each asset that contained [REDACTED].</p> <p>The entity discovered that it did not have evidence of performing a Cyber Impact Evaluation that identified each asset that contained [REDACTED]. The entity was identified as not having any Critical Assets or Critical Cyber Assets under prior versions of the CIP-002 Reliability Standard. Plant personnel were unaware of the revisions to the Standard in CIP-002-5.1 and subsequent versions and the additional requirement to identify low impact BES Cyber Systems.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable. The noncompliance ended on December 5, 2017, when the entity identified each asset that contained [REDACTED] through a Cyber Impact Evaluation.</p> <p>The root cause of this noncompliance was a weak compliance program that lacked clearly defined responsibilities and a lack of awareness by plant personnel of Reliability Standard revisions.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The failure to properly identify and classify BES Cyber Systems increases the potential that the Cyber Systems will not receive the appropriate cyber security protections. The BES Cyber Systems could be compromised and impact the reliable operation of the BPS. The risk to the BPS is reduced because the issue related to a single BES Cyber System with [REDACTED]. The entity included its [REDACTED] in its Cyber Security Training and its Cyber Security Incident Response Plan. The risk was reduced further because the site is a [REDACTED] facility that generally runs for [REDACTED] annually.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity’s compliance history and determined there were no relevant underlying causes.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed the Cyber Impact Evaluation identifying each asset that contains [REDACTED] and it was approved by the CIP Senior Manager; 2) implemented a new file structure to improve document and revision control; 3) developed a new NERC Compliance Program to facilitate a better understanding of NERC Reliability Standards; 4) improved NERC compliance training to complement the new compliance program; and 5) established monthly calls with the corporate office to review all NERC activities and programs. 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021414	CIP-002-5.1	R2.	[REDACTED]	[REDACTED]	07/01/2016	12/05/2017	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>During a Self-Certification conducted March 1, 2019 - April 24, 2019, NPCC determined that [REDACTED] (the entity), as a [REDACTED], was in noncompliance with CIP-002-5.1 R2 (2.1, 2.2). The entity failed to review the identifications in CIP-002-5.1 R1 and its parts through a Cyber Impact Evaluation at least once every 15 calendar months. The entity also failed to have its CIP Senior Manager or delegate approve the identifications.</p> <p>The entity discovered that it did not have evidence of reviewing the identifications in CIP-002-5.1 R1 and its parts or having its CIP Senior Manager review the identifications at least once every 15 months. Before discovering the noncompliance, the entity contracted a third party vendor to update the entity’s procedures. The updated procedures resolved the noncompliance as part of the update to the procedures, but the entity did not realize that it had been noncompliant previously.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable. The noncompliance ended on December 5, 2017, when the entity completed and approved its cyber impact evaluation.</p> <p>The root cause of this noncompliance was a weak compliance program that lacked clearly defined responsibilities and a lack of awareness by plant personnel of Reliability Standard revisions.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The failure to properly identify, classify, and then review BES Cyber Systems increases the potential that the Cyber Systems will not receive the appropriate cyber security protections. The BES Cyber Systems could be compromised and impact the reliable operation of the BPS. The risk to the BPS is reduced because the issue related to [REDACTED]. The entity included its [REDACTED] in its Cyber Security Training and its Cyber Security Incident Response Plan. The risk was reduced further because the site is a [REDACTED] facility that generally runs for [REDACTED] annually.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity’s compliance history and determined there were no relevant underlying causes.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed a Cyber Impact Evaluation and it was approved by the CIP Senior Manager; 2) implemented a new file structure to improve document and revision control; 3) developed a new NERC Compliance Program to facilitate a better understanding of NERC Reliability Standards; 4) improved NERC compliance training to complement the new compliance program; and 5) established monthly calls with the corporate office to review all NERC activities and programs. 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021720	CIP-011-2	R1	[REDACTED]	[REDACTED]	12/10/2018	2/5/2019	Self-Report	June 19, 2020
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On June 18, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-011-2 R1.</p> <p>On January 31, 2019, as a result of a manual analysis of an access request for logical user access to Bulk Electric System Cyber Security Information (BCSI) storage locations, the entity discovered that it provisioned inappropriate access to one individual to BCSI storage locations [REDACTED]</p> <p>Upon noticing the non-traditional access request, the individual who identified the first issue did a search of prior results resulting in the identification of four additional users who required access, [REDACTED] to BCSI storage locations for job duties but had not taken the entity's Information Protection training prior to their access being provisioned. [REDACTED] All four of the individuals were intended to have access to the BCSI storage locations, however their access was granted [REDACTED] s which meant the individuals did not take the entity's Information Protection training per CIP-011-2 R1 prior to receiving access.</p> <p>This noncompliance involves the management practices of asset and configuration management and workforce management. The root cause is the undefined logical access provisioning procedures [REDACTED] The lack of clarity, arising from poor asset and configuration management, [REDACTED] resulted in individuals receiving access to BCSI storage locations prior to the entity's Information Protection training being taken, which implicates workforce management as those individuals should not have been granted access before completing the training.</p> <p>This noncompliance started on December 10, 2018, when the entity granted access to the first of the five users before they had taken the entity's required Information Protection training and ended on February 5, 2019 when the users completed the required training.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed is that granting individuals authorized logical access to BCSI storage locations prior to receiving Information Protection training could result in the mishandling or misuse of BCSI data elements. The risk is minimized because all of the users were intended to have logical access to the BCSI storage locations both prior to and after taking the Information Protection training. The users also received the training only two months late. Additionally, the entity self-identified the noncompliance. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) digitally distributed the BCSI training [REDACTED] to the identified individuals who were granted BCSI access; 2) updated the entity's Information Protection Plan (IPP) to include: specific requirements for access to BCSI for physical individuals, individual accounts, shared accounts, and service accounts or other accounts and identification of and reference to electronic BCSI storage locations; [REDACTED] 4) reviewed the roster of individuals who develop and support [REDACTED] for accuracy and completeness for those who may require access to develop accounts which will include access to BCSI. The individuals identified will be confirmed to have completed the appropriate BCSI training and will be responsible to adhere to the revised IPP (communicated through the training and other milestones in this Mitigation Plan); [REDACTED] <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by June 19, 2020:</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021720	CIP-011-2	R1	[REDACTED]	[REDACTED]	12/10/2018	2/5/2019	Self-Report	June 19, 2020
			<p>6) will inventory and verify all individuals with access to [REDACTED] accessed via password vault to ensure they have proper authorization and training for access to BCSI information;</p> <p>7) will develop an awareness training plan for BCSI users. The plan will include determining the difference between a document of record from convenience copy, examples, and BCSI handling ownership responsibilities. The document of record is BCSI stored in a declared BCSI storage repository as per the IPP where convenience copies are duplicates used for immediate business use and to be destroyed when the business use concluded. This awareness training will reinforce the proper definition, use, transport, and storage of BCSI, detail the requirements for BCSI access with focus on what accounts are allowed to access BCSI;</p> <p>8) will document a review of BCSI storage locations in business unit and corporate directory. The entity will review for consolidation of locations where possible and update locations within the entity's IPP; and</p> <p>9) will document requirements of proper authorization and training within [REDACTED] password vaults and/or access control lists. This will serve as additional awareness for those accessing [REDACTED] and the audience who may receive any output from [REDACTED]</p> <p>Additional time is required to develop the inventory and verify all individuals with access to [REDACTED] and to develop an awareness training plan for BCSI users.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021927	CIP-010-2	R1	[REDACTED]	[REDACTED]	2/9/2019	2/28/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 22, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>On February 9, 2019, two jump-host servers labeled “pre-deploy” were given access to the production environment without being approved intermediate systems. They were not yet approved intermediate systems because the entity missed the last steps in the onboarding process, which was establishing a baseline for the devices [REDACTED] thereby allowing access from the devices into the ESP.</p> <p>As background, in this instance, [REDACTED], allowing access into the ESP, before the devices had been fully moved into production; [REDACTED]</p> <p>In October 2018, the entity hardened the jump hosts and applied all other relevant CIP requirements. The entity then stored the jump-hosts in the Physical Security Perimeter (PSP), disconnected from the ESP until the jump-hosts were incorrectly provided access on February 9, 2019. Upon discovery, access was removed as of February 28, 2019 to allow for the missed last steps to be completed. The entity completed the missed steps later on February 28, 2019 and deployed the servers back into production.</p> <p>The root cause of this noncompliance was lack of controls regarding the granting of logical access to non-production assets via the [REDACTED]. Additionally, an employee presumption of commissioning status by various individuals without validation was a secondary cause.</p> <p>This noncompliance involves the management practices of asset and configuration management and verification. Asset and configuration management is involved because the entity had a faulty process resulting in the jump-host being provided access to the ESP without authorization as required by CIP-010-2 R1. Verification is involved because the entity did not have adequate controls to assure that all assets in the production environment were authorized.</p> <p>This noncompliance started on February 9, 2019, when the entity introduced the jump-host into the production environment without authorization and ended on February 28, 2019, when the entity removed the jump-host from the production environment.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by making unapproved changes when installing a Cyber Asset is that vulnerabilities could be introduced into the system. The risk here is minimal because the jump-hosts had already been hardened pursuant to the CIP requirements, including: 1) disabling unnecessary logical and physical ports; 2) using elevated password complexity parameters; 3) logging security events; and 4) utilizing malicious code deterrence protections. Additionally, the devices were located inside a Physical Security Perimeter (PSP) and thus afforded the protections of a PSP including access authorization, monitoring, and logging. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity’s compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the affected jump-hosts from the production environment, and completed all necessary change control steps; 2) added a process step to its change control process to require an alert if an instance is identified where a non-CIP device would be able to communicate with a CIP device if the change is completed; 3) added a step to its change control process to verify a device is in production [REDACTED]; and 4) added a step to its change control process for servers [REDACTED] to add the device to the production environment has 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
RFC2019021784	CIP-004-6	R2	[REDACTED]	[REDACTED]	5/8/2019	5/15/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 2, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R2. An individual user failed to complete cyber security training during a 15-month interval in violation of CIP-004-6 R2.3. The user had previously completed cyber security training and was trusted by, and in good standing with, the entity. On May 15, 2019, the user discovered that his training lapsed on May 8, 2019, and he completed the training on that same day after discovering the issue.</p> <p>The root cause of this noncompliance was a gap in the entity’s tracking process. The entity utilizes a tool to track the status of training for all individuals with NERC-related access, and the tool includes [REDACTED]. However, the entity did not utilize an active alerting mechanism to notify users or compliance personnel of upcoming deadlines, and no one was closely monitoring the tool at the time of this noncompliance.</p> <p>This noncompliance involves the management practice of implementation. The entity implemented a tool to assist in tracking the status of training for all individuals with NERC-related access, but it failed implement corresponding processes, procedures, or technical solutions designed to address follow-up tasks and activities.</p> <p>This noncompliance started on May 8, 2019, when the user failed to complete training within a 15-month interval and ended on May 15, 2019, when the user completed training.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. Untrained individuals are more likely to misuse access or fail to adhere to security practices, thereby increasing the threat to the reliability and resilience of the BPS. Here, the risk was minimized based upon the following facts. First, this noncompliance involved a trusted user who had previously completed cyber security training. Second, this noncompliance was short in duration (i.e., 8 days). No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity’s compliance history should not serve as a basis for applying a penalty because the prior noncompliance involved separate and distinct issues and different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) completed necessary training with the user; 2) confirmed that no similar instances of noncompliance existed; and 3) implemented an alerting tool to notify the user, their manager, and multiple compliance personnel thirty days from the user’s training anniversary. Additional alerts are sent two weeks prior to a due date, seven days prior to a due date, and then every day until training is 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
RFC2016016472	CIP-002-3	R2	[REDACTED]	[REDACTED]	3/18/2016	10/31/2016	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On November 1, 2016, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance of CIP-002-3 R2.</p> <p>On March 18, 2016, [REDACTED], and the CIP Senior Manager signed the Bulk Electric System (BES) Cyber System Identification document as required by its CIP-002 policy. However, the entity later identified 5 discrepancies impacting 16 assets in the list of BES Cyber Systems.</p> <p>The first discrepancy involves a relay at a medium impact substation that was replaced in January 2016 with a relay performing the same function, but had a different unique identification number. The entity failed to note the new unique identification number on the signed BES Cyber System Identification list.</p> <p>The second discrepancy involves an Electronic Access Control and Monitoring System (EACMS) server placed into the [REDACTED]. This was an emergency installation to quickly assist with the [REDACTED] being generated by [REDACTED] on May 5, 2016. [REDACTED] However, the change control ticket for the [REDACTED] EACMS server incorrectly marked the device as not being a CIP asset. Therefore, it did not show up in the entity’s system of record.</p> <p>The third discrepancy involved twelve documentation errors that the entity discovered during an additional physical inventory on all of its BES Cyber Systems in September 2016. In each case, one character from a device’s unique identification number was transcribed incorrectly.</p> <p>The fourth discrepancy involved a relay at a medium impact substation that had been scheduled to be replaced. The change was properly approved, but not yet completed. However, the entity’s documentation reflected the information for the new relay despite the fact that the old relay remained installed.</p> <p>The fifth discrepancy involved an EACMS that had been misclassified as a Physical Access Control System (PACS).</p> <p>The root cause of these issues are as follows: (a) For the first discrepancy, a change control process for medium impact substations had not yet been implemented; (b) For the second discrepancy, the responsible analyst failed to select the boxes on the change control ticket to identify the EACMS as a CIP asset; (c) For the third discrepancy, the person performing the scribe function recorded numbers incorrectly; (d) For the fourth discrepancy, there was confusion over the internal definitions of a completed change control and a closed change control. [REDACTED] The responsible individual in this case incorrectly updated the BES Cyber System Identification list when the change control was completed, but not yet closed; and, (e) For the fifth discrepancy, the responsible individual mistakenly flagged the Cyber Asset as both an EACMS and a PACS on the [REDACTED]. The [REDACTED] did not have sufficient error checking capabilities to alert the user to this conflict, which resulted in the device being incorrectly classified as a PACS. (These major contributing factors involve the management practices of asset and configuration management, which includes identifying assets and configuration items inventory, and workforce management, which includes managing the system to minimize human performance issues.)</p> <p>The noncompliance began on March 18, 2016, [REDACTED], and ended on October 31, 2016, the date the entity completed its Mitigating Activities.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by these types of asset identification and classification issues is that, without this information, the responsible entity may not be able to properly protect its system because it does not have a complete and accurate view of all of the assets that comprise its system. This risk was mitigated in this case by the following factors. First, the entity self-identified all of these issues through its standard business practices, including voluntary inventory exercises and a mock audit. Second, the majority of these discrepancies (i.e., 12 of 16) were merely documentation errors related to the identification of assets in the system (i.e., incorrect unique identification numbers or misclassifications). These assets were known to the entity and protected within the CIP environment, but just identified incorrectly. Third, for the four remaining assets that were actually missing some baseline information, the entity was still managing and protecting them within its CIP environment through its asset management system, which is a real-time list containing all cyber assets and used by subject matter experts for their daily operations and compliance activities. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) conducted a comprehensive physical inventory of high and medium Impact control centers and substations to validate that all documentation was correct and BES Cyber System Identification (BCSI) list is accurate; 2) added the EACMS server to the entity system of record and is now identified as a CIP asset. The entity updated the BCSI list to reflect the additional EACMS; 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2016016472	CIP-002-3	R2	[REDACTED]	[REDACTED]	3/18/2016	10/31/2016	Self-Report	Completed
			3) updated its Change Control and Configuration Management Procedure to more clearly define the roles and responsibilities associated with completing and closing change control tickets approved for implementation; 4) corrected the twelve documentation errors in its system of record and on the BCSI list; 5) updated the medium impact relay information in its system of record and on the BCSI list; 6) updated the [REDACTED] to help discern between EACMS and PACS; and 7) reviewed and approved an updated BCSI list by the CIP Senior Manager and other entity approvers. 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
RFC2018018928	CIP-004-6	R4	[REDACTED]	[REDACTED]	9/11/2017	11/6/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On December 20, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance of CIP-004-6 R4. [REDACTED]</p> <p>On November 6, 2017, during a physical access quarterly review, the entity discovered that back on September 11, 2017, a security services analyst inadvertently updated the critical PACS portion of an employee’s profile to match what was in the non-critical PACS portion of the profile without first checking to see if the access was authorized. The entity immediately removed the employee’s unauthorized unescorted physical access upon discovery. The entity also reviewed the critical PACS access report and confirmed that the employee did not access, nor attempt to access, the identified CIP Physical Security Perimeter (PSP).</p> <p>The root cause of this noncompliance was the security services analyst’s failure to follow the proper procedure for granting unescorted access. This root cause involves the management practice of workforce management, which includes providing training, education, and awareness to employees.</p> <p>The noncompliance began on September 11, 2017, the date the security services analyst inadvertently provisioned access for this employee and ended on November 6, 2017, when the entity removed the employee’s unauthorized unescorted physical access.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by granting unescorted physical access to individuals who have not been approved for such access is that it increases the likelihood that the unauthorized individual could access a critical location and cause adverse impact. This risk was minimized in this case by the following factors. First, security guards are in place to control daily admittance to the CIP-critical location, which reduces the likelihood that the employee would have accessed the CIP-critical location. Second, the employee is a current employee in good standing who has a current Personnel Risk Assessment, background check, and CIP training, as well as access to other CIP-critical locations. These factors reduce the likelihood that the employee would have done anything to adversely impact the BES. ReliabilityFirst also notes that the employee did not attempt to access the PSP during the time of the noncompliance. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity’s compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) retrained security analysts on the steps required to provision access; 2) developed a PACS report to show physical access changes to critical facilities. The report will be compared against access request and revocation notices by a security analyst on a weekly basis; 3) reviewed existing processes for provisioning of access to determine whether additional controls can be implemented and revised as necessary. As part of such review, security services documented departmental procedures and training; and 4) performed retraining including training on any process revisions. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017016727	CIP-004-6	R5	[REDACTED]	[REDACTED]	10/2/2016	11/15/2016	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On December 28, 2016, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance of CIP-004-6 R5. [REDACTED]</p> <p>On October 1, 2016, a consultant with unescorted physical access to critical locations and electronic access to BCSI completed her work assignment and no longer required access. However, this consultant’s sponsor had left the entity back on August 11, 2016. The new sponsor who took over responsibility for this consultant was a new hire and did not receive sufficient training on his responsibilities as a sponsor. Consequently, when he received an email notification indicating that he was this consultant’s new sponsor, he did not know what that required him to do. As a result, the new sponsor failed to complete the [REDACTED] form when the consultant’s work ended. Subsequently, on November 15, 2016, an entity asset owner was performing his quarterly application access review and discovered that this consultant still had access to her electronic storage locations even though she was no longer engaged with the entity. (The consultant’s unescorted physical access [REDACTED] on October 6, 2016, through separate internal controls.) Immediately upon discovery, the entity completed a [REDACTED] form and removed the consultant’s electronic access.</p> <p>The root cause of this noncompliance was the entity’s failure to make the new sponsor aware of his duties with respect to the consultant’s access. This root cause involves the management practices of workforce management, which includes managing employment status changes, and external interdependencies because the issue involves consultants from outside the company.</p> <p>The noncompliance began on October 2, 2016, the date the entity was required to remove the consultant’s access and ended on November 15, 2016, when the entity actually revoked the consultant’s access.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to revoke access in a timely manner is that an individual who is no longer permitted to have access will use that access in a manner that will compromise the BPS. This risk was minimized in this case by the following factors. First, the consultant did not have Interactive Remote Access, so she would have to first gain physical access in order to utilize her electronic access. The fact that her physical access was removed on October 6, 2016, limits the amount of time that this could have occurred. Second, the consultant left in good standing with the entity and her company’s contract was still active with the entity until the end of 2017, which reduces the likelihood that she would have used her unauthorized access for any nefarious purposes. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity’s compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed electronic access immediately for the consultant upon discovery of the error; 2) performed a validation comparison with Physical Security to make sure that both departments have the same sponsor identified for all CIP authorized consultants; 3) enhanced the change in sponsorship notification from Physical Security to include required notifications from assigned sponsors for them to indicate that they accept sponsorship of consultant. If no response is received from assigned sponsor, escalation to the sponsor’s supervisor will take place; and 4) implemented a process to verify that their records correspond with what Physical Security has documented as sponsors for all CIP authorized consultants. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018251	CIP-004-6	R5	[REDACTED]	[REDACTED]	6/30/2017	7/24/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On August 16, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance of CIP-004-6 R5. During a [REDACTED] change control approval meeting, the entity discovered that it failed to change one shared account password within 30 calendar days of an employee resigning from the company. On May 30, 2017, an employee terminated his employment with the entity. The entity removed the employee’s Interactive Remote Access, electronic access, and physical access within 24 hours. However, the entity failed to change one shared account password relating to [REDACTED] devices at high impact locations within 30 calendar days [REDACTED]. The entity changed the passwords by July 24, 2017, approximately 3 weeks late.</p> <p>The root cause of the noncompliance was multiple process failures by the responsible teams. First, an analyst failed to execute the appropriate procedure in a timely manner, delaying notification of the necessary change. Second, the change procedure for the [REDACTED] devices did not accurately reflect the appropriate process for changing the password, which caused an additional delay in changing the password. Third, once the change was actually attempted, the [REDACTED] at the alternate operations center stopped responding to commands due to a [REDACTED] change. This required suspension of [REDACTED] changes until the issue could be corrected. This root cause involves the management practice of workforce management, which includes managing employees’ access to assets and information.</p> <p>The noncompliance began on June 30, 2017, the date by which the entity was required to change the password, and ended on July 24, 2017, when the entity actually changed the password.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to change a password on a shared account after an employee’s termination is that the former employee could use that password to access the system or device at issue. This risk was mitigated in this case by the following factors. First, any attempt to log onto these devices would have to be initiated from inside the Physical Security Perimeter and come from a device within the Electronic Security Perimeter. Because the entity removed the employee’s physical and electronic access within 24 hours of his resignation, the likelihood of this employee being able to use the password is low. Second, the entity identified the issue through a normally occurring internal control, i.e., a [REDACTED] change control approval meeting. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity’s compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reinforced [REDACTED] Password Change Procedure with [REDACTED] team; 2) updated the automated checklist template for shared account password changes so that it now escalates to the Supervisor [REDACTED] days before the due date for any necessary follow-up; 3) reviewed and revised [REDACTED] Password Change Procedure; 4) updated their processes for terminations and transfers to ensure that the automated reminder sent out for password changes is given a due date [REDACTED] business days in advance of the thirty day window to ensure a buffer before the thirty business day window expiration; 5) updated the automated checklist template for shared account password changes to produce separate notifications per asset type which will be tracked and escalated individually; 6) implemented a mandatory acknowledgement checkbox on access provisioning tool that requires the analyst to confirm the creation of a password change automated checklist when processing a termination or transfer; 7) developed a matrix of responsible individuals for performing password resets on each asset, and ensured these individuals were trained on the responsibilities under the CIP-004-6 R5 P5.5 Standard; 8) developed a process to review and maintain the matrix of individuals designated to perform password changes in order to ensure the appropriate individuals are assigned to perform password change activities; and 9) performed a review and update as necessary to password procedure documents. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018531	CIP-004-6	R5	[REDACTED]	[REDACTED]	6/30/2017	9/6/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On October 18, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance of CIP-004-6 R5. During a paper vulnerability assessment, the entity discovered that it failed to change, within 30 calendar days of an employee resigning from the company, one shared [REDACTED] account password on [REDACTED] at the alternate operations center. The individual resigned from the company on May 30, 2017, and the entity removed his Interactive Remote Access, electronic access, and physical access within 24 hours. However, the entity did not change these passwords until September 6, 2017.</p> <p>The root cause of the noncompliance was the failure by responsible personnel to follow the established change management process. Specifically, despite being included in the [REDACTED] change approval meeting, the responsible personnel did not approve the change request or follow up to determine if the device had shared passwords. Thus, when the employee left the company, notifications to change the passwords were not distributed. This root cause involves the management practice of workforce management, which includes managing employees’ access to assets and information.</p> <p>The noncompliance began on June 30, 2017, the date by which the entity was required to change the passwords, and ended on September 6, 2017, the date by which the entity actually changed the passwords.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to change a password on a shared account after an employee’s termination is that the former employee could use that password to access the system or device at issue. This risk was mitigated in this case by the following factors. First, any attempt to log onto these devices would have to be initiated from inside the Physical Security Perimeter and come from a device within the Electronic Security Perimeter. Because the entity removed the employee’s physical and electronic access within 24 hours of his resignation, the likelihood of this employee being able to use the password is low. Second, the entity identified the issue through a normally occurring internal control, i.e., a paper vulnerability assessment. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity’s compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) added the [REDACTED] asset accounts to the password management system for managing and monitoring; 2) changed the shared account passwords and [REDACTED] account password on the [REDACTED]; 3) augmented the CIP change management process to include a review of any new asset type to validate that the security capabilities are understood and documented before the installation and implementation of the devices into the entity CIP environment. This will facilitate comprehensive identification of technical feasibility exceptions, setup and authorization for shared accounts, initiation of security events and configuration monitoring and other required security controls; and 4) provided training to subject matter experts about the additions to the CIP change management process for new asset types. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2016016471	CIP-006-6	R1	[REDACTED]	[REDACTED]	9/12/2016	9/12/2016	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On November 1, 2016, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance of CIP-006-6 R1. On September 12, 2016, an employee with authorized unescorted physical access to Physical Security Perimeters (PSPs) was escorting two contractors with new furniture into a PSP. The employee followed the physical security process of escorting visitors into a PSP and contacted the security command center to have the contractors’ entry logged, then he escorted the contractors into the PSP.</p> <p>Due to maintenance issues that day, access to the PSP was through a secured alternate entry, which consisted of a double door [REDACTED] [REDACTED]. The employee held the first door open for the contractors while they moved the furniture through the door. The contractors then opened the second door to get the furniture inside the PSP. At that point, the employee let go of the door and let it close by itself. He heard the door click, indicating that it had latched closed, and he continued into the PSP with the contractors to deliver the furniture. However, the first door did not completely close and was resting ajar. [REDACTED]. In this case, because the employee let the first door close on its own while the second door was open, the first door did not completely close. The employee should have pulled the door closed tightly to ensure the lock engaged.)</p> <p>The PSP door alarms were configured to alert the security [REDACTED] once a PSP door remained open for longer than 30 seconds. The door alarm operated as intended in this case, alerting the security [REDACTED]. However, because the security [REDACTED] was aware of the furniture move, they silenced the alarm and documented that the alarm was due to furniture being moved into the PSP.</p> <p>A short time after the door was left ajar, another employee with authorized unescorted physical access was walking past the door and observed that the door was not completely shut. The employee immediately entered the PSP to locate a supervisor. However, because he was acting with urgency, this employee [REDACTED], but failed to [REDACTED] before entering the PSP. Within minutes, the employee located a supervisor and they both investigated the issue. The supervisor pulled the door completely shut and ensured that it was operating correctly. He then contacted the manager of security [REDACTED] to notify him of the occurrence.</p> <p>In total, the door remained ajar for approximately 13 minutes. During this time, two additional employees with authorized unescorted physical access completed their two-factor authentication and entered the PSP. However, they also failed to notice that the door did not completely shut behind them due to the issue [REDACTED].</p> <p>The root cause of this noncompliance was the employees’ lack of awareness [REDACTED] in place on the doors and how to appropriately ensure that the doors shut behind them. This root cause involves the management practice of workforce management, which includes providing training, awareness, and education to employees.</p> <p>The noncompliance began on September 12, 2016, when the employee mistakenly left the door ajar, and ended approximately 13 minutes later when the supervisor pulled the door shut.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by leaving the door ajar is that an unauthorized person could gain access to the PSP. This risk was mitigated in this case by the following factors. First, the door failed to latch for a total of 13 minutes, which reduces the amount of time that an unauthorized person could have gained access to the PSP. Second, the next employee to come upon the door and find that it was unlatched immediately took steps to correct the issue, which demonstrates commitment to security. Third, the door was located at a facility with layered security. Therefore, to access this particular door, a person would first have to [REDACTED]. Then a person would have to [REDACTED]. Second, the PSP entry point was [REDACTED], which would have alerted security personnel had an unauthorized person attempted to gain entry to the PSP. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity’s compliance history should not serve as a basis for applying a penalty because the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) contacted manager of property services to remind his employees to verify that doors are securely closed when opening and closing doors into a PSP; 2) removed the small door [REDACTED] that prohibited the door from completely latching closed; 3) re-emphasized to all relevant personnel who monitor the PSP Physical Access Control Systems to advise employees that after holding PSP access point doors open longer than thirty seconds for business purposes, to call back to the Security [REDACTED] once they are finished with their work and have secured the access point; 4) reviewed the Critical Infrastructure Protection Physical Security 2016 refresher training with property services during their daily morning briefing; 5) conducted a meeting with the entity [REDACTED] employee involved to review the incident and verify that he is aware of the process to follow when entering and exiting a PSP; and 6) visited all of the access point doors located at a PSP to verify that [REDACTED], if discovered, were removed from those doors as well, in order to avoid a similar occurrence from happening in the future. 					

ReliabilityFirst Corporation (ReliabilityFirst)

Compliance Exception

CIP

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2016016471	CIP-006-6	R1	[REDACTED]	[REDACTED]	9/12/2016	9/12/2016	Self-Report	Completed
			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
RFC2017017784	CIP-006-6	R2	[REDACTED]	[REDACTED]	5/1/2017	5/1/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On June 15, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance of CIP-006-6 R2. During a security spot check, the entity discovered that on May 1, 2017, an employee who no longer had authorized unescorted physical access to a Physical Security Perimeter (PSP) was permitted to enter a PSP unescorted.</p> <p>At 1:51 pm, the employee successfully entered a PSP access point using an [REDACTED]. However, when the employee attempted to exit the PSP at 7:30 pm, his [REDACTED] was denied by the [REDACTED]. The employee did not know why his [REDACTED] was denied, so he requested help from a security [REDACTED], who assisted him with exiting the PSP. Then, at 7:45 pm, the employee attempted to reenter the PSP by scanning his [REDACTED] which was denied again. Because the security [REDACTED] knew this employee had been working in the PSP as an authorized employee earlier in the day and just exited 15 minutes earlier, he permitted the employee to reenter the PSP without being logged in as a visitor with an assigned escort. The employee finally exited the PSP at 9:47 pm.</p> <p>The entity discovered that the employee had been transitioning from a job role located inside the PSP to a new job role located outside the PSP. This job role transition officially occurred, and the employee’s authorized physical access was removed at 3:43 pm on the day of this incident. So, the employee was authorized to enter the PSP at 1:51 pm, but that authorization was removed approximately 2 hours later.</p> <p>The root cause of this noncompliance was the security [REDACTED] failure to check the physical access system. Had he done so, he would have learned why the employee’s [REDACTED] was not working. This root cause involves the management practice of workforce management, which includes managing employee permissions and access to assets.</p> <p>The noncompliance began on May 1, 2017, when the employee’s physical access was removed while he was still in the PSP, and ended later that same day when the employee finally exited the PSP.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to properly secure a PSP is that an unauthorized person could gain access to the PSP and take action that has an adverse effect on the BPS. This risk was mitigated in this case by the following factors. First, the employee remains an employee in good standing, which reduces the likelihood that he would have done anything nefarious while within the PSP. Second, the employee had a valid reason for entering the PSP. He was specifically asked by his supervisor to work in the PSP that day [REDACTED]. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity’s compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) enhanced alarm response guidelines for security [REDACTED] to emphasize that processes must be followed regardless of the amount of time that has passed since an individual’s last entry; and 2) provided refresher training for the security [REDACTED] stressing the importance of validating an individual’s access within the Physical Access Control Systems when an [REDACTED] is denied. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019427	CIP-007-6	R5	[REDACTED]	[REDACTED]	12/23/2016	6/28/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On March 15, 2018 and August 16, 2018, the entity submitted Self-Reports to ReliabilityFirst stating that, [REDACTED] it was in noncompliance of CIP-007-6 R5. On January 25, 2018, while performing a review of the [REDACTED] devices, the entity discovered that it failed to change the passwords for [REDACTED] within the required 15 month timeframe. These [REDACTED] devices were installed on June 1, 2016. However, the entity failed to add these devices into its password management system at the time of installation. Consequently, the entity did not change the passwords until February 5, 2018, approximately 5 months late.</p> <p>The root cause of this first instance of the noncompliance was a lack of a documented process for adding these devices into the entity’s password management system and the entity’s failure to verify the accuracy of the information in the password management system. This root cause involves the management practices of implementation, because the error occurred when the entity installed these devices, and verification, in that the entity failed to verify the accuracy of the information in its password management system.</p> <p>Subsequently, the entity performed an extent of condition review pursuant to which it compared the records of [REDACTED] in its asset management system to its application for managing passwords. During this review, the entity identified one additional [REDACTED] that did not have its password changed at the time it was installed (i.e., December 23, 2016), or within the next 15 calendar months.</p> <p>The root cause of this second instance of the noncompliance was a lack of a documented process for [REDACTED] to follow when reporting configuration changes to existing [REDACTED]. In this case, the entity assigned the same IP address to two different [REDACTED] in the password management system and the asset management system. As a result, the entity was unaware that this additional [REDACTED] did not have its password changed on time. This root cause involves the management practice of asset and configuration management, which includes controlling changes to assets, and verification, because the entity failed to verify the accuracy of the information in its password management system and asset management system.</p> <p>The noncompliance began on December 23, 2016, the date the entity installed the additional [REDACTED] without changing its password. The noncompliance ended June 28, 2018, the date the entity changed the password on the last [REDACTED].</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to change the passwords on these devices in a timely manner is that it increases the likelihood of these passwords being compromised by unauthorized individuals. This risk was mitigated in this case by the following factors. First, with respect to the initial [REDACTED] identified, the entity was 5 months late changing the passwords, which reduced the amount of time that these passwords could have been compromised. Second, with respect to the additional [REDACTED] identified during the extent of condition review, that [REDACTED] does not have the ability to perform any control functions. Therefore, even if its password had been compromised, an unauthorized person would not have been able to use the device to impact other devices. Third, the [REDACTED] are protected by the entity’s defense-in-depth strategy, including both electronic and physical security controls. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity’s compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) changed the passwords on the [REDACTED] devices; 2) performed a validation comparing the [REDACTED] recorded in the access management system, the [REDACTED], and the [REDACTED] in the entity’s asset management system; 3) developed a process to perform a quarterly review of the [REDACTED] devices recorded in access management system compared to the asset management system; 4) developed a password process for the access management system that notifies the on-call [REDACTED] of the completion of [REDACTED] installation and the current device password; and 5) provided training on the newly implemented processes with the [REDACTED] teams. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019979	CIP-010-2	R2	[REDACTED]	[REDACTED]	2/27/2017	4/12/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On June 27, 2018, and August 30, 2018, the entity submitted Self-Reports to ReliabilityFirst stating that, [REDACTED] it was in noncompliance of CIP-010-2 R2. On November 1, 2017, while the cybersecurity team was performing a [REDACTED] review of [REDACTED] reports, the team discovered an alert that indicated [REDACTED] was unable to connect to the entity's [REDACTED]. Consequently, the entity was not monitoring for changes to the server's baseline.</p> <p>The cybersecurity team followed up with the [REDACTED] team to investigate the status of the [REDACTED]. When they did not receive a response back, [REDACTED] incorrectly assumed that the [REDACTED] had been powered off and was only being powered on when needed. [REDACTED]</p> <p>Subsequently, the [REDACTED] team attempted to run a [REDACTED] report for the [REDACTED] and discovered the same issue. That team concluded that the reason [REDACTED] could not connect to the [REDACTED] was because it had been removed [REDACTED] and [REDACTED]. Once it was made a [REDACTED], [REDACTED] could not connect to it because [REDACTED] needed to be modified. Once the modifications were made, [REDACTED] connected to the [REDACTED] and collected all of the configuration files.</p> <p>The root cause of this first instance of the noncompliance was a communication breakdown between the [REDACTED] team and the [REDACTED] team. When the [REDACTED] team noticed the alert, they contacted the [REDACTED] group, who never responded. This root cause involves the management practice of work management, which includes establishing a work management process that ensures proper coordination between business units.</p> <p>As part of its mitigation, the entity validated the configuration baselines for (a) all devices that have their baseline configuration automatically monitored by [REDACTED] and, (b) all high impact cyber assets that are manually monitored for baseline configuration changes. During the course of this validation review, the entity discovered issues with some of the devices that are manually monitored. Specifically, the entity discovered that for [REDACTED] device, it had performed one monitoring interval 1 day late. Additionally, the entity discovered that for [REDACTED], it had performed one monitoring interval 3 days late.</p> <p>The root cause of this second instance of the noncompliance was an error in the setup of the automated email notifications and workflows. The entity originally configured these reminders to start every 35 calendar days, rather than every 35 days from the subject matter expert's (SME) previous completion date. This configuration failed to take into account that SMEs sometimes complete their reviews earlier than the due date, which affects the completion deadline for the next review. This root cause involves the management practice of reliability quality management, which includes maintaining a system for deploying internal controls.</p> <p>The first instance of the noncompliance began on November 1, 2017, when [REDACTED] was first unable to communicate with the [REDACTED] and ended on April 12, 2018, when the entity modified the [REDACTED] [REDACTED] to [REDACTED]. The second instance of the noncompliance began on February 27, 2017, when the entity missed the first 35 day review period, and ended on February 28, 2018, when the entity completed the required reviews.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to monitor for changes to baseline configurations is that unauthorized changes could go undetected. This risk was mitigated in this case by the following factors. First, with respect to the first instance, the [REDACTED] continues to reside on the entity's secure, isolated network [REDACTED]. [REDACTED]. Consequently, in order to gain access to this [REDACTED], a user would need to have a [REDACTED]. Additionally, although [REDACTED] could not connect to the [REDACTED] for baseline monitoring purposes, [REDACTED] did not fail and continued to collect security log files where any security related event was investigated. Security patches also continued to be installed on the [REDACTED]. Second, with respect to the second instance, the entity missed the monitoring intervals for a maximum of three days, which reduces the risk of any unauthorized changes occurring. Additionally, all of the affected devices were protected by the entity's electronic defenses, including [REDACTED]. All interactive remote connection attempts into the ESP require [REDACTED]. Finally, the [REDACTED] have [REDACTED] to protect against the unauthorized use [REDACTED].</p> <p>No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) modified the [REDACTED] to allow [REDACTED] to connect to the [REDACTED] for baseline monitoring; 2) developed a formalized process for investigating and tracking issues following [REDACTED] alerts; 					

ReliabilityFirst Corporation (ReliabilityFirst)

Compliance Exception

CIP

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019979	CIP-010-2	R2	[REDACTED]	[REDACTED]	2/27/2017	4/12/2018	Self-Report	Completed
			3) performed a validation of CIP high impact assets automatically monitored by [REDACTED] to verify baseline configuration monitoring was being performed on all applicable assets at appropriate intervals; 4) developed and implemented a documented process for tracking and maintaining this [REDACTED]; 5) conducted a validation for CIP high impact assets that are manually monitored to verify baseline configuration monitoring is being performed on all applicable assets at appropriate intervals; and 6) configured, with respect to the second instance, automated email notifications and workflows for the 35-day clock based on the SME's previous completion date. 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
RFC2017017783	CIP-011-2	R1	[REDACTED]	[REDACTED]	4/19/2017	5/17/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On June 15, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance of CIP-011-2 R1. On May 11, 2017, an entity employee emailed Bulk Electric System (BES) Cyber System Information (BCSI) to 5 internal employees without the information being appropriately labeled as [REDACTED]. Additionally, one of the 5 employees on the email list was the sender's manager, who was not an authorized CIP user at the time the email was sent. Within 1 hour of the email being sent, the sender's manager identified the issue and escalated it to the CIP Senior Manager.</p> <p>Moreover, the same employee also saved the BCSI on a [REDACTED] that was not an approved electronic storage location for 23 days. There were 4 other employees who had access to this information and were not CIP trained. However, the entity found no evidence that any of these individuals accessed the BCSI.</p> <p>The root cause of the noncompliance was the employee's lack of awareness regarding the entity's information protection policies. This root cause involves the management practices of workforce management, which includes providing training, education, and awareness to employees, and information management, which includes managing information items' confidentiality.</p> <p>The noncompliance began on April 19, 2017, the date the employee saved the BCSI on the [REDACTED]. The noncompliance ended on May 17, 2017, the date the entity deleted the email including the BCSI and ensured the information was no longer on the [REDACTED].</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to properly protect BCSI is that it increases the likelihood that the information could be obtained by an unauthorized person. This risk was mitigated in this case by the following factors. First, the email was sent to only internal employees and the entity identified the mistake within one hour of transmission. Second, access to the [REDACTED] where the BCSI was stored was limited to 6 entity employees. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) deleted the emails from the individuals' mail files and from the email servers (including backup servers); 2) deleted the [REDACTED] data on the [REDACTED]; 3) had the employee complete the CIP Cyber Security training again as a refresher course; 4) performed a one-on-one review of the entity's Information Protection Program with employee; 5) included an Information Protection Program awareness review in the Compliance's [REDACTED] meeting; 6) distributed a communication reiterating the entity's Information Protection Program to individuals who are CIP certified; 7) implemented a quarterly spot check process to assess handling of BES Cyber System Information. This process included a random sample of [REDACTED] and business computer of individuals with authorized access to BES Cyber System Information; and 8) reviewed and updated the BES Cyber System Information section within the CIP training to include the approved electronic storage locations. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019182	CIP-011-2	R1	[REDACTED]	[REDACTED]	7/1/2016	12/4/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 2, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in noncompliance of CIP-011-2 R1. On November 13, 2017, an entity [REDACTED] discovered that Bulk Electric System (BES) Cyber System Information (BCSI) (i.e., [REDACTED]) was stored in an unapproved electronic storage location and the files were not labeled as [REDACTED]. The entity determined that the BCSI had been stored in this location since before the effective date of the Standard.</p> <p>The root cause of the noncompliance was lack of awareness by the [REDACTED] responsible for managing this type of information. These [REDACTED] continued to use the [REDACTED] that they used under Version 3, before this type of information was considered BCSI. This root cause involves the management practices of workforce management, which includes providing training, education, and awareness to employees, and information management, which includes managing information item confidentiality.</p> <p>The noncompliance began on July 1, 2016, the date the entity was required to comply with CIP-011-2 R1. The noncompliance ended on December 4, 2017, the date the entity moved the BCSI to an appropriate storage location.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to properly protect BCSI is that it increases the likelihood that the information could be obtained by an unauthorized person. This risk is minimized based on the following factors. First, all individuals with access to this storage location had current CIP training and Personnel Risk Assessments. Second, the storage location was protected electronically by [REDACTED]. Third, the storage location was protected physically within a Physical Security Perimeter. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) moved the [REDACTED] files for [REDACTED] to an approved BES Cyber System Information electronic storage location; 2) distributed an email communication to the [REDACTED] employees reiterating what is considered BES Cyber System Information as well as how to store and properly protect this type of information; 3) established a new electronic location within an existing approved BES Cyber System Information electronic storage location for the [REDACTED] to store [REDACTED] files; 4) conducted supplemental training for the [REDACTED] on what is BES Cyber System Information and the proper handling and storage of BES Cyber System Information per the entity’s Information Protection Program; 5) developed and implemented additional processes for the retrieving, handling, and storing of BES Cyber System Information associated with the [REDACTED] files; 6) completed a scan on each of the [REDACTED] personal computer hard drives to verify that BES Cyber System Information is no longer being stored in unapproved storage locations; and 7) completed a scan of [REDACTED] where [REDACTED] have access to verify that BES Cyber System Information is not being stored in unapproved storage locations. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021929	CIP-004-6	R5	[REDACTED]	[REDACTED]	5/18/2019	5/31/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 19, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5.</p> <p>On May 30, 2019, the entity discovered one shared account password that was not changed within 30 calendar days following the voluntary resignation (termination) of one employee. Although the individual’s unescorted physical access and Interactive Remote Access (IRA) were removed on the termination date, the shared account password was not changed until 44 days after the termination date (14 days late).</p> <p>The entity identified this issue through an internal control (a quality assurance check) that is performed on password changes due to a termination or a job transfer. [REDACTED] Immediately after the discovery of this unchanged password, the entity entered and approved a change request to expedite changing of the shared account password by the next day.</p> <p>This noncompliance involves the management practices of work management, workforce management, and planning due to an unclear procedure that created confusion around responsibilities. The root cause of this noncompliance was that the responsibility for changing the shared account password had been reassigned to a new owner during the process of changing all the shared passwords known to the terminated user. At the time of reassignment, the entity failed to create a task to track completion of the password change in the entity’s task workflow system for the new owner to complete the password change. As a result, the task workflow system never issued an email reminder to the new owner to change the password.</p> <p>This noncompliance started on May 18, 2019, when the entity was required to change the shared password within 30 days following the employee’s termination and ended on May 31, 2019, when the entity changed the shared password.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is allowing a terminated employee to retain access to Cyber Assets which could allow the terminated employee to exploit those Cyber Assets. The risk is minimized because the employee’s termination was a voluntary resignation and the entity removed the employee’s unescorted physical access and IRA on the employee’s last day of employment prior to departure. The entity accomplished this by retrieving the employee’s [REDACTED] on his last day. Additionally minimizing the risk, the shared account password was changed just 14 days late. Lastly, any changes made to any Cyber Assets would have been detected by the entity’s configuration monitoring system. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history does not warrant an alternative disposition method and should not serve as a basis for applying a penalty because most of the prior noncompliances are distinguishable as they involved different circumstances or root causes. For the one issue that is arguably similar, ReliabilityFirst determined that the current noncompliance continues to qualify for compliance exception treatment as it posed only minimal risk and is not indicative of a systemic or programmatic issue. Further, the entity quickly identified the noncompliance and corrected the issues through its internal controls.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) identified the new owner in the password management system, created the password change task, and changed the shared account password; 2) revised entity task workflows and now requires performing the quality assurance check after each shared account password known to a user has been changed, instead of waiting to perform the validation until all password changes for a termination/job transfer have been completed; and 3) implemented, for this specific shared account password, another internal control to reduce the risk of recurrence. [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
RFC2019021928	CIP-008-5	R3	[REDACTED]	[REDACTED]	2/27/2019	3/14/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 19, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-008-5 R3.</p> <p>Following a Cyber Security Incident Response (CSIR) plan test, the entity had identified lessons learned that required an update to defined roles in the CSIR plan. Although the entity documented the lessons learned and updated the CSIR plan within 90 calendar days, the formal notification to each group with a defined role in the CSIR occurred 105 days after completion of the test (15 days late).</p> <p>Additionally, although the entity submitted the updates for review to the groups having defined roles in the CSIR plan within the 90 calendar days, the official notification to those groups that the CSIR plan had been updated was not issued on time.</p> <p>The entity identified this noncompliance during the execution of an internal control (an annual internal compliance review). The reviewed identified that the notification distributed to the personnel/groups for the CSIR Test conducted in November was issued on the 105th calendar day after the exercise.</p> <p>This noncompliance involves the management practices of work management, workforce management, and planning due to an unclear procedure that created confusion around responsibilities. The root cause of this noncompliance was because responsibility for completing the official notification was not clearly defined. After resolving responsibility and issuing the notification, the personnel involved did not recognize it was beyond the 90 calendar days which caused a delay in identifying this instance.</p> <p>This noncompliance started on February 27, 2019, when the entity was required to notify each person or group with a defined role in the CSIR plan of the updates to the CSIR plan based on any documented lessons learned, and ended on March 14, 2019, when the entity completed the required notifications.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed is that updates to the CSIR may not be communicated to relevant personnel and groups which could negatively impact the quality of the response to an actual Cyber Security Incident. The risk is minimized because the entity submitted the CSIR plan changes for review to the persons/groups who had a defined role within the 90 calendar day requirement. Additionally, the CSIR plan changes were documented and approved within 90 calendar days. Lastly, the notification was sent just 15 days late. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the CSIR plan to provide a clear understanding of the group responsible for the distribution of notifications within 90 calendar days following a test or actual event when updates are made to the CSIR plan based on any documented lessons learned identified during the test or actual event; and 2) updated the CSIR plan to include the creation of a task using the entity task workflow tool. The task will be assigned to the responsible group for communicating any updates made to the CSIR plan based on documented lessons learned within 90 calendar days. The tool will issue email reminders as the task is coming due and escalate notifications to entity management if not completed as the deadline approaches. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021718	CIP-011-2	R1	[REDACTED]	[REDACTED]	12/10/2018	2/5/2019	Self-Report	June 19, 2020
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On June 18, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-011-2 R1.</p> <p>On January 31, 2019, as a result of a manual analysis of an access request for logical user access to Bulk Electric System (BES) Cyber Security Information (BCSI) storage locations, the entity discovered that it provisioned inappropriate access to one individual to BCSI storage locations [REDACTED] prior to the individual taking the entity’s Information Protection training.</p> <p>[REDACTED] the individual who identified the first issue did a search of prior results resulting in the identification of four additional users who required access, [REDACTED] to BCSI storage locations for job duties but had not taken the entity’s Information Protection training prior to their access being provisioned [REDACTED]. All four of the individuals were intended to have access to the BCSI storage locations, however their access was granted [REDACTED] which meant the individuals did not take the entity’s Information Protection training per CIP-011-2 R1 prior to receiving access.</p> <p>This noncompliance involves the management practices of asset and configuration management and workforce management. The root cause is the undefined logical access provisioning procedures [REDACTED]. The lack of clarity, arising from poor asset and configuration management, within procedures [REDACTED] resulted in individuals receiving access to BCSI storage locations prior to the entity’s Information Protection training being taken, which implicates workforce management as those individuals should not have been granted access before completing the training.</p> <p>This noncompliance started on December 10, 2018, when the entity granted access to the first of the five users before they had taken the entity’s required Information Protection training and ended on February 5, 2019 when the users completed the required training.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed is that granting individuals authorized logical access to BCSI storage locations prior to receiving Information Protection training could result in the mishandling or misuse of BCSI data elements. The risk is minimized because all of the users were intended to have logical access to the BCSI storage locations both prior to and after taking the Information Protection training. The users also received the training only two months late. Additionally, the entity self-identified the noncompliance. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) digitally distributed, upon discovery, the BCSI training [REDACTED] to the identified individuals who were granted BCSI access; 2) updated the entity’s Information Protection Plan (IPP) to include: specific requirements for access to BCSI for physical individuals, individual accounts, shared accounts, and service accounts or other accounts and identification of and reference to electronic BCSI storage locations; <p>[REDACTED]</p> <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by June 19, 2020:</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021718	CIP-011-2	R1	[REDACTED]	[REDACTED]	12/10/2018	2/5/2019	Self-Report	June 19, 2020
			<p>6) will inventory and verify, all individuals with access [REDACTED] accounts accessed via password vault to ensure they have proper authorization and training for access to BCSI information;</p> <p>7) will develop an awareness training plan for BCSI users. The plan will include determining the difference between a document of record from convenience copy, examples, and BCSI handling ownership responsibilities. The document of record is BCSI stored in a declared BCSI storage repository as per the IPP where convenience copies are duplicates used for immediate business use and to be destroyed when the business use concluded. This awareness training will reinforce the proper definition, use, transport, and storage of BCSI, detail the requirements for BCSI access with focus on what accounts are allowed to access BCSI;</p> <p>8) will document a review of BCSI storage locations in business unit and corporate directory. The entity will review for consolidation of locations where possible and update locations within the entity's IPP; and</p> <p>9) will document requirements of proper authorization and training within [REDACTED] password vaults and/or access control lists. This will serve as additional awareness for those accessing [REDACTED] (shared accounts) and the audience who may receive any output from [REDACTED] accounts.</p> <p>Additional time is needed to develop the awareness training plan and review BCSI locations for consolidation where possible.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021808	CIP-006-6	R2	[REDACTED]	[REDACTED]	6/26/2019	6/26/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 5, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-006-6 R2. On June 26, 2019, the HVAC unit for one of the Physical Security Perimeters (PSPs) at the entity’s backup control center failed, causing excessive heat inside the PSP. As a result, the entity’s [REDACTED] received a request to have the PSP door propped open to reduce the heat, which it approved. During the time that the door was propped open, the entity had an authorized individual in place at the door to sign people in and out. Additionally, the [REDACTED] operators were monitoring the door as well. During this time, an HVAC technician entered the PSP through the propped door a total of 5 times. Although this individual was properly signed in and out each time, the authorized individual acting as an escort did not maintain visibility of the HVAC technician while he was in the PSP.</p> <p>The root cause of this noncompliance was the escort’s failure to follow established procedures for maintaining visibility of visitors. This root cause involves the management practice of workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on June 26, 2019, when the escort failed to maintain visibility of the HVAC technician and ended later that same day, when the HVAC technician completed his work and exited the PSP for the final time.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The risk posed by failing to maintain visibility of a visitor within a PSP is that the visitor could take adverse actions causing harm to the BPS without the entity’s knowledge. This risk was mitigated in this case by the following factors. First, the asset located within the PSP is a network communications switch that is used to transfer camera feeds (used for investigative purposes) and Physical Access Control System (PACS) controller information back to the primary PSP. There is no interface connected to this switch that would allow for configuration changes and all unused interfaces are configured to be “administratively down,” which reduces the likelihood that a visitor could harm the entity’s network from within this PSP. Second, all assets within the PSP are monitored from multiple locations, which makes it more likely that the entity would have been able to quickly detect if the visitor had taken any adverse actions. ReliabilityFirst also notes that, based on an after-the-fact investigation by the entity, there was no indication that this visitor had taken any adverse actions. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) created a report to determine if any tamper alarms were received from the PACS controller during the event; 2) reviewed switch configuration settings to determine if any changes were made and to verify unused ports were configured to be “administratively down”; and 3) conducted a refresher training with the individuals who acted as escorts during the event with specific emphasis on their responsibilities as escorts. A review of the incident itself was performed as part of the 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
RFC2019021197	CIP-007-6	R5	[REDACTED]	[REDACTED]	7/1/2018	12/31/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On March 1, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-007-6 R5. The entity completed its acquisition of all [REDACTED] assets on [REDACTED]. Subsequently, on [REDACTED], the entity discovered that the distributed control system (DCS) was still using a default password for the associated service account at its [REDACTED] generation plant. The service account is a non-interactive system account which is used for computer-to-computer communications. Upon discovery, the entity contacted the system vendor to understand how to appropriately change the default password. Note that while the self-report also stated that it found this issue at the entity’s [REDACTED] generation plant, pursuant to written notice provided by [REDACTED] as of [REDACTED] that plant no longer met the criteria to be considered Medium Impact because its Automatic Voltage Regulator system was no longer critical to the derivation of an Interconnection Reliability Operating Limit and its associated contingencies. Therefore, ReliabilityFirst determined that this issue did not constitute a compliance issue at this plant.</p> <p>The root cause of this noncompliance was the entity’s failure to identify this default password and change it prior to implementation. This root cause involves the management practices of implementation because this issue should have been identified during the implementation process, and information management, which includes managing information confidentiality.</p> <p>This noncompliance started on July 1, 2018, when the entity was required to comply with CIP-007-6 R5 and ended on December 31, 2019, when the entity changed the default password. [REDACTED]</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The risk posed by failing to change default passwords is that those passwords could be compromised by unauthorized individuals to cause harm to the BPS. This risk is mitigated in this case based on the following factors. First, the DCS resides behind a data diode that physically prevents External Routable Connectivity, meaning that an unauthorized individual would require physical and local electronic access to the DCS in order to exploit the default password vulnerability. To limit physical and local electronic access, [REDACTED]. Second, this account was a service-only account whose local policy was set to “Deny log on locally,” which prevents interactive user access. Third, even if an unauthorized individual gained access to the DCS, [REDACTED]. Fourth, as of [REDACTED] sent written notice of this fact to the entity on this date.) [REDACTED] is no longer considered Medium Impact because its AVR system is no longer critical to the derivation of an Interconnection Reliability Operating Limit (IROL) and its associated contingencies, which mitigates the potential impact to the system if an unauthorized individual successfully exploited the default password vulnerability. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> worked with the vendor to establish the necessary activities to change the password and has scheduled outages for both generation plants; implemented alarms at the [REDACTED] generation plant such that operators are notified of any AVR status change and communicate to the operators that any such change that is not anticipated should be investigated. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021194	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/1/2018	7/28/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On March 1, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1. On July 25, 2018, during a routine internal spot check, the entity discovered a missing baseline for its on-site monitor (OSM) system, which is classified as a Protected Cyber Asset (PCA). Upon discovery, the entity ran a system information gathering script to extract the baseline.</p> <p>The root cause of this noncompliance was inadequate controls in place to ensure that plant personnel captured all required baselines. This root cause involves the management practices of asset and configuration management, which includes establishing inventory and configuration baselines, and reliability quality management, which includes maintaining a system for identifying and deploying internal controls.</p> <p>This noncompliance started on July 1, 2018, when the entity was required to comply with CIP-010-2 R1 and ended on July 28, 2018, when the entity generated the baseline. [REDACTED]</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to establish baselines is that the entity could make changes to the asset that have unintended adverse consequences. This risk was mitigated in this case by the following factors. First, the entity identified and corrected the issue quickly, minimizing the amount of time that the risk could have been realized. Second, this issue was limited to one system out of the entity’s entire CIP inventory, which indicates that this was an isolated incident. ReliabilityFirst also notes that no changes were made to the asset during the time of the noncompliance. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) created detailed job aids and checklists to help plant personnel establish and monitor baselines; and 2) established monitoring controls to verify proper performance of baselining. These controls are performed on a frequency commensurate to the likelihood and potential impact of non-compliance. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018020880	CIP-006-6	R1, P1.8	[REDACTED]	[REDACTED]	10/09/2018	10/09/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 20, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R1, P1.8. The Entity failed to log entry of an employee with authorized unescorted physical access into a Physical Security Perimeter (PSP).</p> <p>On October 9, 2018, an employee with authorized unescorted access into the [REDACTED] (Employee A), attempted to access the PSP using the Entity-issued fob and personal identification number (PIN). Employee A had forgotten the personal employee primary badge and attempted to use the backup fob to gain access. The Physical Access Control System (PACS) denied access on several attempts to the backup fob. Employee A then called into the PSP, and another employee with authorized unescorted access (Employee B) let Employee A into the PSP. Employee A did not sign in using the provided visitor log once inside the PSP.</p> <p>Because of Employee A’s unsuccessful access attempts, the Entity’s PACS generated unauthorized access attempt alerts through the paging system, which notified the Entity’s on-call [REDACTED]. In response to the alerts, the [REDACTED] logged into the PACS to view the logged unsuccessful attempts, and into the camera system to analyze the events that triggered the alerts. The video revealed that, after the badge reader denied access, Employee B allowed Employee A entry into the PSP. The [REDACTED] also noted that Employee A did not sign into the PSP visitor log. In addition, the [REDACTED] visited the PSP and reviewed the logs and confirmed that Employee A had not signed in. Further investigation revealed that Employee A’s fob was still active but that Employee A kept the fob next to other cards inside the employee’s wallet and had attempted to gain access by swiping the wallet without removing the fob. The physical security analyst suspected that the resulting access denials were caused because another card within Employee A’s wallet was read by the PACS.</p> <p>The Entity conducted an immediate extent-of-condition (EOC) by reviewing the PACS failed badge attempt notifications and discovered that no other notifications had been received.</p> <p>This noncompliance started on October 9, 2018, when Employee A failed to sign the visitor log upon being manually let into the PSP by Employee B, and ended on October 9, 2018, when Employee A exited the PSP.</p> <p>The Entity determined the cause for this noncompliance was inadequate training regarding PSP logging requirements for manual PSP entry. The responsibility to sign-in fell on Employee A, who did not follow the PSP entry procedures. Employee A did not sign the visitor log because the employee incorrectly believed that by signing the visitor log, a visitor escort would be required, which would prevent the employee from performing their daily duties.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity’s failure to log entry of an employee with authorized unescorted PSP access could hinder an after-the-fact investigation to determine who had entered the PSP of situations that may warrant the use of the logs. However, Employee A was reporting to his normal work location to perform authorized duties. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) had a phone conversation with Employee A and explained the access process and reiterated the importance of following entry procedures into designated PSPs when one’s assigned fob is unavailable or not working, regardless of the reason; 2) sent an email from Entity compliance to Employee A’s manager to reinforce the access process and expectations for entering the [REDACTED]; and 3) conducted training to all employees requiring access to CIP applicable systems, which restated and explained more fully the process and expectations for gaining access into PSPs. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018020881	CIP-003-6	R1	[REDACTED]	[REDACTED]	07/01/2018	11/06/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 20, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-003-6 R1. The Entity failed to review and obtain [REDACTED] approval at least once every 15 calendar months for one or more documented cyber security policies.</p> <p>On October 17, 2018, during the gathering of documentation for an internal CIP program gap analysis, the Entity discovered that the [REDACTED] had not reviewed and approved the Entity Cyber Security Program within 15 months from the last review cycle (March 31, 2017). The review was due by July 1, 2018, but the cyber security policies in the Cyber Security Program had only been reviewed by the [REDACTED].</p> <p>The Entity performed an extent-of-condition assessment by reviewing its cyber security policies and found no other instances where the review and signature did not occur when required.</p> <p>This noncompliance started on July 1, 2018, when the [REDACTED] was required to review and approve the cyber security policies, and ended on November 6, 2018, when the [REDACTED] reviewed and approved the cyber security policies.</p> <p>The cause of this noncompliance was management oversight. Management failed to ensure that the necessary internal control, i.e., a workflow process, was implemented to ensure the [REDACTED] [REDACTED]s review and approval occurred in a timely manner.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity [REDACTED] failure to review and approve the cyber security policies in the Entity Cyber Security Program when required could have caused confusion to individuals reviewing policies with no recently signed Cyber Security Program on the internal website. However, the Entity had not made any changes to the Cyber Security Program from the previously approved and signed version. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revised the Cyber Security Program document by updating job titles and clarified what documentation supports the implementation of the Entity’s overarching program referenced in CIP-003-6 R1; 2) had the [REDACTED] review and sign the Entity Cyber Security Program document; 3) developed a workflow process to serve as an internal control for timely review of program documentation and other CIP related tasks to include assignment to the appropriate subject matter expert and manager along with e-mail notifications to the assignees and escalation if no action is taken within the required timeframe. The Entity [REDACTED] also monitors the workflow and updates it as needed; and 4) conducted a comprehensive CIP program 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
SERC2019021386	CIP-009-6	R1, P1.4	[REDACTED]	[REDACTED]	05/23/2018	10/25/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 17, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-009-6 R1, P1.4. The Entity failed to verify the successful completion of the backup processes in P1.3 and to address any backup failures for [REDACTED] network switches.</p> <p>On March 29, 2019, during a comprehensive review of the Entity’s compliance program, the Entity determined that it was unable to produce evidence verifying successful completion of backup processes for [REDACTED] network switches (Electronic Access and Control Monitoring Systems (EACMS)) in its primary data center from May 23, 2018 to October 25, 2018. The Entity’s data backup plan requires the switches to be backed-up daily.</p> <p>On May 23, 2018, there was an unsuccessful software upgrade on the [REDACTED] network switches, which the Entity then restored from a backup configuration file. After restoration of the switches, the Entity did not update the user account credentials to enable the backup system access to switch configurations. This resulted in the backups not executing from May 23, 2018 through October 25, 2018.</p> <p>The Entity performed an extent-of-condition assessment by verifying all other switch backups within its backup software and determined that the [REDACTED] network switches at issue were the only ones affected.</p> <p>This noncompliance started on May 23, 2018, when the Entity restored the [REDACTED] network switches and did not correct the user account credentials, and ended on October 25, 2018, when the Entity corrected the user account credentials for the [REDACTED] network switches and verified the backups were successfully completed.</p> <p>The cause of this noncompliance was management oversight for failing to implement adequate internal controls to verify backup logging was working properly after a restoration of the switches.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity’s failure to ensure the backups were successful could have hindered its ability to recovery the switches when needed - potentially impacting the network access at one site to [REDACTED]. However, the [REDACTED] switches are [REDACTED] together in a high availability configuration requiring [REDACTED] switches to fail at the same time before any impact to the network would occur. The Entity compared the switch backup configurations dating back prior to May 23, 2018, and determined that the configuration did not change during that time in a manner that would prevent expedient recovery of critical services. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) entered the correct username and password to immediately begin backups of the switches; 2) modified the data backup and protection plan to require the personnel responsible for reviewing the backup configuration file to insert a comment in the backup system noting the name of the reviewer and the date/time of the review; 3) conducted training regarding this change in process for all relevant [REDACTED]; and 4) created a monthly Microsoft Outlook calendar reminder to notify the responsible personnel of the need to complete the backup 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
SERC2019021387	CIP-006-6	R2, P2.2	[REDACTED]	[REDACTED]	11/30/2016	03/13/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 18, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R2, P2.2. The Entity had nine instances where it failed to properly complete visitor logs with the required elements for its Physical Security Perimeters (PSPs).</p> <p>On January 14, 2019, during a comprehensive review of the Entity’s compliance program, the Entity determined that there were gaps in its documentation for logging of visitors into and out of its PSPs containing medium impact Bulk Electric System Cyber Systems. While the Entity’s visitor program documentation outlines how to comply with CIP-006-6 R2, P2.2, Entity personnel did not maintain the visitor program logs in such a way as to ensure it properly recorded the required elements for each and every visitor.</p> <p>On March 13, 2019, the Entity completed the extent-of-condition (EOC) assessment by reviewing of all manual visitor logs spanning July 1, 2016 through March 13, 2019. As a result of the EOC, the Entity determined that since the Standard and Requirement became mandatory and enforceable on July 1, 2016, there were nine total manual log entry omissions relating to eight visitors across [REDACTED]. For the nine instances of failure to properly log visitors, the Entity identified four instances in which it did not record an escort, and five instances where it did not record the time of a visitor’s last exit.</p> <p>This noncompliance started on November 30, 2016, when the first incomplete visitor log entry occurred, and ended on March 13, 2019, when the last incomplete visitor log entry occurred.</p> <p>The causes for this noncompliance were inadequate training related to visitor escort responsibilities, and management oversight to have an internal control in place for regular collection and review of the visitor logs for compliance verification.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity’s failure to properly record visitor log required information could hamper its ability to perform after-the-fact investigations regarding PSP access. However, as the manual logs included all visitor names and the Entity employs door alarms that would have triggered an alert to notify security of any unauthorized entry into a PSP. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) provided training to personnel with authorized unescorted access regarding the requirement to fully complete all visitor logs upon each entry into and exist from a PSP; 2) provided additional training materials to all personnel and vendors related to visitor access and visitor logging requirements; 3) revised its paper visitor log sheets to state, “Escorts must ensure all fields are completed upon entry and exit to the PSP”; and 4) implemented an internal control for the Entity’s [REDACTED] department to collect and review the logs on a monthly basis. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2019021471	CIP-004-6	R1, P1.1	[REDACTED]	[REDACTED]	07/01/2016	04/01/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On May 3, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R1, P1.1. The Entity failed to provide security awareness material on a quarterly basis that reinforces cyber security practices for personnel with authorized electronic or authorized unescorted physical access to Bulk Electric System (BES) Cyber Systems (BCSs).</p> <p>On February 26, 2019, during a comprehensive internal program and system review, the Entity discovered that it was not providing security awareness material on a quarterly basis to [REDACTED] contractors who had authorized unescorted physical and/or electronic access to BCSs. Of the [REDACTED] contractors, [REDACTED] had authorized unescorted physical access, [REDACTED] had authorized electronic access, and [REDACTED] had both authorized physical and electronic access to BCSs.</p> <p>The Entity provides quarterly security awareness material through various means, including e-mail, onsite posters and signage, and online training. The Entity sends quarterly security awareness material to personnel via e-mail, but the contractors at issue did not have Entity e-mail accounts and were thus not receiving the Entity’s security awareness material. The Entity’s e-mail accounts are the primary method of security awareness communication for contractors since the contractors are not onsite prior to being granted access.</p> <p>On June 14, 2019, the Entity completed an extent-of-condition review and determined that it had authorized access to [REDACTED], not [REDACTED], contractors with access to medium impact BCSs. [REDACTED] contractors had been trained and authorized for access, but were never actually granted access to BCSs. Thus, the Entity had a total of [REDACTED] contractors with actual physical and/or electronic access to BCSs and were not receiving security awareness materials.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on April 1, 2019, when the Entity provided security awareness material to all contractors via e-mail.</p> <p>The cause of this noncompliance was management oversight for failing to ensure that the access management procedure included a step to include authorized contractor e-mails to the distribution list for quarterly security awareness material.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity’s failure to provide quarterly awareness material to contractors with authorized unescorted physical access or electronic access could have caused personnel to become inattentive to potential security threats. However, the contractors at issue had received the proper cyber security training and had personal risk assessments on file prior to being granted access. Additionally, given the work the contractors were performing for the Entity and their professional experience, the contractors were intimately aware of potential cyber security threats. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) sent quarterly awareness material via e-mail to all current contractors with authorized access; 2) modified its [REDACTED] by adding a step in its process to include contractors with authorized access to the distribution list that receives quarterly security awareness material, or otherwise provide awareness material to contractors upon reinstatement of access; and 3) provided additional training to [REDACTED] on the revised 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
SERC2019021518	CIP-005-5	R2, P2.1	[REDACTED]	[REDACTED]	07/01/2016	05/10/2019	Self-Report	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>	<p>On May 10, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-005-5 R2, P2.1. The Entity failed to restrict Interactive Remote Access (IRA) through an Intermediate System such that the Cyber Asset initiating IRA does not directly access an applicable Cyber Asset.</p> <p>On May 3, 2019, during a comprehensive internal program and system review, the Entity discovered that it failed to recognize that IRA was used for a Cyber Asset outside of the Electronic Security Perimeter (ESP) to access a Cyber Asset inside the ESP because the employee performing the work did not fully understand what constituted IRA. The Cyber Asset inside the ESP provided “read only” access to personnel from Cyber Assets outside the ESP on the Entity corporate network, and the Entity did not restrict access to it through an Intermediate System. These pages personnel assessed contained information that could not be modified, and did not provide any control capability for any Bulk Electric System (BES) Cyber Systems (BCSs). The users request access to this information using a web browser from non-BES Cyber Assets outside of the ESP. The Entity previously evaluated the connection and incorrectly believed that it did not qualify as an IRA because the functionality was “read only” access.</p> <p>The scope of this noncompliance involved [REDACTED]</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable and the Entity did not restrict IRA through an Intermediate System, and ended on May 10, 2019, when the Entity removed the access to the web-server inside the ESP and created a web-server outside of the ESP to host the read-only page.</p> <p>The cause for this noncompliance was inadequate training. The individual was trained but the Entity’s training failed to clearly define IRA.</p>							
<p>Risk Assessment</p>	<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The Entity’s failure to protect the applicable Cyber Asset through the use of an Intermediate System could have allowed unauthorized individuals to gain access to confidential non-BES Cyber System Information. However, the Entity restricted the informational page as “read only” and therefore could not affect the operation of BCSs. Additionally, access to the web page required that the user be on the corporate network and defense in depth protections (i.e., intrusion detection systems and malware prevention) provided additional measures mitigating any potential risk to the BPS. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>							
<p>Mitigation</p>	<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) The Entity created a webserver outside of the ESP to host the read-only page. This page now uses a push from CIP to non-CIP to populate the data and eliminate the non-CIP web browser ability to communicate directly with the webserver inside CIP; and 2) provided IRA definition/clarification training to subject matter experts and appropriate Entity 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
SERC2018020051	CIP-003-6	R1, R1.2	[REDACTED]	[REDACTED]	04/01/2017	07/12/2018	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 violation.)			<p>On July 19, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-003-6 R1, R1.2. The Entity’s [REDACTED] failed to review and approve the documented low impact cyber security policies.</p> <p>On July 12, 2018, a newly hired [REDACTED] completed the 15-month review and approval of its cyber security policies and discovered the policies for low impact assets were previously improperly approved by the internal NERC Compliance Manager. The former [REDACTED] misinterpreted the delegation process in CIP-003-6 R4 and had inappropriately delegated cyber security policy approval authority to the NERC Compliance Manager. Although CIP-003-6 R4 allows the delegation of specific tasks, it does not allow the delegation of authority to approve the policies.</p> <p>This noncompliance started on April 1, 2017, when the [REDACTED] failed to approve the low impact cyber security policies, and ended on July 12, 2018, when the [REDACTED] approved the policies.</p> <p>The cause of this noncompliance was misinterpretation of the standard. The Entity erroneously believed that CIP-003-6 R4 allowed approvals of CIP cyber security policies to be delegated.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity’s approval delegation for CIP cyber security policies to a non-[REDACTED] could have created an unclear line of authority and ownership for security matters. However, the Entity did have policies in place, which were reviewed and approved within 15 months by a delegate at the request of the [REDACTED]. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) obtained CIP Senior Manager approval of its low impact policies; 2) communicated to the [REDACTED] that only the [REDACTED] could sign the CIP-003-6 policies; and 3) reviewed all policies with the [REDACTED], and others to ensure correct approval. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2019021419	CIP-007-6	R5 P5.5.1	[REDACTED]	[REDACTED]	01/30/2018	09/12/2018	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 violation.)			<p>On April 30, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5, P5.5.1. The Entity failed to have a password length that was the maximum length supported by the Cyber Asset.</p> <p>The Entity’s field personnel accessed [REDACTED] medium relay devices to perform maintenance activities in 2018. In accordance with the Entity’s procedure, the field personnel contacted the Entity’s Emergency Management System (EMS) personnel to request access to the devices. The EMS personnel modified the complex password to a lesser character complex password to allow the field personnel to obtain easy access to the devices. Upon completion of the maintenance by the field personnel, the EMS personnel was then required to run a program to reset the password to the higher complexity. However, the EMS personnel failed to reset the passwords, which resulted in this noncompliance. The passwords were set to [REDACTED] character passwords when the devices had the capability of an [REDACTED] character password. The Entity discovered this on February 28, 2019 when it performed a periodic review.</p> <p>The extent-of-condition consisted of a review of relay password-related evidence for all substations in service and for managed password reports from the [REDACTED] devices and change ticket orders from January 2018 through September 2018. The Entity reviewed the passwords for this time period because the EMS support staff performed a system-wide password reset in January 2018 and September 2018 that covered all potentially applicable devices. The Entity did not find additional instances of noncompliance.</p> <p>This noncompliance started on January 30, 2018, when the Entity failed to reset the relay password to the higher complexity parameter, and ended on September 12, 2018, when the password complexity level was reset.</p> <p>The cause of the violation was management oversight, specifically a deficient process. Management failed to update its process when CIP version 5 took effect to include instructions to not allow modifications of the the password complexity.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity’s failure to enforce proper password lengths for the relays could have resulted in a malicious actor, with physical access to the devices, to take administrative control of the relays and possibly affect transmission or generation assets. The risk was reduced due to layered security, such as, a security guard at the gate, badge access to enter plant facility, and badge with access rights to enter PSP, as the PSP was located inside a generation plant. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) reset the passwords to meet the length and complexity requirements; 2) performed a root cause analysis; 3) performed an extent-of-condition review; 4) updated the internal operating instruction to state that when field personnel calls System Operations for the password to access the devices, System Operation will only provide the current password that contains the maximum character length and complexity requirements and will not change the password to be simplified. When the work is complete, field personnel is required to notify the System Operations so they can run the password reset program; and 5) provided training on requirement, password change process, and changes to the internal relay maintenance password operating instruction 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
SERC2018020333	CIP-002-5.1a	R2; P2.1; P2.2	[REDACTED]	[REDACTED]	02/01/2017	09/06/2018	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 violation.)			<p>During a Compliance Audit conducted from [REDACTED], SERC determined that the Entity, as a [REDACTED], was in noncompliance with CIP-002-5.1a R2. The Entity did not have evidence to show that it had conducted a review of the identifications of its Bulk Electric System (BES) Cyber Systems (BCSs) and their associated BES Cyber Assets (BCAs) per P2.1 and approvals of such reviews by its [REDACTED] per P2.2 at least every 15 calendar months.</p> <p>In March 2018, the Entity's laptop that was used to track the 15 calendar month review and approvals suffered a hard drive failure. As a result, the only record (original paper copy) that the Entity had to show compliance with the Standard was from October 9, 2015, when [REDACTED] completed its asset risk determinations evaluations of its [REDACTED] Bulk Electric System (BES) [REDACTED], Control Centers, and associated [REDACTED] Facilities. That evaluation classified all assets as low impact and the [REDACTED] had signed the report and approved the evaluation.</p> <p>This noncompliance started on February 1, 2017, when the Entity could not provide evidence to show that the 15 calendar month review and approval occurred, and ended on September 6, 2018, when the Entity performed its review and approval as required.</p> <p>The cause of this noncompliance was ineffective resource management for failing to allocate sufficient resources to track and maintain compliance with the requirement. Management should have had a secure and restricted CIP-002-5 central repository to store electronic documentation in the event of a hard drive failure.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to retain evidence of required review and approvals could have left unknown BCAs, Physical Access Control System (PACS), and/or Electronic Access Control and Monitoring System (EACMS) undocumented and not properly protected providing potential impact to the reliability of the BES. The Entity reduced this risk as it is required to meet [REDACTED] for all information systems. [REDACTED] The Cyber Assets associated with the Entity's facilities are covered by [REDACTED]. The cyber systems at the affected locations all operate [REDACTED].</p> <p>Furthermore, the subsequent review and approval of the BES assets found that no changes had occurred from the October 9, 2015 asset determination that documented that the [REDACTED] BES [REDACTED], Control Centers, and associated [REDACTED] totaled [REDACTED] of net real power, with the largest single plant being approximately [REDACTED]. Each site has [REDACTED] BCAs with a single separate PACS and EACMS. No harm is known to have occurred.</p> <p>SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed a review of its CIP-002-5 Assets and the associated Cyber Assets in accordance with its Asset Risk Determination Matrix; . 2) implemented a secure CIP-002-5 central repository for electronic documentation, which is considered sensitive but not classified, and communicated the central repository to Staff; 3) updated that the list of Cyber Assets was reviewed, approved and signed by its [REDACTED]; 4) reorganized its technical manpower to establish a dedicated team to monitor and track NERC compliance and communicated this to 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
TRE2018020581	CIP-006-6	R1; R1.4	[REDACTED] (the "Entity")	[REDACTED]	08/10/2017	08/10/2017	Self-Report	06/01/2020
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 24, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-006-6 R1.4. In particular, the Entity was unable to monitor for unauthorized access through a physical access point into a Physical Security Perimeter (PSP) for 84 minutes. The PSP at issue has primary and backup network connections to facilitate monitoring for unauthorized access. Due to the incorrect implementation of an authorized change to the networking equipment associated with the primary network connection, the primary network connection was out of service from June 26, 2017 to August 17, 2017. During this time, the secondary connection was initially functioning as intended. However, on August 10, 2017, at 15:38 the service provider for the secondary network connection experienced an unplanned outage. The Entity dispatched personnel to conduct human monitoring of the PSP during the outage. Personnel arrived on site on August 10, 2017, at 17:02. The Entity maintained personnel on site until the service provider for the secondary network connection resolved its outage and communications returned to normal.</p> <p>The root cause of this noncompliance was a lack of detail in work instructions. The Entity has deployed primary and backup network connections so that if one network connection fails, the other network connection is available for use. The outage experienced by the service provider of the secondary network connection would have been a non-issue if the primary network connection was working as intended. However, due to poor work instructions an authorized change to the networking equipment associated with the primary network connection was not implemented properly, resulting in the extended unavailability of the primary network connection.</p> <p>This noncompliance started on August 10, 2017, when PSP monitoring became unavailable and ended on August 10, 2017, when Entity staff arrived on site to manually perform PSP monitoring.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was related to the monitoring of a single PSP for a [REDACTED]. Additionally, the Entity quickly dispatched personnel to the affected PSP upon losing communications with the PACS equipment at the PSP, resulting in a very short noncompliance duration. No harm is known to have occurred.</p> <p>Texas RE determined that the Entity's compliance history should not serve as an aggravation to the risk. The Entity does have compliance history related to CIP-006-6 R1.4; however, the instances of noncompliance have different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity took the following actions:</p> <ol style="list-style-type: none"> 1) to end the noncompliance the Entity dispatched personnel to the affected PSP to manually perform intrusion monitoring; 2) to prevent recurrence of this noncompliance the Entity revised its network drawing process in an effort to eliminate inconsistencies and inaccurate presentations on drawings; 3) to prevent recurrence of this noncompliance the Entity will update applicable policies to explicitly state that the [REDACTED] department is not to add telecom equipment without network drawings that have been issued and approved by the Telecom department; and 4) to prevent recurrence of this noncompliance the Entity will update applicable policies to explicitly state that the [REDACTED] department is not to add telecom equipment without approval from the Telecom department. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017018210	CIP-005-5	R1; P1.3	██████████ (the "Entity")	██████████	4/1/2017	8/2/2017	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted per an existing multi-region registered entity agreement from ██████████, Texas RE determined that the Entity, as a ██████████, was in noncompliance with CIP-005-5 R1. Specifically, the Entity did not document the reason for granting access for several inbound and outbound access permissions for an Electronic Access Point (EAP) for the Medium Impact BES Cyber System associated with a ██████████. After discovering the issue, on August 2, 2017, the Entity documented the reason for granting access for the rules at issue.</p> <p>The root cause of the noncompliance is that the Entity did not have sufficient documentation in place to ensure that the ██████████ was compliant with CIP-005-5 R1. In particular, the Entity had not documented justifications for the rules with adequate granularity.</p> <p>This noncompliance started on April 1, 2017, when CIP-005-5 R1 became applicable to the ██████████ BES Cyber System, and ended on August 2, 2017, when the Entity documented the reason for granting access for the rules at issue.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk posed by this issue is that the Entity could have inbound and outbound access permissions that would permit unauthorized access to BES Cyber Systems. In addition, the ██████████, the ██████████, and the asset is associated with a Medium Impact BES Cyber System. However, the risk posed by this issue was reduced by the following factors. First, this issue was limited to the Entity's documentation only. The Entity ended the noncompliance by revising the documented rule justifications. Second, the Entity deployed an additional preventative control that blocks applications and user activity that have not been previously whitelisted. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) documented the reasons for granting access for the rules at issue; and 2) used an internal software toolset to generate and assign tasks for personnel to perform periodic reviews of firewall configurations and documentation. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2020022980	CIP-004-6	R2; P2.3	[REDACTED] (the "Entity")	[REDACTED]	11/01/2019	01/10/2020	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 28, 2020, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R2, Part 2.3. Specifically, the Entity reported two employees who did not complete cyber security training within the 15 month time frame given by CIP-004-6 R2.</p> <p>The Entity submitted transcript records of the affected users showing when the user's previous and current training sessions were completed. Texas RE reviewed the records and determined that one user did complete training within 15 calendar months and one did not.</p> <p>The root cause for this noncompliance was an insufficient process for alerting employees when training deadlines were upcoming. In particular, the Entity's personnel should have received reminders and alerts that their courses were due soon or past due, but this did not occur.</p> <p>This noncompliance started on November 1, 2019, when the employee was overdue for additional cyber security training, and ended on January 10, 2020, when the employee completed the required training.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious risk to the reliability of the bulk power system. The risk posed by this noncompliance is the potential for a breach in cyber security due to insufficient training of one employee. This risk is reduced by two factors. First, the duration of the noncompliance was relatively short, lasting 71 days, and the user had previously received CIP training. Second, the noncompliance was discovered by an internal control, which reports the training status of users quarterly. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed the required training for the employee; 2) added additional monthly reviews of required training deadlines to the quarterly reviews already employed; 3) instituted a 12 calendar month deadline for completion of training; and 4) redesigned its learning management system to properly alert employees of deadlines. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019022373	CIP-004-3a	R3; P3.2	[REDACTED] (the "Entity")	[REDACTED]	03/19/2016	07/29/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 13, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-004-3a R3 (R3.2). According to the Entity, two employees lacked timely renewal of their criminal history check.</p> <p>The root cause was a data entry error whereby an individual incorrectly populated a driving record date into the Criminal History date field.</p> <p>This noncompliance started on March 19, 2016, when the personnel risk assessment for the first employee was due for renewal but was not performed, and ended on July 29, 2019, when the personnel risk assessments were updated for the two employees.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The potential risk is that failing to timely update a personnel risk assessment could cause an entity to miss changes in an individual's criminal history, an element of potential risk for safety and security. However, the risk of this noncompliance is lessened by a few factors. Both of the two employees noted had previously had a criminal background check with no findings. Additionally, both employees are currently in good standing. Finally, the updated personnel risk assessments did not have any findings. No harm is known to have occurred.</p> <p>Texas RE determined that the Entity's compliance history should not serve as a basis for aggravating the risk.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the criminal history checks for the two missing employees; and 2) to prevent reoccurrence, the Entity implemented a two-person verification for updated criminal history checks conducted for existing employees in order to ensure that updated criminal history checks are entered correctly into the human resources system. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018020246	CIP-005-5	R1.3	[REDACTED] (the "Entity")	[REDACTED]	07/01/2016	07/29/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted per an existing multi-region registered entity agreement from [REDACTED], Texas RE determined that the Entity, as a [REDACTED], was in noncompliance with CIP-005-5 R1.3. In particular, the Entity did not provide the reason for granting inbound and outbound access permissions for [REDACTED] on Electronic Access Points for Medium Impact BES Cyber Systems.</p> <p>The root cause for this noncompliance was a failure to follow internal processes. The Entity's process document related to the management of Electronic Security Perimeters states that the reason for granting access is required for each inbound and outbound access rule.</p> <p>This noncompliance started on July 1, 2016, when CIP-005-5 R1.3 became enforceable, and ended on July 29, 2018, when the Entity provided documentation stating that the firewall rule descriptions had been updated.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk in not providing reasons for granting inbound and outbound access permissions is this can lead to an entity being unaware of what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with. This can lead to unnecessary and overly permissive access permissions.</p> <p>The risk posed by this noncompliance is reduced due to the following:</p> <ol style="list-style-type: none"> 1) [REDACTED] were placed in positions in the firewall configuration where they would be processed after rules which denied all traffic. This results in these rules being effectively non-functional. 2) The remaining rule is required for operations. <p>No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) to end this noncompliance the Entity updated all firewall rules to include documented justification; and 2) to prevent recurrence of this noncompliance the Entity will implement a periodic spot check as internal control. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019022653	CIP-007-6	R2;	[REDACTED] (the "Entity")	[REDACTED]	11/16/2019	11/20/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 17, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-007-6 R2. According to the Entity, the Entity failed to install an applicable security patch within 35 calendar days of completing the evaluation. The security patch was applicable to [REDACTED] Cyber Assets identified as EACMS associated with High Impact BES Cyber Systems.</p> <p>The root cause of the noncompliance was a failure to follow documented procedures. The Entity requires a comprehensive review of newly released patch notes to determine if a released patch is security related, and subsequently if the security patches are applicable. This security patch addressed 12 vulnerabilities, 11 of which were not applicable to the Entity's environment. The one vulnerability applicable to the Entity's environment should have resulted in the patch being deemed applicable.</p> <p>This noncompliance started on November 16, 2019, which is the 36th day after the previous patch evaluation and ended on November 20, 2019, when the patches were installed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was short, lasting only four days. In addition, the patch was installed within 70 days of its release. If the Entity delayed five days in performing the evaluation of the patch, both the evaluation and the installation would have been within compliance.</p> <p>Aggravating risk factors as they relate to the Entity: [REDACTED]</p> <p>Mitigating risk factors as they relate to the Entity: [REDACTED]</p> <p>Aggravating risk factors as they relate to the noncompliance:</p> <ul style="list-style-type: none"> • The affected Cyber Assets are EACMS associated with High Impact BES Cyber Systems; • The affected EACMS are firewalls that control inbound and outbound access to and from the Entity's Electronic Security Perimeters associated with High Impact BES Cyber Systems. <p>Mitigating risk factors as they relate to the noncompliance:</p> <ul style="list-style-type: none"> • The duration of the noncompliance was short, lasting four days; • The Entity self-discovered the issue due to existing compliance controls <p>Texas RE determined that the Entity's compliance history should not serve as a basis for aggravating the risk. The Entity has a prior instance of noncompliance with CIP-007-6 R2 under [REDACTED]. The root causes for these violations are different. In [REDACTED], the root cause of the noncompliance was an inability to demonstrate compliance due to the functionality of the tool being used by the Entity to comply with this requirement. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity took the following actions:</p> <ol style="list-style-type: none"> 1) to end the noncompliance the Entity re-evaluated the patch and determined it to be applicable; 2) to end the noncompliance the Entity installed the patch on the applicable Cyber Assets; 3) to prevent recurrence of the noncompliance the Entity conducted reinforcement training with applicable 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
WECC2018020731	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	05/01/2018	05/23/2018	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 violation.)			<p>On November 21, 2018, the entity submitted a Self Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity had one documented Cyber Security Incident Response Plan (CSIRP) associated with its Control Center, containing a Medium Impact Bulk Electric System (BES) Cyber System (MIBCS). The Plan had been previously tested on January 9, 2017, and therefore should have been tested again by April 30, 2018. During an internal compliance review conducted on July 12, 2018, the entity discovered it had not tested its CSIRP as required by Part 2.1. because it was manually tracking the testing due dates and had miscalculated the April 30, 2018, due date. This issue began on May 1, 2018, when the 15 calendar-month timeframe to conduct the test expired, and ended on May 23, 2018, when the entity completed a tabletop exercise of its Plan.</p> <p>The root cause of the issue was attributed to less than adequate process design. Specifically, the same individual who was responsible for manually tracking the previous test date was also responsible for timely scheduling and completing the subsequent test without additional oversight or automated processes to reduce the occurrence of human error.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to perform a test of its documented CSIRP at least once every 15 calendar months as required by CIP-008-5 R2, P2.1</p> <p>Failure to test the CSIRP could have resulted in the incident response personnel being unfamiliar with their responsibilities which could have delayed response time. Delayed response time to a cyber attack could have led to a lack of visibility or ability to control its MIBCS. However, the CSIRP did not change significantly between 2017 and 2018 and all of the same incident response personnel participated in the 2017 exercise, making it more likely that the responsible personnel would respond appropriately if needed. Additionally, this issue had a short duration of 23 days. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) conducted a tabletop exercise of its CSIRP; 2) developed and implemented a spreadsheet tool to ensure the Plan is tested every 12 months from the previous test date instead of every 15 calendar months; 3) begun to track test dates for the Plan on the compliance calendar within its NERC SharePoint site; 4) provided training to all personnel responsible for testing the Plan on a timely basis; 5) created and filled a new "Compliance Analyst" position, whose duties include implementing and verifying that adequate internal process controls are in place to ensure compliance with all applicable Reliability Standards; and 6) enhanced its internal compliance program by: <ol style="list-style-type: none"> a. adding and clearly defining additional compliance governance, oversight, support and performance responsibilities for all personnel involved in the entity's internal compliance program; b. creating and implementing an internal NERC and WECC compliance committee; aligning O&P and CIP compliance processes, where appropriate, to create consistency within the entity's internal compliance program; and c. more clearly defining the entity's process to identify and self-report potential non-compliance violations to WECC. <p>WECC has verified the completion of all mitigation activities.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021190	CIP-009-6	R2: P2.1	[REDACTED]	[REDACTED]	05/01/2018	05/23/2018	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 violation.)			<p>On March 6, 2019, the entity submitted a Self Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-009-6 R2. Specifically, the entity had one documented Recovery Plan (Plan) associated with its Control Center, containing a Medium Impact Bulk Electric System (BES) Cyber System (MIBCS). The Plan had been previously tested on January 9, 2017, and therefore should have been tested again by April 30, 2018. During an internal compliance review conducted on July 12, 2018, the entity discovered it had not tested its Plan as required by Part 2.1. because it was manually tracking the testing due dates and had miscalculated the April 30, 2018, due date. Accordingly, This issue began on May 1, 2018, when the 15 calendar-month timeframe to conduct the test expired, and ended on May 23, 2018, when the entity completed a tabletop exercise of its Plan.</p> <p>The root cause of the issue was attributed to less than adequate process design. Specifically, the same individual who was responsible for manually tracking the previous test date was also responsible for timely scheduling and completing the subsequent test without additional oversight or automated processes to reduce the occurrence of human error.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to perform a test of its documented Plan at least once every 15 calendar months as required by CIP-009-6 R2, P2.1</p> <p>Failure to test the Plan could have resulted in the incident response personnel being unfamiliar with their responsibilities which could have delayed response time. Delayed response time to a cyber attack could have led to a lack of visibility or ability to control its MIBCS. However, the Plan did not change significantly between 2017 and 2018 and all of the same incident response personnel participated in the 2017 exercise, making it more likely that the responsible personnel would respond appropriately. Additionally, this issue had a short duration of 23 days. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) conducted a tabletop exercise of its Plan; 2) developed and implemented a spreadsheet tool to ensure the Plan is tested every 12 months from the previous test date instead of every 15 calendar months; 3) begun to track test dates for the Plan on the compliance calendar within its NERC SharePoint site; 4) provided training to all personnel responsible for testing the Plan on a timely basis; 5) created and filled a new "Compliance Analyst" position, whose duties include implementing and verifying that adequate internal process controls are in place to ensure compliance with all applicable Reliability Standards; and 6) enhanced its internal compliance program by: <ol style="list-style-type: none"> a. adding and clearly defining additional compliance governance, oversight, support and performance responsibilities for all personnel involved in the entity’s internal compliance program; b. creating and implementing an internal NERC and WECC compliance committee; aligning O&P and CIP compliance processes, where appropriate, to create consistency within the entity’s internal compliance program; and c. more clearly defining the entity’s process to identify and self-report potential non-compliance violations to WECC. <p>WECC has verified the completion of all mitigation activities.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2020022801	CIP-007-6	R2: P2; P2.1, P2.2, P2.3	[REDACTED]	[REDACTED]	10/22/2018	09/13/2019	Self-Log	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)</p>			<p>On October 19, 2019, under an existing [REDACTED], the entity submitted a Self-Log stating that, as a [REDACTED], it was in potential noncompliance with CIP-007-6 R2. Specifically, the entity stated that it did not adequately implement its documented security patch management program when it failed to identify a patch source for an updated version of software, installed on four Bulk Electric System (BES) Cyber Assets (BCA) associated with a High Impact BES Cyber System (HIBCS). The employees that installed the software confirmed with the team responsible for patching, that patches were being monitored for; however, neither of the teams involved discussed whether monitoring was being conducted at the application level and not the version. Consequently, the entity did not identify a patch source for the updated version of the software as required by Part 2.1. As a result, the entity also did not evaluate security patches every 35 calendar days as required by Part 2.2; nor did the entity take one of the following actions: apply the applicable patches; create a dated mitigation plan; or revise an existing mitigation plan within 35 calendar days, as required by Part 2.3.</p> <p>The Part 2.1 issue began on October 22, 2018, when the entity installed an updated version of the software without identifying a patch source and ended on August 20, 2019, when the entity identified a patch source for the updated version. The Part 2.2 issue began on November 27, 2018 when the 35-calendar day timeframe to conduct the initial evaluation of security patches expired and ended on September 5, 2019 when the entity evaluated the security patch. Finally, the Part 2.3 issue began on March 4, 2019, when the 35 calendar days timeframe allowed to act on the security patch expired and ended on September 13, 2019 when the entity applied the security patch.</p> <p>The root cause of the issue was attributed to less than adequate communication between work groups. Specifically, none of the employees involved communicated sufficiently to discover the assumptions being made by both teams that undermined the effectiveness of the collaboration.</p>					
<p>Risk Assessment</p>			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented security patch management program to track, evaluate, and install cyber security patches for applicable Cyber Assets as required by CIP-007-6 R2 Part 2.1 for one patch source. The entity therefore failed to evaluate security patches from that source for applicability every 35 calendar days as required by Part 2.2 and to take one of the following actions: apply any applicable patches; create a dated mitigation plan; or revise an existing mitigation plan with 35 calendar days as required by Part 2.3.</p> <p>Failure to track patches for the associated software could have resulted in malicious actor acting to take advantage of a known vulnerability in the software to gain access to the HIBCS. However, the entity did not experience disruption or Cyber Security Incidents during this period. Additionally, the entity protected its BCS by requiring multi-factor authentication to access either Medium Impact BCS or HIBCS. No harm is known to have occurred.</p>					
<p>Mitigation</p>			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) identified a patch source for the software; 2) evaluated, and applied security patches it determined were applicable; 3) published a list of patch sources in a location accessible to all appropriate employees; and 4) communicated to relevant employees the need to consider whether a patch source has been identified based on version or application. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2020022802	CIP-010-2	R1: P1.1, subpart 1.1.4.	[REDACTED]	[REDACTED]	05/30/2017	9/19/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On October 19, 2019, under an existing [REDACTED], the entity submitted a Self-Log stating that, as a [REDACTED], it was in potential noncompliance with CIP-010-2 R1. Specifically, during the performance of its annual Cyber Vulnerability Assessment, the entity identified that the tool used to automatically capture baseline configurations was not capturing the logical network accessible ports in the baseline configuration of one Cyber Asset associated with a Medium Impact Bulk Electric System (BES) Cyber System (MIBCS) with External Routable Connectivity (ERC). The tool used to capture baseline configurations ran a command that showed ports open on the BES Cyber Asset (BCA); however, it did not include all listening ports. This issue began on May 30, 2017, when baseline configuration documentation did not include logical network accessible ports for one BCA and ended on September 19, 2019, when the entity documented all logical network accessible ports in the baseline configuration.</p> <p>The root cause of the issue was attributed to a less than adequate process design. Specifically, the entity’s process relied on a tool to document logical network accessible ports; however, the tool did not function as expected and did not consistently document ports in the baseline configuration.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented process to develop a baseline configuration for one device that includes the operating system, any commercially available or open-source application software, any custom software installed, any logical network accessible ports, and any security patches applied, as required by CIP-010-2 R1 Part 1.1.</p> <p>Failure to fully develop an accurate baseline configuration could have resulted in the entity failing to identify an unauthorized change. However, the asset was maintained in an environment that required Multi-Factor Authentication for internal and remote connection. Additionally, the asset physically located in a Physical Security Perimeter. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) fully documented the baseline configuration of the BCA including all logical network accessible ports; and 2) implemented a change to its asset commissioning and change management processes to require a separate scan to identify logical network accessible ports and confirmation that all ports are documented in the tool used to monitor for baseline configuration changes. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2020022800	CIP-010-2	R1: P1.3	[REDACTED]	[REDACTED]	07/26/2019	08/06/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On October 19, 2019, under an existing [REDACTED], the entity submitted a Self-Log stating that, as a [REDACTED] it was in potential noncompliance with CIP-010-2 R1. Specifically, the entity did not update the baseline configuration of [REDACTED] Electronic Access Control or Monitoring Systems (EACMS) associated with a Medium Impact Bulk Electric System (BES) Cyber System (MIBCS). The entity had authorized application of a security patch to the one EACMS. At the time, the entity’s process was to review and accept changes to baseline configurations during a weekly compliance meeting. However, the entity was reviewing a report that only listed changes to the baseline configuration of BES Cyber Assets associated with High Impact BCS; in this instance, the baseline configuration change was associated with a MIBCS, and therefore was not reviewed during the weekly compliance meeting. This issue began on July 26, 2019 when the 30-calendar day timeframe to update the baseline configuration expired, and ended on August 6, 2019, when the entity updated the baseline configuration.</p> <p>The root cause of the issue was attributed to a less than adequate process documentation. Specifically, the entity generated multiple reports regarding baseline configuration changes, which increased the likelihood that baseline configuration changes would not be reviewed and approved appropriately.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to, for a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change as required by CIP-010-2 R1 Part 1.3.</p> <p>Failure to timely update the baseline configuration could have resulted in the entity failing to have an accurate baseline to utilize to restore the BCA. However, the configuration change was planned and authorized. Additionally, this was a deficiency in documentation with a short duration. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) updated the baseline configuration of the [REDACTED] BCA; 2) implemented a procedural change that reduced the number of configuration change reports to one all-inclusive report; 3) amended the internal checklist to include the Standard and Requirement language to its weekly compliance checklist to clarify the objective of each step and added detail on the correct report to reference; and 4) conducted training with relevant employees. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2020022892	CIP-006-6	R2: P2.1	[REDACTED]	[REDACTED]	10/4/2019	10/4/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On January 22, 2020, the entity submitted a Self-Log stating that, as a [REDACTED] it was in potential noncompliance with CIP-006-6 R2. Specifically, an employee left two contractors unescorted within a Physical Security Perimeter (PSP) controlling access to the High Impact Bulk Electric System (BES) Cyber Systems. The contractors were scheduled to conduct maintenance on an information storage array. Prior to entering the PSP, Physical security staff provided one of the contractors with a copy of the entity’s visitor instructions for entering and exiting the mantrap. When the contractors had finished their work, the employee escorted the contractors back to the interior exit door of the mantrap. The employee scanned his badge, entered the mantrap, and the mantrap door closed; however, the contractors had not entered the mantrap and remained in the PSP. The employee maintained eye contact and communication with the contractors, and attempted to reenter the PSP, from inside the mantrap. Physical security staff were deployed and instructed the employee to completely exit the mantrap and then reenter the PSP. The employee followed instructions and therefore, lost visual and auditory contact with the contractors for 10 seconds while he reentered the PSP. During the 10 second interval, although physical security staff monitored the contractors via live security camera feed, the entity’s documented visitor control program specifies that escorts can never leave visitors unattended inside a PSP. The employee reentered the PSP via the mantrap and resumed escorting the contractors out of the PSP. This issue began on October 4, 2019, when two contractors were left unescorted and ended on October 4, 2019, when the employee recommenced escorting the contractors.</p> <p>The root cause of the issue was attributed to less than adequate training. Specifically, the employee rarely escorted visitors and was not sufficiently prepared to act appropriately.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to implement its documented visitor control program to require continuous escorted access of visitors within each PSP as required by CIP-006-6 R2 Part 2.1.</p> <p>Failure to continuously escort visitors could have resulted in an actor with malicious intent attempting to physically damage the Cyber Assets within the PSP. However, the duration of the issue was only 10 seconds. Additionally, the contractors were continuously monitored via live security camera footage throughout the duration of the issue. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) recommenced escorting the contractors; and 2) provided additional training regarding continuous escorted access of visitors to employees to relevant employees that rarely act as an escort. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020568	CIP-010-2	R3: P3.1	[REDACTED]	[REDACTED]	07/01/2018	10/19/2018	Self-Report	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)</p>			<p>On October 17, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-010-2 R3.</p> <p>Specifically, on [REDACTED], during an evidence review, the entity discovered a potential gap in evidence to demonstrate compliance with CIP-010-2 R3 P3.1. After further review, the entity determined it had not conducted a paper or active vulnerability assessments at least once every 15 calendar months for [REDACTED] Protected Cyber Assets (PCAs), [REDACTED] Electronic Access Control or Monitoring Systems (EACMS) Cyber Assets, and [REDACTED] Physical Access Control Systems (PACS) Cyber Assets associated with its High Impact BES Cyber System (HIBCS), and for [REDACTED] PCAs associated with its Medium Impact BES Cyber System (MIBCS), as required by CIP-010-2 R3 P3.1. This issue began on July 1, 2018, the day the 15 calendar month window to conduct the vulnerability assessments for the EACMS expired, and ended on October 19, 2018, when the entity completed the vulnerability assessments on all the Cyber Assets in scope.</p> <p>The root cause of the issue was attributed to a lack of internal controls to ensure Subject Matter Experts (SMEs) did not miss the deadline for the periodic activity. Specifically, the entity did not establish a mechanism for reminder dates by which to conduct the next vulnerability assessments. Therefore, the entity’s SMEs were ineffectively manually tracking renewal dates for vulnerability assessments because the entity’s [REDACTED] did not support the 15-calendar month frequency of the standard.</p>					
<p>Risk Assessment</p>			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to conduct paper or active vulnerability assessments at least once every 15 calendar months for [REDACTED] PCAs, [REDACTED] EACMS, and [REDACTED] PACS associated with its HIBCS and MIBCS, as required by CIP-010-2 R3 P3.1.</p> <p>Failure to conduct vulnerability assessments could have resulted in misconfigurations that increased the entity’s cyber-attack surface, making it more likely that malware or malicious activity could affect the entity's systems and reduce the entity's ability to monitor and control its BES infrastructure. However, the entity effectively implemented the related protective measures of CIP-005 R1 (Electronic Security Perimeter), CIP-007 R2 (Security Patch Management), and CIP-010 R1 (Configuration Change Management) as verified [REDACTED]. In addition, the duration of this issue was relatively short (49 to 111 days) for this type of activity. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed vulnerability assessments for the Cyber Assets in scope; 2) implemented a recurring, biweekly meeting of CIP users and administrators to review upcoming work activity; and 3) changed its internal review period from 15 calendar months to 12 calendar months, which is supported by entity’s automated task notification software. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022141	CIP-003-6	R2	[REDACTED]	[REDACTED]	9/27/2017	8/2/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-003-6 R2. Specifically, the entity did not update its Cyber Security Incident response plan within 180 calendar days after testing said plan, as required by CIP-003-6 R2 Attachment 1, Section 4.6. On March 30, 2017, the entity conducted a tabletop exercise of its Cyber Security Incident response plan. Subsequently, in preparation for an audit, the entity discovered it that it had not updated its plan with lessons learned from the exercise. This issue began on September 27, 2017 when the 180 calendar day timeframe expired and ended on August 2, 2019 when the entity updated the Cyber Security Incident response plan.</p> <p>The root cause of this issue was attributed to a less than adequate documented process. Specifically, the entity’s documented process was specific to certain personnel instead of prescribing role-based duties. The personnel associated with this issue were no longer employed with the entity; therefore, the entity was unable to provide further details regarding the root cause.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to update one Cyber Security Incident response plan for its Low Impact BES Cyber System (LIBCS) within 180 calendar days after completion of a Cyber Security Incident response plan test as required by CIP-003-6 R2, Attachment 1, Section 4.6.</p> <p>Failure to timely update a Cyber Security Incident response plan with lessons learned could have resulted in personnel referencing outdated documentation, potentially exacerbating an actual incident. However, this issue was associated with LIBCS. Further, the entity was responsible for [REDACTED] and therefore, was inherently low risk to the BPS. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) updated the Cyber Security Incident response plan with lessons learned from the initial test; 2) implemented a role-based compliance calendar accessible to employees in relevant roles; and 3) revised the Cyber Security Incident response plan to a role-based structure. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022142	CIP-003-6	R2	[REDACTED]	[REDACTED]	9/27/2017	8/2/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-003-6 R2. Specifically, the entity did not update its Cyber Security Incident response plan within 180 calendar days after testing said plan, as required by CIP-003-6 R2 Attachment 1, Section 4.6. On March 30, 2017, the entity conducted a tabletop exercise of its Cyber Security Incident response plan. Subsequently, in preparation for an audit, the entity discovered it that it had not updated its plan with lessons learned from the exercise. This issue began on September 27, 2017 when the 180 calendar day timeframe expired and ended on August 2, 2019 when the entity updated the Cyber Security Incident response plan.</p> <p>The root cause of this issue was attributed to a less than adequate documented process. Specifically, the entity’s documented process was specific to certain personnel instead of prescribing role-based duties. The personnel associated with this issue were no longer employed with the entity; therefore, the entity was unable to provide further details regarding the root cause.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to update one Cyber Security Incident response plan for its Low Impact BES Cyber System (LIBCS) within 180 calendar days after completion of a Cyber Security Incident response plan test as required by CIP-003-6 R2, Attachment 1, Section 4.6.</p> <p>Failure to timely update a Cyber Security Incident response plan with lessons learned could have resulted in personnel referencing outdated documentation, potentially exacerbating an actual incident. However, this issue was associated with LIBCS. Further, the entity was responsible for [REDACTED] and therefore, was inherently low risk to the BPS. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) updated the Cyber Security Incident response plan with lessons learned from the initial test; 2) implemented a role-based compliance calendar accessible to employees in relevant roles; and 3) revised the Cyber Security Incident response plan to a role-based structure. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022455	CIP-004-6	R5: P5.1	[REDACTED]	[REDACTED]	04/13/2019	05/03/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On November 4, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R5.</p> <p>Specifically, upon termination of a contractor on April 12, 2019, the entity initiated the removal of the contractor’s ability for unescorted physical access and Interactive Remote Access. However, the entity did not complete the removals within 24 hours of the termination action, as it failed to retrieve a hard key that opened substation gates and the Physical Security Perimeter (PSP) controlling access to CIP breaker cabinets containing Medium Impact BES Cyber Systems (MIBCS) at [REDACTED] substations. This issue began on April 13, 2019, when the 24-hour timeframe for completing access removals expired, and ended on May 3, 2019, when the entity collected the key.</p> <p>The root cause of the issue was attributed to a misconfiguration of the notifications to personnel responsible for revoking physical access which resulted in the notifications being sent to an inactive email distribution list.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to complete the removal of unescorted physical access to a PSP controlling access to MIBCS with ERC at [REDACTED] substations from a contractor within 24 hours of a termination action as required by CIP-004-6 R5 Part 5.1.</p> <p>Failure to timely remove an individual’s ability for unescorted physical access following a termination action could have resulted in the contractor misusing access to cause physical harm to equipment which could result in loss of visibility or inability to operate transmission elements. However, as compensation, the CIP breaker cabinets had tamper alarms that alerted the entity’s physical security team when opened. Persons with rights to access the CIP breaker cabinets were required to alert the physical security team before opening them, and the entity confirmed from tamper alarm logs that the contractor did not access the CIP breaker cabinets during this noncompliance. No harm is known to have occurred.</p> <p>The entity’s compliance history included three relevant instances of noncompliance. WECC determined that the entity’s compliance history should not serve as a basis for aggravating the disposition track because the prior instances of noncompliance were minimal risk and had different root causes than the instant noncompliance, and the mitigation activities of the prior noncompliance would not have prevented the instant issue.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) collected the substation hard key from the contractor; 2) implemented a temporary work-around solution to forward notifications to the physical security team until the access management system was updated; and 3) updated the access management system to correct the email distribution list of the physical security team. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022643	CIP-004-6	R5: P5.2	[REDACTED]	[REDACTED]	05/03/2019	07/03/2019	Self-Report	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)</p>			<p>On December 12, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R5.</p> <p>Specifically, the entity identified that an employee on extended leave preceding retirement would not be able to complete refresher cyber security training in a timely manner as required by CIP-004-6 R5 Part 5.2 and, based on the timing of retirement, determined the employee no longer required said access. The entity removed unescorted physical access from the employee’s badge but failed to retrieve a hard key that opened substation gates and the Physical Security Perimeter (PSP) controlling access to CIP breaker cabinets containing Medium Impact BES Cyber Systems (MIBCS) at [REDACTED] substations. This issue began on May 3, 2019, the day after the 24-hour timeframe for removing access expired and ended on July 3, 2019, when the entity retrieved the hard key from the employee.</p> <p>The root cause of the issue was attributed to the entity failing to document in its system of record that the employee had been issued a hard key.</p>					
<p>Risk Assessment</p>			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to revoke access to the PSP controlling access to MIBCS with ERC at [REDACTED] substations within 24 hours of determining that the employee no longer required retention of that access, as required by CIP-004-6 R5 Part 5.2.</p> <p>Failure to revoke unescorted physical access to MIBCS with ERC in a timely manner could have resulted in an employee misusing access to cause physical harm to equipment, which could result in loss of visibility or inability to operate transmission elements. However, as compensation, the CIP breaker cabinets had tamper alarms that alert the entity’s physical security team when opened. Persons with rights to access the CIP breaker cabinets were required to alert the physical security team before opening them, and the entity confirmed from tamper alarm logs that the employee did not access the CIP breaker cabinets during this noncompliance. No harm is known to have occurred.</p> <p>The entity’s compliance history included three relevant instances of noncompliance. WECC determined that the entity’s compliance history should not serve as a basis for aggravating the disposition track because the prior instances of noncompliance were minimal risk, had different root causes than the instant noncompliance, occurred in 2010, 2015, and 2017, and the mitigation activities of the prior noncompliance would not have prevented the instant issue.</p>					
<p>Mitigation</p>			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) collected the substation hard key from the employee; 2) reviewed the physical security team’s access database to confirm its accuracy; 3) updated access control policies and procedures to account for issues associated with extended leaves of absence; and 4) updated the physical security team’s key issuance process to include a checklist. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021133	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	07/01/2017	10/24/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On February 28, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2.</p> <p>Specifically, on May 15, 2018, during an internal spot check, the entity discovered that it had not properly tested its Cyber Security Incident response plan (CSIRP) associated with one Control Center containing a High Impact Bulk Electric System (BES) Cyber System (HIBCS). Although the entity conducted a tabletop exercise of its CSIRP, it did not use a Reportable Cyber Security Incident as the basis for its test. This issue began on July 1, 2017, when the Standard and Requirement became mandatory and enforceable, and ended on October 24, 2018, when the entity tested its CSIRP using a Reportable Cyber Security Incident.</p> <p>The root cause of the issue was attributed to less than adequate process documentation. Specifically, the CSIRP did not provide the definition of a Reportable Cyber Security Incident which led the subject matter experts to incorrectly assume what type of incident to use and tested the CSIRP using a non-reportable incident.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to adequately test its CSIRP at least once every 15 calendar months with a tabletop exercise of a Reportable Cyber Security Incident, as required by CIP-008-6 R2 Part 2.1.</p> <p>Failure to test its CSIRP using a Reportable Cyber Security Incident could have resulted in a delayed response by the entity’s incident response personnel. Delayed response time to a cyber-attack could have led to a lack of visibility or ability to control its system. However, as compensation, the entity did timely perform a tabletop exercise of its CSIRP. No harm is known to have occurred.</p> <p>WECC determined that the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) conducted a tabletop exercise of its CSIRP using a Reportable Cyber Security Incident; 2) updated its CSIRP to include a definition of what a Reportable Cyber Security Incident is; 3) updated the work order job plans to reflect the changes in reporting requirements; and 4) provided training to subject matter experts on updated procedures and the definition of Reportable Cyber Security Incident. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017628	CIP-004-6	R3: P3.5	[REDACTED]	[REDACTED]	07/01/2016	12/08/2016	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On May 19, 2017, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R3. Specifically, the entity allowed one employee and one contractor to have unescorted physical access to a Physical Security Perimeter controlling access to the High Impact BES Cyber Systems (HIBCS) located at the primary Control Center and Medium Impact BES Cyber Systems (MIBCS) located at [REDACTED] substations, without confirming they had personnel risk assessments (PRAs) completed within the last seven years. The employee also had authorized electronic access to Cyber Assets associated with the MIBCS. This issue began on July 1, 2016, when two individuals were authorized access without a valid PRA and ended on December 8, 2016, when access for the two individuals was revoked.</p> <p>The root cause of the issue was attributed to errors in software programming in the entity’s new authorization system of record that; (1) omitted a PRA check and (2) failed to validate PRAs when bulk loading user data from the prior authorization system of record.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to ensure that individuals with authorized electronic and authorized unescorted physical access to HIBCS and MIBCS had PRAs completed within the last seven years as required by CIP-004-6 R3 Part 3.5.</p> <p>Such failure could have resulted in individuals with recent criminal history who may have developed ulterior motives towards reliability and security having access to the entity’s primary Control Center, where they could cause damage BES Cyber Systems. Individuals with access to substations could affect transmission at those locations, [REDACTED]. However, both individuals were subject to previous background checks [REDACTED] and their access was necessary for business needs and appropriately authorized. [REDACTED] No harm is known to have occurred.</p> <p>WECC determined that the entity’s compliance history should not serve as a basis for aggravating the disposition track as the prior noncompliance had a different root cause and the mitigation activities of the prior noncompliance would not have prevented the instant issue.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) removed access from the two individuals until completion of a new PRA; 2) updated the automated workflow process in the authorization system of record to include a PRA check task that stops the processing of any CIP electronic or physical access request until a current PRA check is verified by security personnel; and 3) trained systems administrators on using the authorization system of record, including emphasis that the authorization system of record is the only means of authorizing CIP electronic or unescorted physical access and that previously used tracking methods are no longer acceptable. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020637	CIP-004-6	R4: P4.1.3	[REDACTED]	[REDACTED]	07/23/2018	08/13/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On November 6, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R4.</p> <p>Specifically, for two different instances, the entity’s SharePoint development team granted a newly hired employee electronic access to a designated storage location for BES Cyber System Information (BCSI) without capturing the appropriate authorizations or following the entity’s process for access authorizations. The entity was in the process of moving a SharePoint team site to a different server, but the process was paused. The employee was assigned to perform work on the original SharePoint site by a peer who did not realize the process had been paused and that the original server still contained BCSI. The first instance began on July 23, 2018, when electronic access was granted to designated storage locations for BCSI without authorization and ended on July 27, 2018, when the entity revoked access. The second instance began on August 9, 2018, when the entity granted the same employee electronic access to designated storage locations for BCSI without authorization and ended on August 13, 2018, when the entity revoked access.</p> <p>The root cause of the issue was attributed to the entity not adequately communicating changes made to its SharePoint sites. Specifically, the issue arose while the entity was in the process of migrating data to a new server, and the persons that granted access did not understand that the SharePoint site still contained BCSI.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to restrict electronic access to designated storage locations for BCSI to only authorized personnel as required by CIP-004-6 R4 Part 4.1.3.</p> <p>Such failure could have resulted in misuse of information related to the entity’s HIBCS or MIBCS or improper transmission of the information to third parties who could use the information to conduct phishing or to probe the entity’s systems for vulnerabilities in order to implement denial of service attacks, potentially resulting in disruptions or loss of service within the entity’s electric transmission footprint. However, as compensation, the new employee was intended to have access to the Sharepoint site to perform the job function of Sharepoint Developer, had received CIP training and had a completed personal risk assessment. In addition, the entity implemented good detective controls. In the first instance, the access was identified and corrected within four days of being provisioned by personnel who knew that the Sharepoint site contained BCSI and authorization was required. The second instance was discovered within four days of being provisioned when the System Administrator performed a random spot check (performed three times a year) of BCSI storage locations and identified the issue. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) revoked the access improperly granted; and 2) trained the SharePoint [REDACTED] on BCSI information and how to request authorization for new users. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021121	CIP-004-6	R2: P2.3	[REDACTED]	[REDACTED]	01/01/2018	02/25/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On February 27, 2019, the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R2.</p> <p>Specifically, the entity allowed four contract employees [REDACTED] to have unescorted physical access to the Physical Security Perimeter (PSP) controlling access to High Impact BES Cyber Systems (HIBCS) located at the primary Control Center and two [REDACTED] contract employees to have unescorted physical access to the PSP controlling access to Medium Impact BES Cyber Systems (MIBCS) located at [REDACTED] substations without confirming those contract employees had completed cyber security training within the prior 15 calendar months, as required by CIP-004-6 R2 Part 2.3. The entity had been working to transfer data from two current cyber security training tracking programs to one new program. During data cleanup, it was discovered that these six contract employees were granted the access because they did not have accounts in the entity’s [REDACTED] which was needed to be included in the automated annual CIP training report used to identify who required training. This issue began on January 1, 2018, when the timeframe for providing refresher cyber security training to the six contract employees expired and ended on February 25, 2019, when the six contract employees completed cyber security training.</p> <p>The root cause of the issue was attributed to a program design failure. Specifically, when creating and tracking automated reports, the entity did not consider contract employees who did not have [REDACTED] accounts. The design of the automated reports did not consider all possible scenarios. Based on this, the entity failed to manage training dates for the contract employees in scope.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to ensure each individual granted unescorted physical access to BES Cyber Systems had completed cyber security training within the past 15 calendar months, as required by CIP-004-6 R2 Part 2.3.</p> <p>Such failure could have resulted in the contract employees not having current knowledge of the entity’s cyber security training material, which could result in those individuals not taking appropriate actions when accessing the PSP. However, the individuals in scope had unescorted physical access only during business hours to areas monitored by entity personnel and for which access was monitored and logged, and they had previously completed training on cyber security practices. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) conducted and documented cyber training for each of the individuals; 2) implemented an automated nightly check for cyber security training expiration; 3) implemented new workflow to remove access for expired cyber security training; and 4) implemented new cyber security training reports. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021122	CIP-004-6	R3: P3.5	[REDACTED]	[REDACTED]	04/10/2017	02/12/2019	Self-Certification	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)</p>			<p>On February 27, 2019, the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R3.</p> <p>Specifically, without ensuring they had personnel risk assessments (PRAs) completed within the last seven years, the entity allowed one individual to have unescorted physical access to the Physical Security Perimeters (PSP) controlling access to High Impact BES Cyber Systems (HIBCS) at its primary Control Center, a second individual to have electronic access to the entity’s work order software, including BES Cyber System Information associated with HIBCS, and a third individual to have both unescorted physical access to the PSP controlling access to HIBCS located at the primary Control Center and electronic access to the entity’s supervisory control and data acquisition (SCADA) system. The entity had been working to transfer data from its current PRA tracking program to a new program. During data cleanup, it was discovered that the three individuals were granted the unauthorized access in the new program even though they had expired PRA dates that had transferred from the old program. This issue began on April 10, 2017, when the seven-year timeframe for renewing PRAs expired (the earliest date of the three expired PRA dates) and ended on February 12, 2019, when new PRAs for the three individuals were completed.</p> <p>The root cause of the issue was attributed to error inputting data into the PRA tracking software.</p>					
<p>Risk Assessment</p>			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to ensure that individuals with authorized electronic and authorized unescorted physical access had PRAs completed within the last seven years, as required by CIP-004-6 R3 Part 3.5.</p> <p>Failure to ensure PRAs were conducted in a timely manner could have resulted in individuals with recent criminal history who might have developed ulterior motives regarding energy reliability and security having access to HIBCS. An individual with such access could affect the transmission and operations for which the entity was responsible, [REDACTED]. However, the entity had performed previous PRAs on the individuals, [REDACTED]. No harm is known to have occurred.</p> <p>WECC determined that the entity’s compliance history should not serve as a basis for escalating the disposition track as the prior noncompliance had a different root cause than this issue and the mitigation activities of the prior noncompliance would not have prevented the instant issue.</p>					
<p>Mitigation</p>			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) conducted and documented PRAs for the individuals; 2) migrated to a new PRA and cyber security training database; 3) implemented an automated nightly check for PRA and cyber security training expiration; and 4) implemented new PRA and cyber security training reports to ensure accuracy. <p>WECC has verified the completion of all mitigation activity.</p>					

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	MRO2019022522			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
2	MRO2019022106			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
3	MRO2019022478			Yes	Yes			Yes		Yes				Category 1: 3 years; Category 2 – 12: 2 year
4	MRO2019022131	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
5	MRO2019022132	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
6	MRO2019022133	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
7	SPP2017017351	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
8	MRO2019022393			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
9	MRO2019021449			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
10	SPP2018019213	Yes	Yes	Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
11	SPP2018019314	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
12	SPP2018019316	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
13	MRO2018020765	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
14	NPCC2019021631	Yes		Yes	Yes									Category 1: 3 years Categories 3 – 4: 2 years
15	RFC2019021622	Yes	Yes	Yes	Yes	Yes	Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 years
16	RFC2019021833	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
17	RFC2019021931	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
18	RFC2018019609	Yes	Yes	Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
19	RFC2019021476	Yes	Yes	Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 years
20	SERC2018019862		Yes	Yes	Yes				Yes	Yes				Category 2 – 12: 2 year

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
21	SERC2018019719			Yes	Yes					Yes	Yes		Yes	Category 2 – 12: 2 year
22	SERC2018019987			Yes	Yes					Yes				Category 2 – 12: 2 year
23	SERC2018020307			Yes	Yes				Yes	Yes	Yes		Yes	Category 2 – 12: 2 year
24	SERC2018019711			Yes	Yes				Yes	Yes			Yes	Category 2 – 12: 2 year
25	SERC2018020313			Yes	Yes				Yes	Yes	Yes			Category 2 – 12: 2 year
26	SERC2018019960			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
27	TRE2019021397			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
28	TRE2020022807			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
29	TRE2019020892	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
30	TRE2019022651			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
31	TRE2019022652			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
32	TRE2019021757			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
33	TRE2018019736			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
34	TRE2018019740			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
35	TRE2019021321			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
36	TRE2019021322			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
37	WECC2019021045			Yes	Yes					Yes				Category 2 – 12: 2 years
38	WECC2019021327			Yes	Yes				Yes		Yes			Category 2 – 12: 2 years
39	WECC2019021115			Yes	Yes									Category 2 – 12: 2 years
40	WECC2019021136			Yes	Yes									Category 2 – 12: 2 years
41	WECC2018020810			Yes	Yes									Category 2 – 12: 2 years
42	WECC2018020397			Yes	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)
43	WECC2018019679			Yes	Yes					Yes				Category 2 – 12: 2 years
44	WECC2017018615			Yes	Yes					Yes				Category 2 – 12: 2 years

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022522	CIP-004-6	R4	[REDACTED] (the Entity)	[REDACTED]	06/11/2019	06/17/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4. [REDACTED]</p> <p>While performing an internal assurance review of access changes, the Entity discovered that one individual had electronic access to applicable Cyber Assets per CIP-004-6 R4.1, but the access had not been authorized. While manually provisioning other authorized electronic access, the access of issue was assumed to be included based on the individual of issue role.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for authorizing electronic access for individuals.</p> <p>The noncompliance began on June 11, 2019, when the individual was provisioned electronic access, and ended on June 17, 2019, when the access was removed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the individual of issue had a valid Personnel Risk Assessment (PRA) on file and up to date CIP training. The initial access was intended per the job position but undocumented and a subsequent access request was submitted to gain authorization. Additionally, the issue was limited to one individual, and had a duration of six days. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked the unauthorized electronic access to the individual of issue; 2) updated its procedure for the review of variance reporting to include instructions that access for all instances of individuals regardless of the status indicator would be investigated; 3) sent an email communication of the updated procedure to the individuals responsible for executing the procedure. The communication also included re-enforcement information on not making assumptions and staying vigilant; and 4) implemented the updated procedures detailed above. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022106	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	12/06/2018	04/22/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 18, 2019, the Entity submitted a Self-Report stating that as [REDACTED], it was in noncompliance with CIP-010-2 R1. [REDACTED]</p> <p>The Entity reported that there were two instances where it failed to perform the required cyber security control verification per CIP-010-2 R1.4.2 after making a change that impacted both applicable medium impact BES Cyber Systems (MIBCS) and their associated Electronic Access Control or Monitoring Systems (EACMS), Protected Cyber Assets (PCA) and Physical Access Control Systems (PACS) where its [REDACTED] was implemented. The change consisted of reinstalling the [REDACTED] which resulted in the capability of alerting on detection of malicious code to stop working after the change. A Subject Matter Expert discovered the issue while performing related work on an applicable Cyber Asset of issue.</p> <p>The cause of both instances of noncompliance was the Entity’s process lacked sufficient detail for verifying cyber security controls after a baseline deviation.</p> <p>The first instance of noncompliance began on December 6th, 2018, when [REDACTED] were reinstalled at the first MIBCS, and ended on April 22, 2019, when the Entity configured the alerting.</p> <p>The second instance of noncompliance began on December 18th, 2018, when [REDACTED] were reinstalled at the second MIBCS, and ended on April 22, 2019, when the Entity configured the alerting.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk for both instances was minimal because the Entity’s responsibility is limited to MIBCS which control and monitor assets that contain low impact BES Cyber Systems. This inherently limits the impact to the BES. The issue was related to a detective control measure for malicious code and was not related to an active measure for preventing or deterring malicious code. Additionally, for the two changes of issue, it performed a verification of all other cyber security controls per its procedure, limiting the issue to verification of CIP-007-6 R4.2 protections. Lastly, the active measure for detecting malicious code was working during the duration of the issue. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate both instances of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) corrected the alerting configuration on [REDACTED] for all Cyber Assets of issue; 2) implemented a daily automated task that simulates a detected malicious code alert at both medium impact BCSs; 3) implemented a new procedure to produce a daily report from its [REDACTED] that verifies the alerting of detected malicious code is working. The simulated detected malicious code alerts would be captured in the report to verify alerting is working by its [REDACTED], and this new report will be used to verify that CIP-007-6 R4.2 protection remain active under normal baseline changes; and 4) provided training to individuals impacted by the new procedure to verify CIP-007-6 R4.2 protections. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022478	CIP-008-5	R3	[REDACTED] (the Entity)	[REDACTED]	06/13/2018	10/21/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 31, 2019, [REDACTED] submitted a Self-Report stating that [REDACTED], it was in noncompliance with CIP-008-5 R3. [REDACTED]</p> <p>The Entity reported that there were two instances where it failed to update its Cyber Security Incident response plan within 60 calendar days after individual roles were changed when individuals were terminated.</p> <p>The cause of the noncompliance in both instances was that the Entity’s documented process for updating its Cyber Security Incident response plan lacked sufficient detail in that it did not account for all individual’s role changes.</p> <p>The first instance of noncompliance began on June 13, 2018, 60 calendar days after the first individual’s role changed, and ended on July 10, 2018, when the Cyber Security Incident response plan was updated with the role change.</p> <p>The second instance of noncompliance began on September 14, 2019, 60 calendar days after the second individual’s role changed, and ended on October 21, 2019, when the Cyber Security Incident response plan was updated with the role change.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was for both instances was minimal because the Entity only has medium impact BES Cyber Systems. These medium impact BES Cyber Systems only control and monitor assets that contain low impact BES Cyber Systems, which inherently limits the impact to the BES. Additionally, all members with active roles in the Cyber Security Incident response plan were notified within 60 calendar days of the role change, limiting the issue to updating the documented Cyber Security Incident response plan. The durations of 28 and 38 days limited the exposure of any vulnerability, and in instance two, the duration was limited due to the Entity performing a non-CIP required review (internal control). No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate both instances of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated its Cyber Security Incident response plan with the role changes; 2) updated its Cyber Security Incident response plan with a step to ensure notifications are made when a change to the Cyber Security Incident response plan is made. It assigned its [REDACTED] as the responsible party to perform the notification activity; 3) added a step within its onboarding and termination processes to address updates and notifications to any CIP process or procedural documentation that the individual being processed would be responsible for; and 4) provided training to the [REDACTED] individuals and the CIP Senior Manager, who have responsibilities for updating its incident reporting and response plan based on the updated 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
MRO2019022131	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	03/16/2018	05/23/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 26, 2019, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with standard CIP-007-6 R2.</p> <p>The Entity discovered that, for [REDACTED] devices, no documentation could be located which demonstrated that for a period greater than one year, therefore, the Entity was not compliant with CIP-007-6 Parts 2.2 and 2.3. Specifically, no documentation was available to show that patches for the affected devices had been assessed for applicability and, if applicable, were installed. The devices affected included [REDACTED] and [REDACTED].</p> <p>The cause of the noncompliance was due to unfamiliarity with the full scope of its CIP-related responsibilities, the Entity’s subject matter experts responsible for [REDACTED] failed to follow the Entity’s documented processes related to the record keeping aspects of CIP-007-6 Parts 2.2 and 2.3 for these [REDACTED] devices.</p> <p>The noncompliance began on March 16, 2018, when the gap in patch-related documentation began, and ended on May 23, 2019, when the Entity had evaluated and installed all applicable patches.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the Entity determined this was a documentation issue, and patches were being monitored and assessed by the Entity. During the noncompliance, each of the patches was judged to be either not security related or applicable to device functionality that was not used by the Entity; documentation of these actions or decisions was deficient. The issue was discovered by an internal vulnerability assessment. No harm is known to have occurred.</p> <p>The Entity has related compliance history; however, MRO determined that the Entity’s compliance history should not serve as a basis for applying a penalty because the prior instance had different factual circumstances, issues, and/or causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) re-evaluated and installed all applicable patches released for the affected devices and updated evaluation documentation; 2) updated device software to recommended version; 3) provided training on internal policies and procedures related to CIP-007 to the SMEs responsible for the [REDACTED]; 4) assigned oversight of [REDACTED] compliance responsibilities to senior, experienced CIP administrators; and 5) provided refresher training to all CIP SMES on the Entity’s internal policies and procedures related to CIP-007. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022132	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	03/31/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 26, 2019, the submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-010-2 Part 1.1.</p> <p>The Entity reported that it was unable to locate documentation demonstrating that it adequately complied with CIP-010-2 for [REDACTED] BES Cyber Assets. Specifically, the Entity did have documentation of device configurations, ports/services justifications, and access tracking lists. However, with regard to maintenance of information when baseline changes were made, the Entity found several issues with its baseline documentation. The documentation did not include information showing that baseline configurations were updated following changes (as required by Part 1.3), it did not include information that analysis was performed to determine if changes could affect cyber security controls required by CIP-005 or CIP-007 (as required by Part 1.4), and it did not include information that testing was performed in advance of making changes to the baseline configuration (as required by Part 1.5).</p> <p>The cause of the noncompliance was that the Entity failed to follow its process to develop a baseline configuration for [REDACTED] BES Cyber Assets in noncompliance with CIP-010-2 R1.</p> <p>The noncompliance began on July 1, 2016, when the standard became enforceable, and ended on March 31, 2019, when the baseline change monitoring frequency was changed to be less than or equal to 35 days.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the [REDACTED] were monitored for release of security patches/updates; any patches/updates were evaluated and installed when applicable as required by CIP-007-6. The Entity found no security related updates or significant changes (other than password changes) were applied to the affected devices during the period of noncompliance. Even though the Entity was not fully compliant with CIP-010-2 R1, a process was in place to monitor the [REDACTED] for baseline changes. Additionally, its SMEs pulled configuration files for the [REDACTED] quarterly and monitored for deviations. The Entity also determined that the only BES Cyber Assets affected were the [REDACTED]. Lastly, all changes to the affected devices were tested prior to introduction into a production environment. No harm is known to have occurred.</p> <p>The Entity has related compliance history; however, MRO determined that the Entity’s compliance history should not serve as a basis for applying a penalty because the prior instance had different factual circumstances, issues, and/or causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) established baselines for the affected devices and documented its comparisons of current to the initial configurations in accordance with CIP-010-2; 2) provided training, to the SMEs responsible for the [REDACTED], on its internal policies and procedures related to CIP-007-6 and CIP-010-2; 3) assigned oversight responsibilities of [REDACTED] compliance to experience senior CIP administrators; and 4) implemented refresher training on CIP-007-6 and CIP-010-2 policies and procedures for all 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
MRO2019022133	CIP-010-2	R2	[REDACTED] (the Entity)	[REDACTED]	08/05/2016	3/31/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 26, 2019, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-010-2 Part 2.1.</p> <p>The Entity reported that its CIP Senior Manager discovered, during the course of an internal Vulnerability Assessment, that documentation demonstrating the Entity’s compliance with CIP-010-2 R2 could not be located. Specifically, documentation demonstrating that the Entity had monitored at least once every 35 calendar days for changes to the baseline configuration for [REDACTED] was unavailable. The devices include [REDACTED] which [REDACTED] for the Entity’s primary and backup SCADA/EMS control centers and [REDACTED] which [REDACTED] at a Medium Impact generating facility.</p> <p>The cause of the noncompliance was that the Entity failed to follow its documented processes to monitor at least once every 35 calendar days for changes to the baseline configuration and to document and investigate detected unauthorized changes as required by CIP-010-2 Part 2.1.</p> <p>The noncompliance began on August 5, 2016, which was when the standard and requirement became enforceable (Phased-in Implementation Date) for CIP-010-2 Part 2.1, and ended on March 31, 2019, when the Entity changed its monitoring schedule to be compliant with the applicable standard.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the Entity had no security related updates or significant changes, other than password changes, applied to the affected devices during the period of noncompliance. Additionally, although it was not fully compliant with CIP-010-2 R2, a process was in place to monitor the [REDACTED] for baseline changes, and its SMEs [REDACTED] for the [REDACTED] quarterly and monitored for deviations. The only BES Cyber Assets affected were the [REDACTED]; other BCAs were not affected by this noncompliance. Lastly, all changes to the affected devices were tested prior to introduction into a production environment. No harm is known to have occurred.</p> <p>The Entity does not have any relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) compared the current [REDACTED] configurations and documented any changes; 2) shortened baseline monitoring periods to be compliant with the standard and requirement; 3) provided training on its internal policies and procedures related to CIP-007-6 and CIP-010-2 compliance to the SMEs responsible for the [REDACTED]; 4) assigned oversight responsibilities of [REDACTED] compliance to experienced senior CIP administrators; and 5) conducted refresher training on CIP-007-6 and CIP-010-2 policies and procedures for all 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
SPP2017017351	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	07/25/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 6, 2017, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R1. This Self-Report contained three instances that contained several issues. On September 27, 2017, the Entity submitted a scope expansion to its initial Self-Report, which added additional issues to the second instance of noncompliance.</p> <p>The first instance of noncompliance contained two issues where Cyber Assets, [REDACTED], had software installed that was not documented in the baselines.</p> <p>In the first issue, the Entity determined that it had installed software on [REDACTED] Electronic Access Control and Monitoring System (EACMS) devices, which were part of the Intermediate System prior to the implementation of CIPv5, but did not add the software to the baselines. This noncompliance began on July 1, 2016, when the standard became mandatory enforceable, and ended on May 19, 2017, when the Entity added the software to the baselines.</p> <p>In the second issue, the Entity determined it had installed [REDACTED] on [REDACTED] EACMS devices, which are part of the Intermediate System, prior to CIPv5, but it did not add the software to its baselines. The noncompliance began on July 1, 2016, when the standard became enforceable, and ended on December 14, 2016, when the baseline was updated.</p> <p>For the second instance of noncompliance, the Entity determined that it performed [REDACTED] unauthorized changes (software installation) (issues) that deviated from the baseline.</p> <p>In the first issue, the Entity determined that [REDACTED] applications were installed on [REDACTED] servers that were part of the Intermediate System, without prior authorization. This noncompliance began on November 1, 2016, when the applications were installed, and ended on December 9, 2016, when the applications were removed.</p> <p>In the second issue, the Entity determined that a newer version of an [REDACTED] software package was installed on [REDACTED] EACMS devices and [REDACTED] Physical Access Control and Monitoring System (PACS) device without prior authorization. This noncompliance began on November 23, 2016, when the application was installed on the first device, and ended by December 8, 2016, when the Entity approved the software change on the PACS device and the software was removed from the EACMS devices.</p> <p>In the third issue, the Entity discovered that a newer version [REDACTED] was installed on [REDACTED] PACS device without prior authorization. This noncompliance began on November 3, 2016, when the application was installed, and ended on November 28, 2016, when the software change was approved.</p> <p>In the fourth issue, the Entity discovered that an updated version of an [REDACTED] application was deployed to [REDACTED] Cyber Assets without prior authorization. This noncompliance began on January 25, 2017, when the application was installed, and ended on February 6, 2017, when the software change was approved.</p> <p>In the fifth issue, the Entity determined that an updated version of a [REDACTED] application was deployed to [REDACTED] PACS devices without prior authorization. The noncompliance began on March 5, 2017, when the software was installed, and ended on March 16, 2017, when the change was approved.</p> <p>In the sixth issue, the Entity discovered that [REDACTED] software was installed on one BES Cyber Asset (BCA) workstation without prior authorization. The noncompliance began on April 3, 2017, when the software was installed, and ended on April 4, 2017, when the software was removed.</p> <p>In the seventh issue, the Entity discovered that [REDACTED] software updates were applied to [REDACTED] EACMS device without prior authorization. The noncompliance began on July 22, 2017, when the patches were installed, and ended on July 25, 2017, when the virtual Cyber Asset was reverted to its previous state.</p> <p>For the third instance of noncompliance, the Entity determined that it performed unauthorized changes (software removal) that deviated from the baseline in one instance. In this instance, [REDACTED] software was removed from four EACMS servers without prior approval for the change to the baseline. This noncompliance began on October 12, 2016, when the software was removed, and ended on November 9, 2016, when the software removal was confirmed necessary.</p>					

	<p>The cause of noncompliance for the issues associated with the first instance was that the Entity’s process was insufficient and failed to account for software that is not detected automatically by its baseline tools [REDACTED]. The cause of the noncompliance for the issues associated with the second and third instances was that the Entity failed to follow its change management processes, resulting in unauthorized deviations from the established baselines.</p>
<p>Risk Assessment</p>	<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The issues associated with the first instance of noncompliance were minimal risk because the issues were limited to [REDACTED] software applications and [REDACTED] EACMS devices. The Entity identified this through the execution of secondary detective controls not required by the standard, which limited the duration. The issues were documentation-in-nature and, were resolved through updating the documented baselines, rather than making changes to any of the Cyber Assets. The [REDACTED] software applications of issue were core applications on the respective Cyber Assets [REDACTED]. Additionally, the Entity was well aware of the existence of this software, rather than it being unknown software that the Entity missed.</p> <p>The issues associated with the second instance of noncompliance were minimal risk because the longest duration was limited to 39 days and was resolved through a paperwork update of the documented baseline. The durations for the other six instances ranged from two to 25 days, which reflects short durations and reduced risk. Additionally, of the same six instances, four of them were documentation-in-nature and were resolved through approving the changes after the fact (instances one, three, four, and five).</p> <p>The issues associated with the third instance of noncompliance were minimal risk because they were limited to 29 days and a limited number of servers [REDACTED]. Additionally, the issue was documentation-in-nature and was resolved through approving the necessary change after the fact.</p> <p>No harm is known to have occurred.</p> <p>The Entity does not have any relevant compliance history.</p>
<p>Mitigation</p>	<p>To mitigate the issues associated with the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) added the software to the baselines for the affected devices; 2) modified its configuration change management checklist to identify whether software uses an installer and clarifying necessary actions; and 3) modified its process to package software such that it appears in the registry. <p>To mitigate the issues associated with the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) removed the software of issue; 2) authorized the PACS device software change and removed the EACMS devices software; 3) authorized software changes (instances three through five); 4) removed software from BCA workstation; 5) reverted the [REDACTED] Cyber Asset to its previous state; 6) added a peer review/cross-check step to the software deployment process prior to deployment; 7) held a coaching session for its SMEs to discuss the issues found and inform of the new peer review/cross-check process; 8) implemented a dedicated configuration management system for managing [REDACTED] Cyber Assets [REDACTED], which will allow for more focused attention as opposed to managing many device collections spread across multiple areas; and 9) conducted one on one coaching sessions. <p>To mitigate the issues associated with the third instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) confirmed/approved software change; and 2) held a coaching session for its SMEs to discuss the issues found and to specifically address not modifying scope of documented installations without approval.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022393	CIP-004-6	R5	[REDACTED] (the Entity)	[REDACTED]	08/27/2019	08/28/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 9, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5.</p> <p>The Entity reported that a new supervisor failed to revoke an individual’s (contractor) access to the designated storage locations for BES Cyber System Information (BCSI) by the end of the next calendar day following the effective date of the contractor’s termination.</p> <p>The cause of the noncompliance was that the Entity failed to follow its CIP-004-6 R5 process to revoke access to BCSI following a termination action.</p> <p>The issue began on August 27, 2019, when the Entity should have revoked the access, and ended on August 28, 2019, when the Entity revoked access to the BCSI.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the contractor did not access the BCSI storage location following the termination action. Additionally, the access was for BCSI storage locations only and did not provide access to any BES Cyber Assets. The duration of non-compliance to 16 hours, which significantly reduces the risk from exposure. Lastly, background checks, required training, and confidentiality terms were up to date for the terminated individual. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked the individual’s access to the BCSI; and 2) implemented a process to send access revocation notifications to new supervisors. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021449	CIP-010-2	R2	[REDACTED] (the Entity)	[REDACTED]	04/06/2018	04/26/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R2.</p> <p>While performing a review of a baseline, the Entity discovered that a baseline for one high impact BES Cyber Asset (BCA) had not been monitored for change within 35 days of the most recent monitoring cycle.</p> <p>The cause of the noncompliance was that the Entity did not follow its process to monitor at least once every 35 calendar days for changes to the baseline configuration as required in Requirement R1, Part 1.1.</p> <p>The noncompliance began on April 6, 2018, which was the 36th day after the last baseline verification was performed, and ended on April 26, 2018, when the baseline of the affected BCA was monitored for change from the most recent monitoring cycle.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was minimal because it was detected during the Entity’s baseline review process, limiting the duration to 21 days and was limited to one BCA. Additionally, the affected device resides within an Electronic Security Perimeter (ESP) and a Physical Security Perimeter (PSP) and thus required authentication to access the device. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed the baseline review; and 2) provided reinforcement training on 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
SPP2018019213	CIP-004-6	R4	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	02/28/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 15, 2018, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-004-6 R4. Additionally, the Entity submitted a Self-Certification on February 28, 2018 and a subsequent Self-Report on June 28, 2018. All three instances are being processed under this NERC violation ID.</p> <p>In the first Self-Report, the Entity reported that it discovered, during the 2017 Q4 access review, a physical access card, which granted access to both the primary Control Center (PCC) and alternate Control Center (ACC), was provisioned for a contractor. However, the contractor only had authorization for access to the PCC. The cause of the noncompliance was that the Entity failed to follow its documented process for provisioning physical access, which included reviewing the access after provisioning. The Entity reported that this was a fairly new step; however, the responsible individual relied on memory rather than referring to the documented process for provisioning access. The noncompliance began on December 22, 2017, when the contractor’s unauthorized access to the ACC was granted, and ended on December 29, 2017, when the individual’s access to the ACC was revoked.</p> <p>In the Self-Certification submittal, the Entity stated that it was in noncompliance with CIP-004-6 R4. This submittal contained ten instances where the Entity failed to authorize access to BES Cyber System Information (BCSI) storage locations.</p> <p>In the first instance of noncompliance reported in the Self-Certification, the Entity determined that [REDACTED] employees had unauthorized access to a [REDACTED] location that contained BCSI due to inherited permissions from a user group. The cause of the noncompliance was that the Entity failed to account for nested accounts with inherited permissions when determining individuals with access to its electronic BCSI storage locations. The noncompliance began on July 1, 2016, when the standard became enforceable, and ended on July 26, 2017, when the access was removed.</p> <p>In the second instance of noncompliance reported in the Self-Certification, the Entity determined that [REDACTED] employees that were members of a default administrators group had unauthorized access to two hard drives that contained BCSI. The cause of the noncompliance was that the Entity failed to account for nested accounts with inherited permissions when determining individuals with access to its electronic BCSI storage locations. The noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on August 1, 2017, when the access was removed.</p> <p>In the third instance of noncompliance reported in the Self-Certification, the Entity determined that [REDACTED] employees that were members of a default administrators group had unauthorized access to a hard drive that contained BCSI. The cause of the noncompliance was that the Entity failed to account for nested accounts with inherited permissions when determining individuals with access to its electronic BCSI storage locations. The noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on August 16, 2017, when the access was authorized.</p> <p>In the fourth instance of noncompliance reported in the Self-Certification, the Entity determined that [REDACTED] employees had unauthorized access to a shared storage location that contained BCSI due to inherited domain permissions. The cause of the noncompliance was that the Entity failed to account for nested accounts with inherited permissions when determining individuals with access to its electronic BCSI storage locations. The noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on August 1, 2017, when the access was removed.</p> <p>In the fifth instance of noncompliance reported in the Self-Certification, the Entity determined that [REDACTED] that was a member of a default administrators group had unauthorized access to a directory that contained BCSI. The cause of the noncompliance was that the Entity failed to account for nested accounts with inherited permissions when determining individuals with access to its electronic BCSI storage locations. The noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on August 7, 2017, when the access was authorized.</p> <p>In the sixth instance of noncompliance reported in the Self-Certification, the Entity determined that [REDACTED] employees that were in a default administrators group had unauthorized access to a directory that contained BCSI. The cause of the noncompliance was that the Entity failed to account for nested accounts with inherited permissions when determining individuals with access to its electronic BCSI storage locations. The noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on September 10, 2017, when the access was authorized.</p> <p>In the seventh instance of noncompliance reported in the Self-Certification, the Entity determined that [REDACTED] employees that were in a default administrators group had unauthorized access to a directory that contained BCSI due to an embedded shared service account. The cause of the noncompliance was that the Entity failed to account for nested accounts with inherited permissions when determining individuals with access to its electronic BCSI storage locations. The noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on September 10, 2017, when the access was authorized.</p> <p>In the eighth instance of noncompliance reported in the Self-Certification, the Entity determined that [REDACTED] employees were in a default administrators group had unauthorized access to a directory that contained BCSI due to an embedded shared service account. The cause of the noncompliance was that the Entity failed to account for nested accounts with inherited permissions when determining</p>					

	<p>individuals with access to its electronic BCSI storage locations. The noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on September 10, 2017, when the access was authorized.</p> <p>In the ninth instance of noncompliance reported in the Self-Certification, the Entity discovered that [REDACTED] had unauthorized access to a safe that contained physical BCSI information. The cause of the noncompliance was that the Entity failed to follow its policy of not sharing keys to physical storage locations containing BCSI. The noncompliance began on September 26, 2016, when the employee was hired (the Entity was unable to determine exactly when the employee obtained the code for the safe), and ended on May 11, 2017, when the access was authorized.</p> <p>In the last instance of noncompliance reported in the Self-Certification, the Entity determined that it discovered that [REDACTED] user accounts were created during the installation of log aggregation software before access roles were updated and authorized for new access privileges. The cause of the noncompliance was that the Entity's process failed to ensure that access to new accounts included with software applications was authorized prior to being granted. The noncompliance began on December 7, 2016, when the accounts were created, and ended on August 1, 2017, when the access was authorized.</p> <p>In the second Self-Report submittal, the Entity stated that it was in noncompliance with CIP-004-6 R4. This Self-Report contained two instances of noncompliance.</p> <p>In the first instance of noncompliance, the Entity determined that during a verification of access group consolidations performed on February 16, 2018, [REDACTED] employees had unauthorized access to a BCSI storage location. Further, the Entity did not identify this issue during the required 15-calendar month verification due to the accounts not appearing in the report because the accounts were nested within a larger organizational group. The cause of the noncompliance was that the Entity was not able to determine when or why the access was initially granted to these four individuals. The Entity did determine that its 15 month required review of access failed to account for nested accounts with inherited permissions when verifying that access to this storage location was correct. The noncompliance began on July 1, 2016, when CIPv5 became enforceable (the entity was unable to determine when access was actually granted so it submitted a date of July 1, 2016), and ended on February 28, 2018, when the unauthorized access was revoked.</p> <p>In the second instance of noncompliance, the Entity determined that while reviewing user access records on June 5, 2018, [REDACTED] had unauthorized access to a BCSI storage location. The cause of the noncompliance was that the Entity failed to accurately follow its process for granting access, resulting in additional access being granted beyond what was initially requested. The noncompliance began on August 23, 2016, when the user was created, and ended on March 14, 2017, when the user access was authorized.</p>
<p>Risk Assessment</p>	<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first Self-Reported instance of noncompliance was minimal risk because [REDACTED] did not have logical access to Cyber Assets at the ACC, which limited the harm that the contractor could cause to physical harm, which would not have impacted the PCC, and would have resulted in generated alerts in the event of unavailability. The access granted [REDACTED] was similar to that which was accurately authorized and granted at the PCC and had access been necessary to the ACC, it would have been granted without issue. The ACC resides within [REDACTED] which is staffed 24/7 and protected by access restrictions, which reduces the likelihood [REDACTED] would have accessed it. Additionally, the duration of the issue was limited to eight days and [REDACTED] was not used to access the ACC during the period of noncompliance. Lastly, the Entity has cameras placed around the cabinet housing the ACC, which provides an additional level of situational awareness of activities occurring at the ACC.</p> <p>The instances of noncompliance included in the Self-Certification were minimal risk because due to the nature of the Entity's cyber security training program that requires all Entity employees and contractors (not just those applicable to CIP-004) to complete annual cyber security training, which includes information protection, in addition to the CIP-004 required training. These employees are informed of the need to maintain the security, confidentiality, sensitivity, and integrity of the Entity's information, including BCSI. Additionally, [REDACTED], failure to properly handle sensitive and restricted information could lead to fines, suspension, job termination, or even confinement. MRO concluded that this demonstrates a heightened level of personal accountability for every individual with unauthorized access, which reduces the risk to the BPS. Additionally, all employees and contractors of the Entity (not just those applicable to CIP-004) are required to have successfully completed background investigations, resulting in all individuals with unauthorized access having completed the same. Lastly, the Entity's Control Centers contains medium impact BES Cyber Systems (BCS) (no high impact BCS were identified). These Control Centers only control and monitor assets that contain low impact BES Cyber Systems, which inherently limits the impact to the BES.</p> <p>The second Self-Reported instances of noncompliance were minimal risk. In first instance, the unauthorized access granted to [REDACTED] was limited to a single, empty folder in [REDACTED] for which the Entity had not published links. The lack of data within the folder, as well as the difficulty locating the folder, significantly reduced the likelihood of access and thus reduced the likelihood of harm. In the second instance, the unauthorized access granted to the individual was discovered and corrected as a result of an authorization request to grant that individual access, which demonstrates that the individual had a business need for access, was unaware of their unauthorized access, and that the issue was documentation-in-nature, which limited the risk it posed.</p> <p>No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>

<p>Mitigation</p>	<p>To mitigate the first Self-Reported instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked access to the ACC from [REDACTED]; and 2) updated its physical access provisioning automated workflow process to request confirmation that provisioned access matches what was authorized and to submit a screenshot demonstrating it. The Entity had attempted mitigation for reoccurrence; however it later found that the mitigation did not work correctly. It was subsequently revised as described above and confirmed it is working. <p>To mitigate the first instance of noncompliance in the Self-Certification, the Entity:</p> <ol style="list-style-type: none"> 1) removed access for the [REDACTED] employees; and 2) reminded employees who grant electronic access to be mindful of inherited access and nested groups and to reorganize access structures carefully. <p>To mitigate the second instance of noncompliance in the Self-Certification, the Entity:</p> <ol style="list-style-type: none"> 1) removed access for the [REDACTED] employees; and 2) reminded employees who grant electronic access to be mindful of inherited access and nested groups and to reorganize access structures carefully. <p>To mitigate the third instance of noncompliance in the Self-Certification, the Entity:</p> <ol style="list-style-type: none"> 1) authorized the access for the [REDACTED] employees; and 2) reminded employees who grant electronic access to be mindful of inherited access and nested groups and to reorganize access structures carefully. <p>To mitigate the fourth instance of noncompliance in the Self-Certification, the Entity:</p> <ol style="list-style-type: none"> 1) removed access for the [REDACTED] employees; and 2) reminded employees who grant electronic access to be mindful of inherited access and nested groups and to reorganize access structures carefully. <p>To mitigate the fifth instance of noncompliance in the Self-Certification, the Entity:</p> <ol style="list-style-type: none"> 1) authorized the access for [REDACTED] and 2) reminded employees who grant electronic access to be mindful of inherited access and nested groups and to reorganize access structures carefully. <p>To mitigate the sixth instance of noncompliance in the Self-Certification, the Entity:</p> <ol style="list-style-type: none"> 1) authorized access for the [REDACTED] employees; and 2) reminded employees who grant electronic access to be mindful of inherited access and nested groups and to reorganize access structures carefully. <p>To mitigate the seventh instance of noncompliance in the Self-Certification, the Entity:</p> <ol style="list-style-type: none"> 1) authorized access for the [REDACTED] employees; and 2) reminded employees who grant electronic access to be mindful of inherited access and nested groups and to reorganize access structures carefully. <p>To mitigate the eighth instance of noncompliance in the Self-Certification, the Entity:</p> <ol style="list-style-type: none"> 1) authorized access for the [REDACTED] employees; and 2) reminded employees who grant electronic access to be mindful of inherited access and nested groups and to reorganize access structures carefully. <p>To mitigate the ninth instance of noncompliance in the Self-Certification, the Entity:</p> <ol style="list-style-type: none"> 1) authorized access for [REDACTED] and 2) reminded authorized users of BCSI physical storage locations that access is limited to those authorized and not to share access tools, such as keys, with other personnel. <p>To mitigate the last instance of noncompliance in the Self-Certification, the Entity:</p> <ol style="list-style-type: none"> 1) authorized access associated with the new accounts; and 2) modified its change request template to require that its information security officers be notified of new software applications and accounts so that access authorizations can be completed prior to their implementation. The change request cannot progress through the workflow without approved access authorizations for the new accounts. <p>To mitigate the first instance of the second Self-Reported noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked access to the [REDACTED] 2) reminded employees who grant electronic access to be mindful of inherited access and nested groups and to reorganize access structures carefully; 3) implemented an automated access request system to replace its manual workflows, which will ensure that the process is followed; and
--------------------------	--

	<p>4) provided training on the new process and a refresher on the CIP-004 access requirements and associated responsibilities to those responsible for access.</p> <p>To mitigate the second instance of the second Self-Reported noncompliance, the Entity:</p> <ol style="list-style-type: none">1) authorized [REDACTED]2) implemented an automated access request system to replace its manual workflows, which will ensure that the process is followed; and3) provided training on the new process and a refresher on the CIP-004 access requirements and associated responsibilities to those responsible for 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
SPP2018019314	CIP-003-3	R6	[REDACTED] (the Entity)	[REDACTED]	06/16/2016	09/19/2016	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 28, 2018, the Entity submitted a Self-Certification stating that, as [REDACTED], it was in noncompliance with CIP-003-3 R6. The Entity reported four instances of noncompliance related to its change management program. All four instances occurred with the same overall change, which was the addition of a network intrusion detection system (NIDS).</p> <p>The Entity reported that it authorized the change request to add the NIDS, however it failed to explicitly authorize changes to associated network devices as required by its processes. In the first instance of noncompliance, [REDACTED] and one switch stack were changed. In the second instance of noncompliance, [REDACTED] was changed. In the third instance of noncompliance, [REDACTED], one router, and one switch were changed. In the fourth instance of noncompliance, after modifications to one switch for the addition of a NIDS sensor to the backup Control Center, the Entity determined it failed to perform the post-change testing as required by CIP-010-2 R1 Part 1.4.2. The next security controls assessment for switch in instance four occurred after the modifications were made, which reflects the occurrence of post-change verification of required security controls.</p> <p>Instances one and two, actually began under CIP-005-3a, R1.5 and instances three and four occurred under CIP-010-2 R1, Part 1.2. Since CIP-010-2 R1 has a clear path back to CIP-003-3a R6 and CIP-005-3a R1.5 refers to the requirements in CIP-003-3a R6, MRO determined to process all instances under CIP-003-3 R6.</p> <p>The cause of the noncompliance for all instances was that the Entity’s change control process lacked clarity for situations where tangential Cyber Assets (CA) were also impacted, which led to missed verification and authorization for those CAs.</p> <p>The aggregate of the noncompliance began on June 16, 2016, when changes that deviated from the baseline for instance three were not authorized, and ended on September 19, 2016, when all changes were approved.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk for all instances was minimal because they were documentation issues and the failure to authorize a change that was necessary was subsequently approved. Additionally, the risk for the fourth instance was minimal because the duration was 13 days; however, since the standard does not include a required timeline for when post-change verification must occur, MRO concluded that this delay in post change verification reflects a reasonable timeframe and significantly reduced risk. Lastly, in all instances, the issue was mitigated through secondary controls before the noncompliance was discovered, which limited the duration of the noncompliance. No harm was known to have occurred.</p> <p>MRO considered the Entity’s compliance history and determined that it should not serve as a basis for applying a penalty.</p>					
Mitigation			<p>To mitigate the instances of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) approved changes, after the fact (instances one through three); 2) performed post change verification (instance four); and 3) revised its policy to require separate change requests for changes impacting associated assets. This includes the requirement for separate approval of the changes as well as separate post-change verification of security controls. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2018019316	CIP-007-3a	R3	[REDACTED] (the Entity)	[REDACTED]	05/04/2016	03/01/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 28, 2018, the Entity submitted a Self-Certification stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2. The Entity identified three instances where it failed to either evaluate or install a patch within the required 35-day window.</p> <p>In the first instance of noncompliance, (CIP-007-6 R2, Part 2.2) the Entity discovered that during its annual vulnerability assessment, it identified [REDACTED] that were not running the most recent security related versions of firmware, indicating that a patch had been missed. The patch of issue was originally not identified as a security patch by the vendor. The vendor later updated the patch details and identified it as a security patch, however this occurred after the Entity’s patch evaluation window. Subsequent patch evaluations did not identify the patch because its release date occurred during previous reviews, so it was not re-considered. The noncompliance began on March 7, 2017, which was 36 days after the previous patch evaluation, and ended on May 1, 2017, when the patch was evaluated.</p> <p>In the second instance of noncompliance (CIP-007-3a R3.1), the Entity determined that during its annual vulnerability assessment, it identified one switch [REDACTED] that was not running the most recent security related version of firmware, indicating that one or more patches had been missed. One patch had been placed on the switch, but the switch configuration had not been updated to point to the new version; this occurred for one subsequent patch as well. The noncompliance began on May 4, 2016, which was the day after the Entity planned to install the patch on the switch (and did install the patch on the partner switch of the switch stack), and ended on May 8, 2017, when the switch configuration was modified to point to the latest patch.</p> <p>In the third instance of noncompliance (CIP-007-6 R2, Part 2.2), while performing a vulnerability assessment during the implementation of a new Control Center, the Entity identified one application on [REDACTED] that had not been patched. Further review determined that a total of two patches had not been evaluated or installed for that application. The noncompliance began on January 3, 2019, which was the day after the patch evaluation date that should have included the first missed patch, and ended on March 1, 2019, when the second patch was evaluated.</p> <p>The cause of noncompliance for all three instances was that the Entity failed to follow its processes for patch evaluation and implementation.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance of noncompliance was minimal risk because this issue was the result of a change made by the vendor after the initial release of the patch. MRO determined that rather than being a systemic failure of the Entity’s process, it was an atypical case, with limited likelihood for reoccurrence and limited the risk posed. The Entity’s Control Centers contain medium impact BCS; no high impact BCS were identified. These Control Centers only control and monitor assets that contain low impact BCS, which inherently limits the impact to the BES.</p> <p>The second instance of noncompliance was minimal risk because the issue was limited to two patches on one switch. The Entity’s Control Centers contain medium impact BCS; no high impact BCS were identified. These Control Centers only control and monitor assets that contain low impact BCS, which inherently limits the impact to the BES. Since the BCA of issue is a network switch, its misuse is limited to obtaining a foothold on the CA, which could lead to impacts on network availability of BCS components such as turning off the switch or disabling ports and/or attempting to access other connected Cyber Assets within the Electronic Security Perimeter for which additional physical or electronic access would also be required.</p> <p>The third instance of noncompliance was minimal risk because the issue was limited to two patches for one application. The issue was identified during a vulnerability assessment performed as part of the new commissioning of these CAs, which limited the duration to 58 days. The Entity’s Control Centers contain medium impact BCS; no high impact BCS were identified. These Control Centers only control and monitor assets that contain low impact BCS, which inherently limits the impact to the BES.</p> <p>No harm is known to have occurred.</p> <p>The Entity does not have any relevant compliance history.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) evaluated the missed patch; 					

<p>2) increased its staff to include an additional network administrator as well as replaced its lead network administrator for management of the SCADA network devices.</p> <p>To mitigate the second instance of noncompliance, the Entity:</p> <p>1) updated the switch configuration to use the most recent patches; and 2) increased its staff to include an additional network administrator as well as replaced its lead network administrator for management of the SCADA network devices.</p> <p>To mitigate the third instance of noncompliance, the Entity:</p> <p>1) evaluated the missing patches; and 2) provided employees with a refresher on using the vendor’s site for identifying applicable patches.</p>

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020765	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	09/20/2016	03/17/2017	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], MRO determined that the Entity, as a [REDACTED], had two instances of noncompliance for CIP-007-2 R2.</p> <p>In the first instance of noncompliance, it was discovered that patch assessments for its Intrusion Detection System (IDS) application had been completed late for [REDACTED] sampled medium impact BES Cyber Assets (BCAs), Protected Cyber Assets (PCAs), associated Physical Assess Control and Monitoring Systems (PACS), and associated Electronic Access Control and Monitoring Systems (EACMS) devices. However, after an extent of condition analysis, the Entity determined that this issue actually affected [REDACTED] medium impact BES Cyber Assets (MIBCA) that were a combination of, PCAs, associated PACS, and associated EACMS. The cause of this instance of noncompliance was the Entity did not follow its CIP-007-6 process to identify and track cyber security patch sources. This instance of noncompliance began on September 20, 2016, when the Entity failed to assess a single IDS patch, and ended on November 2, 2016, when the Entity evaluated the patch.</p> <p>In the second instance of noncompliance, it was discovered that patch assessments for a single vendor patch had been completed within the required 35 days for [REDACTED] sampled MI BCAs, PCAs, associated PACS, and associated EACMS. After an extent of condition analysis, the Entity discovered that this issue affected a combination of [REDACTED] MIBCA, PCAs, associated PACS, and associated EACMS. The cause of this instance of noncompliance was an employee failed to recognize that a second vendor patch notification email in the same day was actually a separate patch that the Entity needed to evaluate within 35 days. This instance of noncompliance began on March 11, 2017, when the Entity failed to assess the patch, and ended on March 17, 2017, when the Entity evaluated the patch.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance is minimal risk because the Entity’s Control Center only contains medium impact BES Cyber Systems and [REDACTED]. Additionally, this issue only impacted a single patch from a single source. Lastly, the duration of the noncompliance was limited to 44 days, reducing the exposure of the vulnerability on the Entity’s BCAs.</p> <p>The second instance is also minimal risk because the Entity’s Control Center only contains medium impact BES Cyber Systems and [REDACTED]. Additionally, this issue only impacted a single patch from a single source. Lastly, the duration of the noncompliance was limited to seven days, reducing the exposure of the vulnerability on the BCAs.</p> <p>No harm is known to have occurred.</p> <p>The Entity does not have any relevant compliance history.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) identified the patch source and evaluated the single cyber security patch released by the source. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) evaluated the missed cyber security patch. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021631	CIP-007-6	R1.	[REDACTED]	[REDACTED]	12/13/2017	01/07/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>On June 3, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED], it discovered through a NERC Cyber Vulnerability Assessment (CVA) that it was in noncompliance with CIP-007-6 R1. (1.2). The entity failed to protect against the use of unnecessary physical input/output (I/O) ports for seven assets.</p> <p>The CVA was performed by a third party vendor at all of the entity’s High Impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) and Protected Cyber Assets (PCA).</p> <p>The vendor’s assessment, aided by the entity staff, found that seven assets were noncompliant. [REDACTED] three PCAs had a degradation of the adhesive backing material of each piece of tamper tape, causing the tape to peel away from each of their input/output (I/O) ports. The [REDACTED] also held two additional PCAs with I/O ports that were devoid of tamper tape. Another [REDACTED] location, held two PCAs with I/O ports devoid of tamper tape.</p> <p>This noncompliance started on December 13, 2017 when the entity reclassified the assets as Protected Cyber Assets (PCAs) and failed to ensure I/O ports were protected against inadvertent use by the application of tamper tape. The noncompliance ended on January 7, 2019 when the entity applied new tamper tape to all I/O ports of the seven devices.</p> <p>The root cause of this noncompliance was a failure to associate the reclassification of assets with the necessity of performing a review of I/O ports.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not applying tamper tape to applicable I/O ports the entity would not be able to convey the applicable I/O ports should not be used without proper authorization. An I/O port without the required tamper tape could expose the entity’s assets hosting such I/O ports to unauthorized access, misuse and/or accidental use due to the noncompliance.</p> <p>However, the entity reduced the risk because the assets hosting each I/O port at issue reside within high impact Physical Security Perimeters (PSPs). The PSPs are [REDACTED]. The PSPs are [REDACTED]. The noncompliance was mitigated upon discovery and an interrogation of each asset found no unauthorized access or use prior to the tamper tape being reapplied/applied to the applicable I/O ports.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) applied tamper tape to each I/O port for PCAs; and 2) revised the change management document directing review of impacted resources at least every 15 months unless prompted sooner by a change. 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021622	CIP-011-2	R1	[REDACTED]	[REDACTED]	2/21/2019	3/29/2019	Self-Report	May 29, 2020
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)</p>			<p>On May 23, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-011-2 R1. This noncompliance involves two instances.</p> <p>First, on February 21, 2019, when an entity employee in the [REDACTED] group copied Bulk Electric System Cyber System Information (BCSI) material from their company laptop to an unencrypted removable media device. [REDACTED] The entity was undergoing a personal computer/laptop hardware refresh which includes a small number of employees who have a business need to write to unencrypted removable media who also have access to BCSI. During the refresh, the employee attempted to backup their files to a removable media device which included documents labeled and containing data elements considered BCSI. The employee kept the removable media with him in his laptop bag as part of their issued equipment for the duration of the instance.</p> <p>The entity's automated detective control [REDACTED] flagged transfer of data labeled as "Confidential Special Handling" on February 21, 2019 and directed that flagging to IT Security. On February 25, 2019, IT Security informed the [REDACTED] Group of this instance. The [REDACTED] Group then reached out to the employee at issue on March 18, 2019 and the employee informed the [REDACTED] Group that BCSI was no longer stored on the unencrypted removable media device as the BCSI was deleted from that device on March 18, 2019. [REDACTED]</p> <p>Second, on March 29, 2019, as a result of event logs from the [REDACTED] endpoint agent, the entity discovered that an individual in [REDACTED] transferred files to unencrypted removable media, which included documents labeled and containing data elements [REDACTED] which were labeled "Confidential Special Handling." [REDACTED] The employee transferred the data to the removable media because the workstation assigned to the employee was undergoing PC Lifecycles and the employee was backing up data from his workstation prior to turning in his workstation for a replacement. The employee retained the removable media on his person for the duration of the noncompliance. The entity's automated detective control [REDACTED] flagged transfer of data labelled as "Confidential Special Handling" on March 29, 2019. IT Security was notified of the log generation who directed it to the [REDACTED] team that same day. [REDACTED] contacted the employee and manager the same day and had the sensitive data removed from the unencrypted removable media.</p> <p>In both instances, the employees were granted access to BCSI and an exemption to be able to write to unencrypted removable media due to technology limitations and job requirements. Both employees were performing a PC Lifecycle replacement process, did not follow instructions included with the new device, and used a personal unencrypted removable media device to back up information from the old computer prior to transferring to the new computer. Copying the old computer hard drive to removable media is not part of this process, but employees took this step based on historical processes and in prevention of losing information. Both employees had received the appropriate CIP training.</p> <p>The entity identified both instances through a detective control [REDACTED] to identify when files labelled as "Confidential Special Handling" are transferred from the laptop to removable media. The control event detection alerted IT Security who notified [REDACTED] (These were the first instances of BCSI data transferred to unencrypted removable media identified through this detective control which had been in place since 2016.)</p> <p>This noncompliance involves the management practices of work management, workforce management, and verification. The root cause is a lack of awareness regarding policies and requirements for data transfer from computers to removable media. In both instances, the employees did not understand and follow the entity's policies and procedures for handling and transferring BCSI.</p> <p>This noncompliance started on February 21, 2019, when an individual in [REDACTED] transferred files to unencrypted removable media (the first instance) and ended approximately on March 29, 2019, when the information was removed from the removable media (the second instance).</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is transferring BCSI data to an unencrypted external media increases the likelihood that the BCSI data could be lost, become irretrievable, or become compromised. The risk is minimized because the BCSI data transferred to the unencrypted removable media [REDACTED] The unencrypted media at issue remained in possession and control of the person authorized to use the unencrypted external media for the duration of the noncompliance in both instances. The employees at issue in both instances also had up to date Personnel Risk Assessments (PRA) and up to date NERC CIP training. Lastly, both instances were identified by the entity's detective control. No harm is known to have occurred.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021622	CIP-011-2	R1	[REDACTED]	[REDACTED]	2/21/2019	3/29/2019	Self-Report	May 29, 2020
			<p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) contacted the entity employee and manager and confirmed that the BCSI was removed from the removable media. The entity provided verbal coaching to the employee on the policy not to use unencrypted removable media with BCSI material (first instance); 2) contacted the entity employee and manager and confirmed that the BCSI was removed from the unencrypted removable media and were trained on BCSI storage requirements. The entity provided verbal coaching to the employee on the policy not to use unencrypted removable media with BCSI material (second instance); 3) updated the [REDACTED] tool configuration in the corporate environment (where the incidents occurred) to alert users if they are attempting to copy BCSI to removable media and verify that is the intent; 4) reviewed and documented removable media technologies applicable to the entity which would minimize the need for unencrypted removable media; 5) identified and documented stakeholders in supporting CIP-011 R1 and drafted a [REDACTED] matrix in order to incorporate in the Information Protection Plan (IPP). Formalizing these responsibilities will clarify communication requirements for later milestones (awareness, training, and technology/controls implementation) 6) incorporated CIP-011 R1 [REDACTED] and stakeholder list in IPP. The entity will revise the IPP framework with stronger definitions of BCSI for an entity applicable environment. [REDACTED] 7) created and documented processes to support the IPP on the use case for reproducing BCSI, storage requirements for BCSI, and a process flow and checklist for desk reference. These will be child documents of the IPP updated by the applicable BU and housed with the IPP. <p>To mitigate this noncompliance, the entity will complete the following mitigation activities by May 29, 2020:</p> <ol style="list-style-type: none"> 1) will approve a CIP-011 R1 Awareness Program Plan to include awareness of this situation when backing up PCs, not saving "convenience copies" of BCSI to hard drive. This awareness will provide training to groups who have write access to removable media. This training will be delivered via several methods - meetings, blog posts and emails, and other methods - over the course of the next year in order to increase the presence of the IPP in everyday entity activities; 2) will document review of available security tools and recommendation for use; and 3) will test the chosen encrypted removable media technology with documented learnings. For users with authorized electronic or BCSI access who also have USB removable media exceptions, (1) reaffirm the exceptions are still needed by end users and (2) roll out new encrypted removable media technology to end users. Provide new encrypted removable media technology with training and documentation on use, administration, and distribution of devices. Document evidence of implementation and adoption. <p>The entity needs until May to complete mitigation because of the time it will take them to approve a new CIP-011 R1 Awareness Program and Plan. Additionally, the entity needs additional time to test the chosen encrypted removable media technology and document learnings.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021833	CIP-004-6	R5	[REDACTED]	[REDACTED]	2/12/2019	2/13/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 10, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5.</p> <p>The entity discovered that an employee separation form was backdated and that resulted in an individual having authorized unescorted physical access to multiple Bulk Electric System (BES) Cyber Systems for more than 24 hours after the individual's termination date.</p> <p>The employee was terminated on February 11, 2019. His access should have been revoked on February 12, 2019, but his access was not revoked until February 13, 2019. The entity discovered this issue through an automated notification (an internal control) to investigate the employee's access on February 13, 2019 based on the employee's termination date.</p> <p>This noncompliance involves the management practices of workforce management through ineffective training and planning. The root cause of this noncompliance was ineffective training as an entity employee incorrectly submitted backdated personnel action forms. The entity also did not have an effective internal control in place to ensure that personnel action forms were properly submitted and processed.</p> <p>This noncompliance started on February 12, 2019, when the entity was required to remove the individual's access due to a termination and ended on February 13, 2019 when the entity removed the individual's access.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by not timely revoking the terminated individual's access is that it allows an individual to continue to access and potentially harm BES Cyber Systems when that individual is no longer authorized to have such access. The employee had a valid Personnel Risk Assessment (PRA) and CIP Training at the time of his termination. The risk is further reduced because the entity removed the individual's access just one day late, and identified the issue as a result of an internal control. Lastly, ReliabilityFirst notes that there were no adverse effects to any BES Cyber Assets due to this delayed access removal. The employee did not use his unescorted physical access privileges after his last day of work. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed access in the Physical Access Control Systems (PACS) and obtained the employee's badge. Review of the PACS indicated the badge was last used on January 25, 2019; and 2) sent a communication [REDACTED] The email alerted them to the compliance issues of back dating terminations and transfers and reiterated the procedures to be followed which ensure compliance with company policies. [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
RFC2019021931	CIP-004-6	R4	[REDACTED]	[REDACTED]	6/4/2019	7/11/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 18, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R4.</p> <p>During a quarterly access reconciliation review on July 11, 2019, the entity determined that an employee was granted access to an electronic storage location containing Bulk Electric System Cyber Systems Information (BCSI) without appropriate authorization.</p> <p>The employee had access to reports that contained no actual BCSI. (The entity employee accessed one of the reports on two separate occasions.) The entity classified the reports as containing BCSI out of an abundance of caution. [REDACTED] Nothing that the employee had access to could lead to compromise or misuse of any CIP asset.</p> <p>Following this discovery, the entity investigated the matter and determined that an individual responsible for provisioning access inadvertently added the employee to an Active Directory (AD) group in the corporate domain which provided access to an electronic storage location containing reports classified as BCSI.</p> <p>This noncompliance involves the management practice of workforce management through ineffective training. The root cause of this noncompliance was ineffective training as the individual responsible for provisioning access inadvertently added the employee to an AD group in the corporate domain which provided access to an electronic storage location containing reports classified as BCSI. The entity also did not have an effective internal control to help prevent or quickly detect this type of inadvertent error.</p> <p>This noncompliance started on June 4, 2019, when the entity inappropriately granted an employee access to an electronic storage location containing reports classified as BCSI without appropriate authorization and ended on July 11, 2019, when the employee’s access was removed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is allowing an unauthorized employee to access and potentially compromise BCSI. The risk is minimized because the employee only had access to reports that contain no actual BCSI. The entity had classified the reports as containing BCSI out of an abundance of caution. The employee at issue was also a trusted employee. Additionally, ReliabilityFirst notes that there were no adverse effects to any equipment identified because of this inadvertent provisioning of access. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the employee from the AD group that provided electronic access to a storage location containing BCSI; and 2) revised an access provisioning procedure and retrained staff to perform a visual verification control for provisioning access in AD domains granting electronic access to CIP assets to include provisioning of AD groups in the corporate domain. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019609	CIP-007-6	R2	[REDACTED]	[REDACTED]	2/3/2018	2/5/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On April 20, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [REDACTED] it was in violation of CIP-007-6 R2.</p> <p>The entity failed to apply a [REDACTED] within thirty-five (35) days of the patch assessment as required under CIP-007-6 R2.3 The security patch assessment was performed on December 29, 2017, and thus the patch application due date was February 2, 2018. The entity completed patch installation on February 5, 2018 (i.e., 3 days late).</p> <p>The engineer responsible applied the security patch to [REDACTED] within the time frame of the requirement but failed to apply to the fifth [REDACTED] because he did not refer to the [REDACTED] list while [REDACTED]. The server that did not receive the patch update in time under CIP-007-6 R2.3 was a backup server.</p> <p>The root cause of this noncompliance was twofold. First, the engineer failed to refer to the [REDACTED] while patching the applicable [REDACTED]. Second, the engineer in charge waited until the 35th day to apply the patches, which provided the entity no margin for error to identify the missed [REDACTED] and remediate.</p> <p>This noncompliance involves the management practices of asset and configuration management and verification. Asset and configuration management is involved because the entity did not have an adequate configuration change management process to identify all affected devices for patching. Verification is involved because the process lacked an adequate step to verify that all affected devices were included in patch application.</p> <p>The violation began on February 3, 2018, the date the thirty-five (35) day window for patch installation ended, and ended on February 5, 2018, the date the entity applied the patch to the [REDACTED].</p>					
Risk Assessment			<p>This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this noncompliance is that applying a patch three days late increases the opportunity for vulnerabilities that could provide a larger attack surface via the unpatched device. The risk in this violation is minimal because only one device was impacted and the duration was limited to three days. Additionally, the [REDACTED] resides on an internally protected network segment, which is separated from the rest of the network and by a firewall device. Further, the entity utilizes malicious code prevention tools and continuous monitoring. No harm is known to have occurred.</p> <p>Although the current noncompliance involve conduct that is arguably similar to the previous noncompliances, the current noncompliance continues to qualify for compliance exception treatment as it involves high-frequency conduct for which the entity has demonstrated an ability to promptly identify and correct noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) deployed the security patches to the affected systems; 2) edited the [REDACTED] 3) added additional oversight to the Patch Management Compliance Review Process; 4) created an updated Mitigation Plan method which will update its internal mitigation method to account for delays in patching beyond entity control; 5) provided training on the new Mitigation Plan for all subject matter experts that will use the Mitigation Plan method to ensure that there is no confusion on the new method; 6) employed the assistance of an external vendor to assist in the Security Patching process. The vendor will send reports to the entity on a monthly basis to inform the entity on new or pending Security Patches; and 7) provided training of the [REDACTED] to ensure that multiple individuals now are able to read and ensure that action is taken on [REDACTED]. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021476	CIP-010-2	R3	[REDACTED]	[REDACTED]	7/1/2018	9/13/2018	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 noncompliance.)			<p>On May 7, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R3.</p> <p>The entity did not perform an Active Vulnerability Assessment as required by CIP-010-2 R3 Part 3.2 by the July 1, 2018 implementation date. Entity staff missed the initial performance date due to insufficient oversight and inadequate tracking of interval-driven CIP requirements. [REDACTED] The entity’s [REDACTED] discovered this noncompliance while preparing to perform a Paper Vulnerability Assessment.</p> <p>This noncompliance involves the management practices of workforce management and reliability quality management. The root cause is that the entity did not have adequate internal controls in place to ensure it completed the Active Vulnerability Assessment on time. The entity misunderstood that although the interval for performing an Active Vulnerability Assessment is at least once every 36 months, the initial performance for an Active Vulnerability Assessment for High Impact Bulk Electric System Cyber Systems was required by July 1, 2018 (24 months after the effective date of CIP-010-2).</p> <p>This noncompliance started on July 1, 2018, when the entity was required to comply with CIP-010-2 R3 and ended on September 13, 2018, when the entity completed the overdue Active Vulnerability Assessment.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed is failing to identify security related vulnerabilities which could result in [REDACTED]. The risk is minimized because the entity performed the Active Vulnerability Assessment approximately two months late. ReliabilityFirst notes that when the entity performed the overdue Active Vulnerability Assessment, no problems that could have exposed assets to attack were detected. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) performed the overdue Active Vulnerability Assessment. The entity confirmed that no other Vulnerability Assessments were missed; 2) [REDACTED] 3) trained staff on the new tool [REDACTED] 4) [REDACTED] 5) implemented network based periodic task scheduling with automated reminders. <p>The entity also instituted short, weekly meetings to discuss upcoming compliance tasks: (a) Short interval (e.g., 15 and 35 day) compliance tasks due within the next two weeks; (b) Longer interval compliance tasks (e.g., quarterly or longer) due within the next 6 weeks; and (c) The compliance tasks that have been completed since the last meeting, what evidence has been produced, and the location of that evidence. (Subject matter experts examine longer interval tasks in order to determine if preparation is necessary, such as defining a plan or ensuring that proper resources are available. Short interval tasks are far more routine in nature, and are typically addressed in stride. Meeting minutes are kept of each meeting, and spreadsheets track the completion date for each periodic task and the location of the evidence produced.)</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019862	CIP-010-2	R4	[REDACTED]	[REDACTED]	04/13/2018	04/13/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On June 15, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R4. The Entity reported an instance where it connected a Transient Cyber Asset (TCA) to a BES Cyber Asset (BCA), in violation of its TCA procedure.</p> <p>On April 13, 2018, the Entity’s technician intended to connect his laptop (TCA) to a non-production network switch for troubleshooting purposes, however, he unintentionally connected the TCA to the console port of a production network switch. The production network switch is a BCA that is part of a medium impact substation BES Cyber System (BCS). The Entity’s procedure specifically prohibits the use of TCA for accessing a BCA in a High or Medium BES Cyber System. Shortly after, a [REDACTED], who was involved in troubleshooting the non-production network switch, recognized the procedural oversight and alerted the Entity. The connection lasted for twenty-five minutes.</p> <p>On May 1, 2018, the Entity conducted an extent-of-condition by interviewing all personnel involved. The Entity did not find any additional instances of noncompliance.</p> <p>The scope of affected facilities included [REDACTED]</p> <p>This noncompliance started on April 13, 2018, when the technician connected a disallowed TCA into a BCA, and ended on April 13, 2018, twenty-five minutes later, when the Entity disconnected the TCA from the BCA.</p> <p>The cause of this noncompliance was management oversight for failing to implement an adequate control to prevent the noncompliance. The Entity failed to have a unique label to distinguish the non-production devices from the production devices, as both devices were labeled with the same asset name.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Entity Staff connecting an unapproved TCA to a BCA increased the risk of introduction of malicious code. Misoperations, configuration changes, or degradations in situational awareness could have compromised grid safety and security. However, the duration was on 25 minutes, and the connection was only provisioned for read-only access as the technician did not know the enable password on the network. Additionally, the Entity employed antivirus on Cyber Assets and utilized a centralized real-time monitoring system to detect and respond to unexpected logging activity. The Entity also had a real-time security configuration management system in place to detect and alert for use of undefined ports or services. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> completed forensic analysis of the TCA that was connected to the network switch (BCA), which included a review of the local logs [REDACTED] that indicated no suspicious activity identified during the timeframe in question, and there was no evidence of malicious code found on the laptop; Reviewed the running configuration file for the network switch (BCA), which indicated no changes made to the configuration of the network switch (BCA) based upon the last configuration change date of 01/24/2018 indicated in the file; the Manager of [REDACTED] provided, during a previously scheduled [REDACTED] training engagement for the [REDACTED], a physical copy of [REDACTED] to those in attendance, as well as, spoke to the group about the process breakdown that created the potential non-compliance violation; the Manager of [REDACTED] sent an email to the [REDACTED] to reiterate the importance of following the [REDACTED] published on [REDACTED]. The manager also provided insight into NERC terminology used in the procedure, instructions on how to access NERC procedures on [REDACTED] as well as detailed description of the process breakdown that created the potential compliance violation; The Manager of [REDACTED] discussed the potential TCA non-compliance violation, as well as facilitated a general compliance discussion with attendees of the [REDACTED] All Employees department meeting; added TCA-related administrative procedure training to all departmental employee onboarding checklists to make them aware of existing regulations; and ensured that equipment labeling is proper, standardized, and put in place for all existing and new [REDACTED]/NERC sites. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019719	CIP-007-6	R5, P5.2, P5.6	[REDACTED]	[REDACTED]	07/01/2016	06/30/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], SERC determined that the Entity, as a [REDACTED], was in noncompliance with CIP-007-6 R5, P5.2. The Entity did not identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type (Instance 1). During the same Compliance Audit, SERC determined that the Entity was in noncompliance with CIP-007-6 R5, P5.6. The Entity did not implement one or more documented process that included, where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months (Instance 2). SERC has determined that Instance 2, designated as [REDACTED], involves the same Standard and Requirement as Instance 1. Therefore, SERC is utilizing a single tracking number, SERC2018019719, for both instances and has dismissed [REDACTED].</p> <p>In Instance 1, on [REDACTED], SERC Audit discovered [REDACTED] default accounts that were not included in the Entity’s list of default or other generic accounts. Despite not appearing on the formal list of default or other generic accounts, SERC Audit noted that the Entity was otherwise properly protecting the default accounts at issue.</p> <p>The Entity performed an extent-of-condition assessment by reviewing its known default or other generic accounts to its accounts list for [REDACTED]. The Entity found no other missed default or other generic accounts.</p> <p>The cause of Instance 1 was inadequate training. While the Entity’s procedure states that the accounts at issue need to be listed on the account inventory list, the quality of the training on the procedure was inadequate and these accounts were missed during documentation checks.</p> <p>In Instance 2, on [REDACTED], SERC Audit reported that since July 1, 2016, the Entity’s Systems Security Management Program referenced a procedure for system operator password changes; however, this referenced procedure did not exist.</p> <p>The Entity determined that the cause of Instance 2 was management oversight. The Entity had the automation for the password change every 15 months for support personnel and had a procedure stating that it needed to be done; however, for the system operators, the Entity did not have the associated procedure referenced in the Systems Security Management Program. Entity management changed in 2016 and new management was unaware that this additional procedure for system operator password changes was required.</p> <p>These instances of noncompliance began on July 1, 2016, the implementation date of NERC CIP Version 5, and ended on June 30, 2018, when the Entity updated its default account list and updated its Security Management Program to state that the Entity relies on automation to force system operator password changes.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The Entity’s failure to document all of its default or other generic accounts and its failure to have a procedure for system operator password changes at its [REDACTED] could enable a person with bad intentions to gain access to the BPS through unknown or unchanged password accounts. However, the Entity was otherwise properly protecting the accounts, the devices were behind a firewall that logged and monitored, the devices were secured within a physical security perimeter. Additionally, only users with valid credentials could access the devices. Furthermore, while the Entity only had a partial procedure for its system operators, it had a complete procedure for its support personnel. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the “Default and Generic Account” list, which was uploaded to SERC’s CIP-Up site; 2) updated the CIP-007 compliance procedure to provide better clarity regarding identifying and inventorying default accounts, deleting the reference to the missing procedure, and referencing that the Entity relies on automation to force password changes for system operators; and 3) trained SCADA IT Team on the updated procedure and uploaded the training roster to SERC’s CIP-Up site. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019987	CIP-004-6	R5, P5.1	[REDACTED]	[REDACTED]	07/01/2018	07/02/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 11, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5, P5.1. The Entity did not initiate removal of a retiring employee’s unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action.</p> <p>On July 2, 2018, an Entity support employee with knowledge of this particular employee’s retirement, which was effective on June 30, 2018, at 11:59 p.m., discovered that the Entity had not completed a work order to remove access permissions within 24-hours of the effective date of retirement. On July 2, 2018, while waiting for the work order to be submitted, the support employee removed the IRA to the Electronic Access Control or Monitoring System (EACMS) at 8:38 a.m., and removed physical access to the medium impact facilities at 10:40 a.m. Also, on July 2, 2019, at 10:52 a.m., the work order to revoke the access came through the system.</p> <p>The Entity conducted its extent-of-condition assessment by examining all revocations that occurred between January 1, 2017 and June 27, 2018. The Entity compared the revocation service request tickets to the actual time stamps within the systems to determine if any revocations exceeded the 24-hours permitted. No additional instances were discovered.</p> <p>The scope of affected facilities in this instance of noncompliance included [REDACTED]</p> <p>This noncompliance started on July 1, 2018 at 12:00 a.m., when the Entity failed to remove unescorted physical access and IRA from the employee within 24 hours of the employee’s effective date of retirement, and ended on July 2, 2018, at 10:40 a.m., when the Entity removed unescorted physical access and IRA for the retired employee.</p> <p>The causes of this noncompliance were a deficient process for the revocation of logical access and a deficient internal controls to ensure that the revocation of logical access process was implemented correctly. The physical access process did not clearly define the “effective date” of a termination action. Additionally, the tool (the internal control) used to initiate the access revocation by Human Resources (HR) was a corporate-wide tool without obvious indicators and time constraints required for NERC CIP access revocations. Due to this, employees who were monitoring the reports and tasked with the actual revocations in the appropriate applications failed to place the proper emphasis on the NERC CIP revocation.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity’s failure to revoke all unescorted physical access and IRA upon a termination action could have allowed a malicious actor to gain access to the PSPs and degrade BCA or BCS functionality. However, the employee at issue was a retiree in good standing with the Entity, who was current with existing cyber security training and had a valid Personnel Risk Assessment on file. Additionally, the retired employee’s electronic access was limited to “view only” access to the EACMS Cyber Assets. The Entity reviewed all access by the retired employee, and found that the last physical access occurred on June 12, 2018, and the last login to the system occurred on June 12, 2018, both well prior to the employee’s official retirement date. Furthermore, no use of the involved credentials occurred after the retirement date, and the revocation of both the physical and electronic access occurred only 10 hours and 41 minutes late. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the Physical Access Control Guidelines to include language to define the “effective date” of the termination action as the latter of the email notification date or midnight of the effective date included in the notification email, and to verify that the notification system had all critical parties in the email notification list; 2) added NERC CIP and NERC Non-CIP box in the notification system, which is updated by NERC Compliance as employees are on boarded and changes occur; 3) implemented verbal confirmation process from HR to NERC Compliance (NERC Compliance began tracking completion of access revocation from this point); 4) updated workflow ticket with immediate processing flag and ability to insert an effective date; 5) conducted training for the appropriate groups to review the updated process and expectations of each department; and 6) created an annual training notification to the review process in later years. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018020307	CIP-010-2	R1: P1.1	[REDACTED]	[REDACTED]	07/01/2016	08/30/2018	Compliance Audit	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>During a Compliance Audit conducted from [REDACTED], SERC determined that the Entity, as a [REDACTED], was in noncompliance with CIP-010-2 R1, P1.1. The Entity failed to include enabled logical network accessible ports in its baseline configurations for [REDACTED].</p> <p>During the Audit, SERC reviewed the Entity’s 2017 Cyber Vulnerability Assessment (CVA) and found that it identified [REDACTED] that had logical network access ports not listed in the Entity’s baseline documentation. Prior to the Audit, on May 9, 2017, the Entity was made aware of the CVA’s findings and determined that a port for the [REDACTED] was misspelled in the original baseline documentation. On June 6, 2017, the Entity updated the baseline configurations with the corrected port name. Additionally, in February 2017, a port for [REDACTED] was inadvertently enabled as part of a default manufacturer clustering setting after an operating system update. On May 17, 2017, the Entity disabled the [REDACTED]’ default clustering setting and closed the port.</p> <p>On August 31, 2018, the Entity submitted a Self-Report stating that it was in noncompliance with CIP-010-2 R1, P1.1. The Entity failed to document logical network accessible ports in its baseline configurations for [REDACTED]. SERC determined that the instances in this Self-Report involved the same Standard and Requirement as the instances found in the Audit. Therefore, SERC dismissed and consolidated [REDACTED].</p> <p>On August 29, 2018, the Entity reviewed its 2018 CVA and discovered that a port on [REDACTED] was not included in the baseline configurations. The Entity determined that while preparing for the CIP-005 transition in June 2016, it updated the baseline configurations to include this port; however, after the change was made, the [REDACTED] were not immediately rebooted. Shortly thereafter, the Entity applied a firmware update and rebooted all [REDACTED]. The failure to reboot the [REDACTED] prior to applying the firmware update resulted in the baseline reverting back to the previous configuration.</p> <p>The 2018 CVA also identified [REDACTED] had an open port that was not listed on the baseline. On February 26, 2018, the Entity upgraded security patches on its Cyber Assets. When the security patches were applied it caused a port to unknowingly open on [REDACTED]. Thus, the baseline documentation did not contain the newly opened port.</p> <p>For its extent-of-condition, the Entity reviewed open port evidence along with baseline documentation for all Cyber Assets, and found no additional instances of noncompliance.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on August 30, 2018, when the Entity updated the baseline configurations with the logical network accessible ports.</p> <p>This cause of this noncompliance was management oversight. Management failed to ensure that its change management process clearly defined that all devices with logical network access ports be evaluated for potential security control impacts and changes to the baselines. Here, the Entity used an automated change management program to detect changes to ports during the change management process; however, only certain cyber assets were configured for this automated detection. Thus, the extent of the evaluation being performed and baselines being updated under the process were limited to only those devices that had automated port verifications, and did not include any cyber asset that required a manual review of changes to its ports. In all instances above, the affected cyber assets required a manual review of its ports.</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Having unknown open ports could allow malicious actors to deliver malware payloads, gather intelligence, or extract data, which could potentially lead to adverse effects to the reliability of the BPS. However, this risk is reduced because the cyber assets resided within a protected network with multiple layers of security. No harm is known to have occurred.</p> <p>SERC determined that the Entity’s compliance history should not serve as a basis for applying a penalty because the root causes between the prior and instant noncompliances are different, and the prior mitigation plans would not have prevented these instances of noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) disabled the service which required the undocumented port on the [REDACTED]; 2) updated the baseline for all [REDACTED]; 3) disabled the clustering setting and closed the port on the [REDACTED]; 4) modified the change management process to include a manual review of open ports on all cyber assets without automated port detection for every known change to those assets; and 5) provided training to appropriate personnel regarding the updated 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
SERC2018019711	CIP-010-2	R1: P1.2	[REDACTED]	[REDACTED]	03/14/2018	07/18/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On May 14, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1, P1.2. The Entity did not authorize and document changes when installing a firmware upgrade that deviated from the existing baseline configuration.</p> <p>In Instance 1, on March 14, 2018, the Entity’s [REDACTED] installed an upgrade to [REDACTED] medium impact Bulk Electric System (BES) Cyber Asset (BCA) relay firmware without first getting authorization through its change control process. On May 30, 2017, the [REDACTED] group sent an email request to the [REDACTED] to upgrade the relay firmware, but failed to submit a formal change request, as required by the change control process. Because a change request was never submitted, the relay firmware upgrade was never approved. Prior to installing the upgrade, the [REDACTED] did not realize that the [REDACTED] did not submit a change request.</p> <p>On March 26, 2018, while testing out a new internal control, the Entity’s [REDACTED] discovered that the [REDACTED], in reliance of the May 30, 2017, [REDACTED] group’s email, installed the upgrade to the BCA relay firmware. That same day, the [REDACTED] retroactively followed its change control process, by submitting a change request, and receiving the required approval in order to mitigate the finding.</p> <p>For its extent-of-condition (EOC), the Entity reviewed all of its relay firmware information and compared it to the baseline. The Entity completed the EOC on August 1, 2018, and found no other baseline mismatches.</p> <p>The cause of Instance 1 was management oversight for failing to implement an internal control to ensure adherence to the process. The Entity lacked an internal control to require personnel to verify that a request change was made prior to applying firmware changes. Instance 1 was also a result of inadequate training. The Entity had a sufficient procedure in place, but the new personnel requesting the upgrade were not aware that requests for upgrades to relay firmware was required to follow the change control process. The [REDACTED] failure to follow the process caused a miscommunication with the [REDACTED], which caused the [REDACTED] to mistakenly believe the [REDACTED] submitted a change request under the established process.</p> <p>This instance started on March 14, 2018, when the Entity implemented the firmware upgrade without authorization, and ended on March 26, 2018, when the Entity obtained authorization of the upgrade.</p> <p>Additionally, on August 21, 2019, the Entity submitted a Self-Report stating that it was in noncompliance with CIP-010-2 R1, P1.2. The Entity discovered that it did not authorize and document changes when applying security patches that deviated from the existing baseline configuration. SERC determined that this noncompliance involved the same Standard and Requirement as NERC Violation ID [REDACTED]. Therefore, SERC dismissed and consolidated [REDACTED].</p> <p>In Instance 2, on July 17, 2019, the Entity’s [REDACTED] technicians’ [REDACTED] automatically deployed July’s monthly Microsoft security patches to [REDACTED] high impact Protected Cyber Assets (PCAs) prior to receiving formal authorization from the asset business owner, [REDACTED]. [REDACTED] was in the process of evaluating the security patches when [REDACTED] automatically deployed the security patches. Within hours of the automatic deployment, the [REDACTED] technician realized the mistake and stopped the deployment from progressing throughout the BES Cyber System (BCS). The [REDACTED] technician attempted to uninstall the July 2019 Microsoft security patches that were applied to the three PCAs, however, the patches were unable to be removed. One day later, [REDACTED] approved the security patches for installation, and the security patches were re-applied through the BCS. The Entity’s impacted systems comprised [REDACTED] high impact BCSs.</p> <p>On July 17, 2019, the Entity conducted an EOC by using its [REDACTED] to analyze the CIP environment and found no additional patches were applied prior to approval.</p> <p>The cause of Instance 2 was management oversight for failing to implement an internal control to ensure adherence to the process. The Entity’s process did not require [REDACTED] to confirm the approval status of the patches before they were deployed.</p> <p>This instance started on July 17, 2019, when the Entity implemented the security patches without authorization, and ended on July 18, 2019, when the Entity obtained authorization and applied the security patches.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Specifically, the Entity’s failure to assess and approve both relay firmware upgrades prior to upgrading its firmware and Microsoft patches to its BCS could have negatively affected the reliability of those systems or introduced vulnerabilities into those systems, thereby creating a risk to the BPS. However, in these instances the Entity previously approved and applied the relay firmware and Microsoft patches to its assets in other locations, including its corporate environment and energy management system (EMS) test environment, without any issues. With respect to the relay firmware, the vendor did not release any security vulnerabilities for either the old or</p>					

	<p>new firmware, and the update only related to protective elements in the relay and was not security related. With respect to the Microsoft security patches, the Entity’s automated detective internal control would have detected the unauthorized patches the next day and appropriate personnel would have been notified. No harm is known to have occurred.</p> <p>SERC determined that the Entity’s compliance history should not serve as a basis for applying a penalty. The Entity’s relevant prior noncompliance with CIP-010-2 R1, P1.2 includes NERC Violation ID [REDACTED]. While the underlying cause of the two noncompliances are arguably similar, the prior mitigation plan only required training of the change control process for [REDACTED] administrative personnel and not the relay groups. Therefore, the mitigation plan for the prior noncompliance would not have prevented this instance of noncompliance. Additionally, this instance of noncompliance continues to qualify for compliance exception treatment as it only posed a minimal risk and is not indicative of a systemic or programmatic issue. Further, the Entity quickly detected the current instances of noncompliance through its internal controls, which resulted in a short duration of 12 days for Instance 1 and one day for Instance 2.</p>
<p>Mitigation</p>	<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) created and received authorization for a change request to install the BCA relay firmware (Instance 1); 2) performed a manual review of all CIP V5 medium impact relay firmware to ensure that all changes were approved (Instance 1); 3) created a new notification in its application to test relays during changes, which prompts the user to consider if a proper change request with authorization was made, and acknowledge the notification before proceeding with the change (Instance 1); 4) required all personnel in the relay groups to take a mandatory CIP-010 training module, which covered the Entity’s internal change management tool and process (Instance 1); 5) enhanced its automated voice recognition system for entry into substations to include a reminder that if a change to a CIP asset is the reason for the visit, a change request ticket must be submitted and approved (Instance 1); 6) enhanced its internal control to include rescheduling of the automatic deployment of approved patches from Wednesday to Thursday, so that [REDACTED] weekly [REDACTED] occurs prior to the patches being installed in non-[REDACTED] environments (Instance 2); 7) enhanced its process to require [REDACTED] personnel to verify the approval status before pushing any patches to the EMS environment (Instance 2); and 8) distributed a training reminder email to the supervisors o [REDACTED] personnel, which provided instructions on how to create a ‘change event’ for other areas outside of [REDACTED] and to coordinate with personnel in the impacted area prior to making the change (Instance 2).

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018020313	CIP-007-6	R4, P4.4	[REDACTED]	[REDACTED]	09/07/2017	10/09/2017	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], SERC determined that the Entity, as a [REDACTED], was in noncompliance with CIP-007-6 R4, P4.4. The Entity had two instances where it failed to perform the required 15 calendar day review of a summarization or sampling of logged events to identify undetected Cyber Security Incidents.</p> <p>In Instance 1, on August 22, 2017, the Entity conducted a review of logged events. The next review was required within 15 calendar days, or no later than September 6, 2017. On September 8, 2017, the Entity conducted the review of logged events two days late.</p> <p>In Instance 2, on September 22, 2017, the Entity conducted a review of logged events. The next review was required within 15 calendar days, or no later than October 7, 2017. On October 9, 2017, the Entity conducted the review of logged events two days late.</p> <p>On October 13, 2018, the Entity [REDACTED] conducted an extent-of-condition (EOC) assessment that included an additional review of all log review tickets that had been scheduled to perform log review since July 1, 2016, the effective date of CIP Version 5. The Entity identified no additional instances of noncompliance with CIP-007-6 R4, P4.4.</p> <p>The scope of this noncompliance included [REDACTED].</p> <p>This noncompliance started on September 7, 2017, when the Entity was required to conduct the log review for Instance 1, and ended on October 9, 2017, when the Entity conducted a log review for Instance 2.</p> <p>The cause of this noncompliance was determined to be management oversight for failing to implement an adequate internal control, such as implementing alerts for incomplete log review prior to the 15 calendar day timeframe.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity’s failure to review the logged security events within the required 15 calendar days, could create potential for a malicious event to go undetected. During such period, malicious actors could have delivered malware payloads or conducted intelligence and/or data exfiltration. However, the Entity protected the CIP Cyber Assets affected by the oversight with several layers of cyber defense, including placement within Electronic Security Perimeters behind firewalls. The Entity also restricted physical access by placing the Cyber Assets within Physical Security Perimeters. Additionally, the Entity utilized password controls and patch management, and Interactive Remote Access with Cyber Assets required use of [REDACTED] and two-factor authentication. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) performed an EOC assessment by reviewing all the log review tickets that had previously been scheduled to perform log review since the effective date of CIP Version 5; 2) held a meeting with [REDACTED] to review the transition plan to move the review of logs to the [REDACTED]; 3) created a change alert to notify the [REDACTED] and/or [REDACTED] if a log review change incident is not completed from the prior day; 4) updated the procedure to add the new [REDACTED] role and relevant steps; and 5) created an internal process to ensure a daily review of logged security events is performed and trained the [REDACTED] personnel on the 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
SERC2018019960	CIP-010-2	R1 P1.1	[REDACTED]	[REDACTED]	07/01/2016	06/27/2018	Self-Report	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>	<p>On June 28, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1, P1.1. The Entity failed to include the correct firmware version number for [REDACTED] of its BES Cyber Assets (BCAs) in its baseline configurations.</p> <p>On April 5, 2016, when version 3 of the CIP standards was still in effect, the Entity performed a firmware upgrade on [REDACTED]. None of the Cyber Assets at the substation were identified as Critical Cyber Assets under version 3 of the CIP standards, therefore, the Cyber Assets receiving the upgrade were not required to have a documented baseline configuration, nor follow a configuration management process. The Entity’s personnel did not notify the individual responsible for maintaining inventory records that the firmware upgrade had taken place.</p> <p>When version 5 of the CIP standards took effect on July 1, 2016, the Cyber Assets at the [REDACTED] and were required to have a documented baseline configuration in accordance with CIP-010-2 R1, P1.1. The Entity used a manual process to establish and document baseline configurations for its medium-impact BCS. The manual process utilized information from the aforementioned inventory records, which had not been updated to reflect the firmware upgrade, to build the newly required baseline configuration documentation. The Entity did not discover the incorrect firmware version number recorded in the baseline for the [REDACTED] Cyber Assets until April 4, 2018, when the Entity conducted a forensic analysis for an unrelated noncompliance. The Entity updated the baseline configuration to include the correct firmware version for the [REDACTED] BCAs on June 27, 2018.</p> <p>For the extent-of-condition, the Entity’s NERC Compliance Group identified the business units that have compliance responsibilities under CIP-010-2 R1, which included [REDACTED]. The groups were asked to review their most recent Cyber Vulnerability Assessment results for any baseline discrepancies. No additional discrepancies were found.</p> <p>The scope of affected assets consisted of [REDACTED].</p> <p>This noncompliance started on July 1, 2016, when the standard became effective, and ended on June 27, 2018, when the Entity updated the baseline configurations to include the correct version number of the affected firmware for the [REDACTED] BCAs.</p> <p>The cause of this noncompliance was ineffective project management. Management did not anticipate the transitional activities that were going to be required when CIP Version 5 took effect and failed to have a change management process in place to require a documented baseline configuration when an upgrade occurred.</p>							
<p>Risk Assessment</p>	<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failing to document the correct firmware version number in the baseline configuration could lead to installation of the wrong version in the event that a Cyber Asset needed to be rebuilt from scratch, or could lead to applicable cyber security patches being missed. However, as part of its patching program, the Entity monitored for security updates pertaining to firmware versions running from the version incorrectly listed in the baseline documentation through the latest available version. No security updates were released for any of these versions during the time period at issue. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>							
<p>Mitigation</p>	<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the baseline configurations to include the correct firmware version for the [REDACTED] BCAs; 2) held training meetings to reinforce the importance of the documented Change Management Process; and 3) completed an extent-of-condition assessment that confirmed no additional Cyber Assets were affected. 							

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019021397	CIP-010-2	R2	[REDACTED] (the "Entity")	[REDACTED]	02/22/2019	03/06/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 17, 2019, the Entity submitted a Self-Report to Texas RE under an existing multi-region registered entity agreement stating that, as a [REDACTED] it was in noncompliance with CIP-010-2 R2. Specifically, a baseline comparison was due on February 21, 2019, but was not timely run, exceeding the thirty-five (35) day requirement of CIP-010-2 R2.</p> <p>The root cause of the noncompliance was a lack of adequate testing prior to a PACS upgrade.</p> <p>This noncompliance started on February 22, 2019, the 36th day after the last baseline was run, and ended on March 6, 2019, the date that evidence that the baselines were completed was created.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). A failure to monitor for baseline changes can result in unauthorized changes going undetected. Unauthorized changes may be of a malicious nature, such as the installation of unauthorized software or the enabling of network accessible ports to facilitate communication with an outside source. These changes can be used to take control of Facilities capable of affecting the BPS, attack other systems required for the reliable operation of the BPS, or to exfiltrate data that can be used to plan more in-depth attacks. The Entity has a [REDACTED].</p> <p>However, the risk of these noncompliances was reduced by the following factors. To begin, the duration of the noncompliance was relatively short, at 12 days. Additionally, there were other safeguards in place to protect the system from unauthorized changes during that time, including use of a software for monitoring for patches and software changes in the protection system, system protection through whitelisting software, and limited access to the system both physically and electronically. Furthermore, only the PACS and EACMS were affected, and the only changes that the new baseline report identified were (1) updated patches that are approved as part of the Entity's patching program and (2) non-substantive changes in ephemeral ports that programs use when they listen on a random port. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) ended the noncompliance by running the baseline; 2) prevented reoccurrence by resolving the UAC settings issue caused by the upgrade; and 3) prevented reoccurrence by adding a control to run a baseline prior to applicable changes to help ensure compliance with the reoccurring 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
TRE2020022807	CIP-006-6	R2	████████████████████ (the "Entity")	██████	10/31/2019	10/31/2019	Self-Log	10/31/2020
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 21, 2020, the Entity submitted a Self-Log stating that, as a ████████████████████ it was in noncompliance with CIP-006-6 R2. Specifically, the Entity did not log an escorted visitor's entry and exit from a Physical Security Perimeter (PSP). The Entity identified this issue through a daily review of badge access.</p> <p>On October 31, 2019, an individual with authorized access to the PSP provided continuous escort to a visitor but did not log the visitor entry and exit from the PSP.</p> <p>The root cause of the noncompliance is insufficient training of staff regarding CIP-006-6 R2 protocols.</p> <p>This noncompliance started on October 31, 2019, when a visitor was granted access to a PSP without a visitor entry log being created, and ended on October 31, 2019, when a visitor exited the PSP without a visitor exit log being created.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system due to several factors. First, the duration of the issue was limited to one day, one individual, and one instance. Second, the visitor that was not logged was escorted throughout their stay in the PSP. Third, the issue was a documentation issue. Fourth, the issue was discovered shortly after occurrence using effective detective controls. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity will complete the following mitigation activities by October 31, 2020:</p> <ol style="list-style-type: none"> 1) counsel individuals involved with noncompliance and require the escorter and visitor to take the Entity's NERC Cyber Security Training; and 2) develop formalized and repeatable training regarding the Entity's physical security, which will include explicit escorting instructions. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019020892	CIP-002-5.1	R1	██████████ ("the Entity")	██████████	07/01/2016	11/27/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 21, 2018, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-002-5.1a, R1. Specifically, the Entity did not implement a process to identify whether it owned assets listed in CIP-002-5.1, R1.1-3.</p> <p>The Entity failed to have a process in place to evaluate whether or not it had any of the assets listed under CIP-002-5.1 R1.</p> <p>This noncompliance started on July 1, 2016, when the standard became effective, and ended on November 27, 2018, when the Entity determined that it had no assets that contain high, medium, or low impact BES Cyber Systems (BCS) under CIP-002-5.1a, R1.3.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The failure to properly identify and classify a BCS increases the potential that the BCS will not receive the appropriate cyber security protections. However, the risk was mitigated by the following factors: The Entity has ██████████. The Entity ██████████. The Entity ██████████. Upon discovering that this standard did apply to the Entity, the Entity's required review of its assets revealed that it had no assets that were identified under CIP-002-5.1a, R1. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) determined that it owned no assets identified under CIP-002-5.1a, R1; 2) formally adopted a process to consider, at least every 15 months, Entity-owned assets as directed by CIP-002-5.1a R1; and 3) formally adopted a process to annually review all NERC reliability standards to determine which standards are applicable to the Entity and assess the risk posed to the BES related to noncompliance. <p>Texas RE has verified completion of all mitigating activities.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019022651	CIP-003-6	R1	[REDACTED] (the "Entity")	[REDACTED]	08/01/2019	08/26/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 12, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-003-6 R1. In particular, the Entity discovered that CIP Senior Manager approval was not obtained within 15 months for a single internal document as required by NERC Reliability Standard CIP-003-6 R1. The document was previously reviewed and approved on April 19, 2018, but it should have been reviewed and approved again by July 31, 2019, in order to meet the 15 month requirement.</p> <p>The root cause of the noncompliance was that each document comprising the Entity's cyber security policy had a different review and approval timeline that was the responsibility of the individual document owner, making it easier for a noncompliance to occur when one of the document owners did not follow the existing process to complete their review and approval task.</p> <p>This noncompliance started on August 1, 2019, when more than 15 months passed since the last review and approval, and ended on August 26, 2019, when the required document was reviewed and approved.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to obtain the CIP Senior Manager's approval of the Cyber Security Policy document every 15 calendar months could have led to reduced awareness and engagement by senior leadership, leading to diminished focus on compliance by the Entity. However, lessening the risk of this noncompliance is the fact that when the review and approval were complete, there were no changes to policy protections. Additionally, the duration of the noncompliance was relatively short at 25 days. No harm is known to have occurred.</p> <p>Texas RE determined that the Entity's compliance history should not serve as an aggravating factor, as the root cause of the Entity's 2017 noncompliance involving this same standard and requirement was distinguishable.</p>					
Mitigation			<p>The Entity took the following steps:</p> <ol style="list-style-type: none"> 1) To mitigate this noncompliance, the Entity initiated the document review and approval process, and the CIP Senior Manager's approval was obtained. 2) To prevent reoccurrence, the Compliance department will be primarily responsible for monitoring and managing the review of applicable documents and all documents will be reviewed and approved by the CIP Senior Manager in December of each calendar 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
TRE2019022652	CIP-008-5	R3	[REDACTED] (the "Entity")	[REDACTED]	03/16/2018	09/04/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 12, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-008-5 R3. Specifically, the Entity did not update and communicate its Cyber Security Incident response plans within 60 days of changes in personnel. Specifically, an employee left on January 15, 2018, and the plan should have been updated by March 16, 2018. A second employee left on June 15, 2018, and the plan should have been updated by August 14, 2018. However, the plan was not updated until September 4, 2018.</p> <p>The root cause was a failure to follow the existing process of updating individuals named in the plan within the 60 day requirement.</p> <p>This noncompliance started on March 16, 2018, which is 60 days after the first employee left but the plan was not updated, and ended on September 4, 2018, when the plan was updated.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although the two employees should have been removed from the plan, there were several other team members included in the plan with their correct contact information. Additionally, the Entity did have a Cyber Security incident response plan and recovery plan in place, which had both previously been documented and distributed. Finally, there were no cyber security incidents during this time. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>The Entity took the following actions:</p> <ol style="list-style-type: none"> 1) to mitigate this noncompliance, the Entity updated the plan; and 2) to prevent reoccurrence, the entity replaced individual names with position titles. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019021757	CIP-004-6	R5; P5.1	[REDACTED] (the "Entity")	[REDACTED]	05/01/2019	05/06/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On June 26, 2019, the Entity submitted a Self-Log stating that, as [REDACTED] nce with CIP-004-6 R5. Specifically, the Entity terminated an employee with unescorted physical access and interactive remote access on April 30, 2019 and did not revoke that access within 24 hours, as required by Part 5.1. The Entity identified this issue during a compliance spot check on May 6, 2019, at which time it revoked both physical and remote access.</p> <p>The root cause of this issue is a lack of controls on the employee termination process in regards to CIP access. Two failures occurred during this noncompliance. One, the system of record for employment was not updated with the termination until May 2, 2019, already after the 24 hour window. Two, the revocation process wasn't completed by CIP compliance personnel until May 6, 2019.</p> <p>This noncompliance started on May 1, 2019, 24 hours after the employee was terminated and the employee's access had not been revoked, and ended on May 6, 2019, when the access was revoked.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed by this issue is that the terminated employee could have used their continued access for malicious purposes. However, the risk posed by this issue is reduced by several factors. First, there was no actual impact to the BPS because there were no access by the employee after the termination. The Entity checked physical and remote access logs during the time period of the noncompliance and found no access was made by the terminated employee. Second, the instance only lasted five days, at which point it was caught by internal controls. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked the employee's access; 2) trained managers to notify the compliance team upon employee termination, in addition to human resources; and 3) implemented a new daily automated control to cross reference the list of active employees and contractors with the human resources termination report. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019736	CIP-002-5.1a	R2	██████████ ("the Entity")	██████████	09/01/2017	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 violation.)			<p>On May 23, 2018, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-002-5.1a R2. The Entity, failed to have its CIP Senior Manager review and approve its categorization of its BES Cyber Systems within 15 months of its prior assessment.</p> <p>The root cause of the noncompliance was that the Entity failed to follow its existing procedures.</p> <p>This noncompliance started on September 1, 2017, the first calendar month following the expiration of 15 calendar months since the last review, and ended on April 5, 2018, when the Entity updated its BES Cyber Systems Categorization assessment and had that update reviewed and approved by its CIP Senior Manager.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure to review and approve the identified BES Cyber System could have resulted in the mis-categorization of a BES Cyber System and potentially led to ineffective or nonexistent protective measures for the Entity's BES Cyber Assets. However, in this instance, the Entity did not have any newly identified BCS. Additionally, the noncompliance was identified during a self-imposed compliance review. ██████████</p> <p>██████████ No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated its BES Cyber Systems Categorization assessment and had that update reviewed and approved by its CIP Senior Manager; 2) reinforced awareness of NERC Standards and compliance requirements with managers and operations staff; 3) implemented a robust, organized electronic data warehouse to centrally catalog its procedures, compliance evidence, training materials and all other related documentation (including links to the NERC Standards web page); and 4) established a single contact point and calendar to centralize compliance-related communications and scheduling. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019740	CIP-003-6	R3	██████████ (the "Entity")	██████████	09/30/2016	05/17/2018	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 violation.)			<p>On May 23, 2018, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with, CIP-003-6 R3. The Entity failed to identify a CIP Senior Manager by name as of the date of Entity's registration in Texas RE.</p> <p>The root cause of the noncompliance was that the Entity did not follow its existing procedures that detail the applicable requirements.</p> <p>This noncompliance started on September 30, 2016, when the Entity registered as a ██████████ in Texas RE without identifying a CIP Senior Manager, and ended on May 17, 2018, when the Entity documented the CIP Senior Management.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk in not documenting a change to the CIP Senior Manager is that it may result in a lack of guidance or accountability, which can result in an entity not complying with NERC CIP Requirements. However, the noncompliance was identified during a self-imposed compliance review and no harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) executed an attestation detailing the Entity's CIP Senior Manager history; 2) reinforced awareness of NERC Standards and compliance requirements with managers; 3) established a single contact point and calendar to centralize compliance-related communications and scheduling; and 4) implemented a robust, organized electronic data warehouse to centrally catalog its procedures, compliance evidence, training materials and all other related documentation. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019021321	CIP-002-5.1a	R2	██████████ ("the Entity")	██████	08/01/2018	09/10/2018	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 violation.)			<p>On April 5, 2019, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-002-5.1a R2. Specifically, the Entity did not perform the review of the identifications in CIP-002-5.1a R1 and its parts at least once every 15 calendar months.</p> <p>The root cause of this noncompliance was a lack of adequate tracking of necessary tasks, which allowed the noncompliance to occur when there was a change in personnel.</p> <p>This noncompliance started on August 1, 2018, first calendar month after the expiration of 15 calendar months from the last review, and ended on September 10, 2018, when the necessary review was completed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to review, and if necessary, update the identifications could have resulted in the Entity failing to provide the BCAs all required protections under the CIP Standards. However, the threat of the noncompliance is lessened by a couple of factors. To begin, although the Entity did not perform the review within 15 months, upon review there were no changes to the BES Cyber classification. Additionally, the duration of the noncompliance was relatively short. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) performed the necessary review; 2) added an Outlook Calendar Reminder for Plant Engineer & CIP Manager for every 12 Months, rather than every 15 Months; and 3) added NERC CIP Review to Regulation Tracker Checklist for Plant Engineer. <p>Texas RE has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019021322	CIP-003-6	R1	[REDACTED] ("the Entity")	[REDACTED]	07/01/2018	08/31/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 5, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-003-6 R1. Specifically, the Entity failed to have its CIP Senior Manager review and approve its documented cyber security policies at least once every 15 calendar months.</p> <p>The root cause of this noncompliance was a lack of adequate tracking of necessary tasks, which allowed the noncompliance to occur when there was a change in personnel.</p> <p>This noncompliance started on, July 1, 2018, the next month following the expiration of 15 months, and ended on August 31, 2018, when the required review and approval took place.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Such failure could have resulted in distribution of inaccurate guidance or outdated policies. However, the threat of the noncompliance is lessened by a couple of factors. To begin, although the Entity did not perform the review within 15 months, upon review there were no changes to its CIP-003 cyber security policies. Additionally, the duration of the noncompliance was relatively short. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed the necessary review; 2) implemented an Outlook Calendar Reminder for the Plant Engineer & CIP Manager for every 12 months, rather than every 15 months; and 3) added NERC CIP Review to its regulation tracker checklist for its Plant Engineer. <p>Texas RE has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021045	CIP-002-5.1a	R2: P2.1, P2.2	[REDACTED]	[REDACTED]	7/1/2018	2/4/2019	Self-Report	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)</p>			<p>On February 11, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-002-5.1a R2.</p> <p>Specifically, the entity discovered during its Self-Certification that some of the identifications made in its performance of CIP-002-5.1a R1 and its parts, during the required 15 calendar month period from March 2017 to June 2018, were not reviewed at least once every 15 calendar months as required by R2 Part 2.1 and therefore, the entity did not obtain CIP Senior Manager or delegate approval as required by R2 Part 2.2. The identifications that were not reviewed and approved timely included [REDACTED] Medium Impact BES Cyber Systems (MIBCS) located at a [REDACTED].</p> <p>This issue began on July 1, 2018, when the 15-calendar month review should have been completed and ended on February 4, 2019, when the entity reviewed the identifications made pursuant to CIP-002-5.1a R1 and obtained CIP Senior Manager approval of those identifications.</p> <p>The root cause of the issue was attributed to a missing control to ensure compliance. Specifically, the entity had periodic reminders in place for the timely completion of Parts 2.1 and 2.2; however, the reminders only pertained to entity-owned assets and did not include assets that were [REDACTED]. Additionally, the entity’s process did not include steps to address timely completion of compliance task where an inventory review was ongoing at the time the CIP-002-5.1a R2 compliance task was due to be performed.</p>					
<p>Risk Assessment</p>			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to review and obtain CIP Senior Manager approval of the identifications in R1 and its parts at least once every 15 calendar months as required by CIP-002-5.1a Parts 2.1 and 2.2.</p> <p>Failure to review and approve the identified MIBCS could have resulted in the mis-categorization of those systems and potentially led to ineffective or nonexistent protective measures for the same systems. However, as compensation, this issue was related to a small list of [REDACTED] MIBCS of which the entity was in the process of reviewing pursuant to Part 2.1 until it had to reallocate resources to work on another issue, at which time a task reminder to complete the review should have been initiated. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
<p>Mitigation</p>			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) reviewed is identifications made pursuant to CIP-002-5.1a R1, updated its identifications, and obtained CIP Senior Manager approval of those identifications; 2) created a new task notification to include BES Cyber Systems with [REDACTED] to ensure the CIP-002-5.1a R2 task are performed within the required timeframe; and 3) established a rule to review and approve the R1 identifications with the most up-to-date information available at the time review and approval is required to avoid delaying the task due to future inventory planned or in progress. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021327	CIP-011-2	R2: P2.2	[REDACTED]	[REDACTED]	08/17/2016	03/05/2019	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED] WECC determined the entity, as a [REDACTED] had a potential noncompliance of CIP-011-2 R2.</p> <p>Specifically, the entity decommissioned two Protected Cyber Assets (PCAs) associated with a Medium Impact BES Cyber System (MIBCS) that contained BES Cyber System Information (BCSI) but failed to retain records that indicate the data storage media was destroyed prior to disposal of the PCAs. This issue began on August 17, 2016, when the entity failed to retain the disposal documentation for two decommissioned PCAs and ended on March 5, 2019, when the entity documented media sanitization of the two PCAs through an attestation signed by the engineers responsible for the device disposal.</p> <p>The root cause of the issue was attributed to insufficient controls to ensure that the entity documented and retained evidence.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to retain evidence documenting that it had taken action to prevent the unauthorized retrieval of BCSI from two decommissioned PCAs prior to disposal, as required by CIP-011-2 R2 Part 2.2.</p> <p>Failure to prevent the unauthorized retrieval of BCSI from decommissioned PCAs could have resulted in a malicious actor accessing the data and using it to breach the entity's secure infrastructure and potentially gain access to the Electronic Access Control & Monitoring System (EACMS) or Physical Access Control System (PACS) environments. However, although the PCAs had External Routable Connectivity, as compensation, the devices were incapable of any type of control or monitoring and were mainly used for email. Additionally, the entity's [REDACTED] process for disposing of surplus property required sanitization once devices reach the workgroup responsible for technology equipment disposal. This issue was a deficiency in documentation. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) documented media sanitization of the two PCAs through an attestation signed by the engineers responsible for their disposal [REDACTED]; and 2) implemented a process in its automated management tool that ties decommissioning paperwork to the decommissioning change ticket. The change ticket will not close until the paperwork is attached and reviewed for completeness. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021115	CIP-004-6	R3: P3.5	[REDACTED]	[REDACTED]	8/12/2018	1/8/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On February 27, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R3. Specifically, for one employee, the entity did not ensure that a personnel risk assessment (PRA) was completed within the last 7 years prior to expiration of their existing PRA. The employee had authorized unescorted physical access to three Physical Security Perimeters associated with Medium Impact Bulk Electric System (BES) Cyber Systems (MIBCS). In this instance, the entity’s access management tool had a data input error that resulted in inaccurate access history for said employee. Therefore, because the data did not reflect that the employee currently had authorized unescorted physical access, the entity did not initiate its PRA renewal process for this employee. This issue began on August 12, 2018 when the employee’s PRA exceeded the 7-year timeframe and ended on January 8, 2019 when the employee’s access was revoked.</p> <p>The root cause of the issue was attributed to a lack of internal controls. Specifically, the entity had implemented software to track access rights, however, a data input error resulted in inaccurate output from the entity’s access management tool.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented PRA process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a PRA completed within the last seven years as required by CIP-004-6 R3 Part 3.5, for one employee.</p> <p>Failure to renew a PRA could have resulted in the entity failing to detect an employee with a changed, or elevated, risk profile and may have developed the motivation to cause harm to the BES retaining physical access to MIBCS. However, the entity confirmed that the employee did not use their unescorted physical access during the time of the issue. Additionally, the employee did not have electronic access to any BES Cyber Assets. Finally, the employee was in good standing with the entity and did not have derogatory findings in their renewed PRA. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) revoked the employee’s access until a new PRA had been completed; and 2) updated its PRA renewal process to include a review of source data to verify access status of employees due for renewal of their PRA. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021136	CIP-006-6	R2: P2.1	[REDACTED]	[REDACTED]	12/12/2018	12/12/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On February 28, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-006-6 R2. Specifically, two contractors without authorized unescorted physical access were not continuously unescorted for approximately 45 minutes. In this instance, two contractors performed scheduled work on devices located in a Physical Security Perimeter (PSP) associated with High Impact Bulk Electric System (BES) Cyber Systems. The security personnel that escorted the contractors remained at the entrance of the PSP, instead of continuously escorting the contractors inside of the PSP to the worksite while the work was being completed. Two employees saw the security personnel standing at the entrance of the PSP and immediately directed the security personnel to remain directly with the contractors for the duration of their work. This issue began on December 12, 2018, when the guard left the contractors unescorted and ended on December 12, 2018 when the security personnel resumed properly escorting the contractors.</p> <p>The root cause of the issue was attributed to incorrect performance of infrequently performed steps. Specifically, although the security personnel had been trained on how to continuously escort a visitor, they did not frequently serve as an escort and therefore, failed to properly perform their duties.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented visitor control program to require continuous escorted access of visitors within each Physical Security Perimeter as required by CIP-006-6 R2 Part 2.1, for two contractors.</p> <p>Failure to continuously escort visitors could have resulted in individuals accessing, altering, or physically damaging BES Cyber Assets (BCA). However, the contractors had a legitimate business need to enter the PSP. Additionally, the contractors did not have logical access to the BCAs. Finally, the entity reviewed security event logs and did not detect any malicious activity during the relevant period. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) re-established continuous escort of the two contractors; 2) updated the visitor escort policy to exclude security personnel as visitor escorts; 3) distributed awareness communication and visitor escort protocol to relevant employees; 4) updated the visitor check-in procedure for security staff to confirm responsibilities with visitor escorts and include steps for the escort to sign a digital visitor log; 5) created a reference diagram detailing the visitor check-in and escort processes for security personnel; and 6) retrained security personnel on visitor check-in and escort processes. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020810	CIP-007-6	R1: P1.1	[REDACTED]	[REDACTED]	7/31/2018	10/22/2018	Self-Report	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)</p>			<p>On December 13, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] it was in potential noncompliance with CIP-007-6 R1. Specifically, the entity did not enable only logical network accessible ports that determined necessary, on one Physical Access Control Systems (PACS) associated with a High Impact Bulk Electric System (BES) Cyber System at the entity’s primary Control Center. In this instance, the entity had contracted with a known third-party vendor to install a PACS; however, the vendor supplied a new contractor, unfamiliar with the entity’s installation procedures, to install the PACS. The entity did not provide the contractor with documented procedures or work-level instructions prior to installation. This issue began on July 31, 2018, when the PACS were installed and ended on October 22, 2018, when the entity verified that all unnecessary ports had been disabled.</p> <p>The root cause of the issue was attributed to less than adequate process documentation. Specifically, the entity relied solely on internal knowledge during installation of the devices and did not have procedural documentation or work-level instructions to promote secure installation and compliance with the standards.</p>					
<p>Risk Assessment</p>			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to adequately implement its documented process to enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports as required by CIP-007-6 R1 Part 1.1, for one PACS.</p> <p>Failure to disable all unnecessary ports could have resulted in an actor with malicious intent using this access to cause a [REDACTED] thereby, preventing operations personnel from entering the facility. However, the PACS was installed [REDACTED] Additionally, the PACS was [REDACTED] to prevent unauthorized access. No harm is known to have occurred.</p> <p>WECC determined that the entity’s compliance history should not serve as a basis for applying a penalty. Mitigation of the previous noncompliance as documented would not have prevented the current instance.</p>					
<p>Mitigation</p>			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) disabled all unnecessary ports on the affected device; 2) documented and implemented a new commissioning process for this specific Cyber Asset type; and 3) documented and implemented a configuration checklist to clarify details regarding port configuration; and 4) revised the relevant procedural document to provide additional detail regarding port configurations. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020397	CIP-014-2	R3	[REDACTED]	[REDACTED]	12/29/2015	3/22/2016	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED] WECC determined that the entity, as a [REDACTED], was in potential noncompliance with CIP-014-2 R3.</p> <p>Specifically, the entity failed to include the date of completion of its performance of CIP-014-2 R2 when it notified the Transmission Operator (TOP) that had operational control of the primary control center of such identification. This issue began on December 29, 2015, when the notification was sent to the TOP without an R2 completion date and ended on March 22, 2016, when the entity reissued the notification with the physical security plans completion date included.</p> <p>The root cause of the issue was attributed to a lack of internal controls. Specifically, the subject matter expert responsible for performing this task was on vacation and that person’s manager was not aware that an R2 completion date needed to be included in the notification to the TOP.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to include the date of completion of R2 when it notified the TOP that had operational control of the primary control center of such identification as required by CIP-014-2 R3.</p> <p>Such failure could have resulted in the delay of the performance of R5 and R6 by the TOP with operational control of the primary control center; thereby, prolonging the implementation of any physical security controls deemed necessary by the TOP. However, the entity did provide timely notification to the TOP of its actual determination. The issue was limited to an administrative error. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) provided a second notification to the TOP which included the completion date of the performance of R2; and 2) developed a CIP-014-2 R3 template notification letter which includes a line for adding the completion date of R2, to ensure anyone who sends the notification understand what is required. <p>WECC verified completion of mitigating activities.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019679	CIP-014-2	R6: P6.2	[REDACTED]	[REDACTED]	6/29/2016	7/13/2016	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On May 14, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], was in potential noncompliance with CIP-014-2 R6.</p> <p>Specifically, on August 24, 2016, in preparation for a mock audit, the entity performed date calculations to determine if all the actions required by CIP-014-2 had been completed within the required timeframes detailed in R1 through R6. The review of the dates determined that the R6 unaffiliated third-party review of R4 and R5 had been completed more than 90 calendar days after the development of [REDACTED] physical security plans developed in R5, as required by Part 6.2. The entity used the date the request for review was sent to the unaffiliated third party reviewer rather than the date the physical security plans had been completed; thereby, exceeding the “required within 90 calendar days of completion of R5” [REDACTED] for the [REDACTED] physical security plans. This issue began on June 29, 2016, when the unaffiliated third party review should have been completed and ended on July 13, 2016, when the reviews were completed.</p> <p>The root cause of the issue was attributed to a less than adequate process. Specifically, the entity’s informal process did not differentiate between the date the physical security plans were completed and the date they were provided to the unaffiliated third party reviewer when determining the “review within 90 days” timeframe.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to ensure that the unaffiliated third party review of its [REDACTED] physical security plans was completed within 90 calendar days of the completion of those plans, as required by CIP-014-2 R6 Part 6.2.</p> <p>Such failure could have resulted in the delay of the entity assessing the review of its [REDACTED] physical security plans by the unaffiliated third party which could have led to the entity not addressing recommendations resulting from that review and therefore the risk timely. However, the duration of the issue was limited to [REDACTED] days and the unaffiliated third party made no recommendations from its review of the [REDACTED] physical security plans. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has completed:</p> <ol style="list-style-type: none"> 1) developed a calculation check tool for calculating due dates based on the entry of a start date that is both backward and forward looking; and 2) provided training on the calculation check tool to applicable personnel. <p>WECC verified completion of mitigating activities.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018615	CIP-014-2	R6	[REDACTED]	[REDACTED]	7/4/2016	7/14/2016	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On November 9, 2017, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-014-2 R6.</p> <p>Specifically, in preparation for a mock audit, the entity performed date calculations to determine if all the actions required by CIP-014-2 had been completed within the required timeframes detailed in R1 through R6. The review of the dates determined that the R6 unaffiliated third-party review of R4 and R5 had been completed more than 90 calendar days after the development of [REDACTED] physical security plans developed in R5, as required by Part 6.2. The entity used the date the request for review was sent to the unaffiliated third party reviewer rather than the date the physical security plans had been completed; thereby, exceeding the “required within 90 calendar days of completion of R5” for the [REDACTED] physical security plans. This issue began on July 4, 2016, when the unaffiliated third party review should have been completed and ended on July 14, 2016, when the reviews were completed.</p> <p>The root cause of the issue was attributed to a less than adequate process. Specifically, the entity’s informal process did not differentiate between the date the physical security plans were completed and the date they were provided to the unaffiliated third party reviewer when determining the “review within 90 days” timeframe.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to ensure that the unaffiliated third party review of its [REDACTED] physical security plans was completed within 90 calendar days of the completion of those plans, as required by CIP-014-2 R6 Part 6.2.</p> <p>Such failure resulted in the delay of the entity assessing the review of its [REDACTED] physical security plans by the unaffiliated third party which could have led to the entity not addressing recommendations resulting from that review and therefore the risk timely. However, the duration of the issue was limited to [REDACTED] days and the unaffiliated third party made no recommendations from its review of the [REDACTED] physical security plans. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) developed a calculation check tool for calculating due dates based on the entry of a start date that is both backward and forward looking; and 2) provided training on the calculation check tool to applicable personnel. 					

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	MRO2019022428	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
2	MRO2018019616			Yes	Yes									Category 2 – 12: 2 years
3	MRO2019021270			Yes	Yes									Category 2 – 12: 2 years
4	MRO2019021447			Yes	Yes									Category 2 – 12: 2 years
5	MRO2019022029			Yes	Yes					Yes				Category 2 – 12: 2 years
6	MRO2019022030			Yes	Yes				Yes	Yes				Category 2 – 12: 2 years
7	MRO2019022031	Yes		Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 years
8	MRO2019022037			Yes	Yes					Yes			Yes	Category 2 – 12: 2 years
9	MRO2019022378	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
10	MRO2018020763	Yes	Yes	Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 years
11	MRO2018020764			Yes	Yes						Yes			Category 2 – 12: 2 years
12	NPCC2018019131	Yes		Yes	Yes									Category 1: 3 years Categories 3 – 4: 2 years
13	NPCC2019022244	Yes		Yes	Yes									Category 1: 3 years Categories 3 – 4: 2 years
14	NPCC2018019109	Yes		Yes	Yes									Category 1: 3 years Categories 3 – 4: 2 years
15	NPCC2018019265			Yes	Yes									Categories 3 – 4: 2 years
16	RFC2019021141	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
17	RFC2019021140	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
18	RFC2019021145	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
19	RFC2019021236	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
20	RFC2019021142	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)
21	RFC2019021827	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
22	RFC2019021308			Yes	Yes									Category 2 – 12: 2 years
23	RFC2019021309			Yes	Yes									Category 2 – 12: 2 years
24	RFC2019020929	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 years
25	RFC2019020928	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 years
26	RFC2019021144	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
27	RFC2019021143	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
28	RFC2019022536	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
29	RFC2019022537	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
30	RFC2019022538	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 years
31	SERC2018020796			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
32	SERC2019022268			Yes	Yes									Category 2 – 12: 2 year
33	TRE2019022217	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
34	WECC2020022797			Yes	Yes									Category 2 – 12: 2 year
35	WECC2018020231			Yes	Yes					Yes	Yes			Category 2 – 12: 2 years
36	WECC2018020232			Yes	Yes					Yes	Yes			Category 2 – 12: 2 years
37	WECC2019021588			Yes	Yes					Yes				Category 2 – 12: 2 years
38	WECC2018020164			Yes	Yes					Yes				Category 2 – 12: 2 years
39	WECC2018020396			Yes	Yes				Yes		Yes			Category 2 – 12: 2 years
40	WECC2019020954			Yes	Yes				Yes					Category 2 – 12: 2 years
41	WECC2019020953			Yes	Yes				Yes					Category 2 – 12: 2 year

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022428	CIP-004-6	R2	[REDACTED] (the Entity)	[REDACTED]	06/01/2019	06/04/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R2.</p> <p>The Entity reported that on June 1, 2019, it reactivated a contract individual's electronic access account. The account user was a member of a user group that had access to an Electronic Access Control and Monitoring System (EACMS) device associated with a medium impact BES Cyber System (BCS), resulting in the Entity inadvertently granting access to the device. However, the time since the individual's previous NERC CIP training had exceeded the 15-month interval therefore, the individual was no longer current on their training as required by CIP-004-6 R2.</p> <p>The cause of the noncompliance was the Entity failed to follow its process for account reactivation, which required the removal of the account from all Active Directory user groups.</p> <p>The noncompliance began on June 1, 2019, when the individual was granted access, and ended on June 4, 2019, when the access was revoked (user removed from user group).</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the issue was discovered by an internal control which reports individuals with electronic access to applicable systems that have expiring or expired training. This control limited the duration to four days and it was limited to a single individual and a single EACMS device associated with a medium impact BCS. Additionally, the individual of issue was still employed by the contractor, had a current personnel risk assessment, and had previously received the required CIP training. Lastly, the electronic access granted was not utilized by the impacted individual. No harm was known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) removed the individual's access to the Cyber Asset by removing the user from the user group providing access; 2) enhanced its account reactivation task to more explicitly remind the responsible team to delete non-default user group membership prior to reactivating a user; and 3) implemented a new, ongoing process to delete user accounts [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
MRO2018019616	CIP-002-5.1	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	07/20/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 1, 2017, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-002-5.1, R1.</p> <p>The Entity discovered that it failed to identify a substation as an asset containing a low impact BES Cyber System (BCS). After the initial discovery, further reviews by the Entity revealed six additional assets containing low impact BCS which had not been identified as required by Part 1.3.</p> <p>The cause of the noncompliance was that Entity's process failed to consider assets owned by other entities when identifying assets containing its low impact BCS.</p> <p>The noncompliance began on July 1, 2016, when the Standard and Requirement went into effect, and ended on July 20, 2018, when the additional assets containing low impact BCS were identified.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because all affected Cyber Systems (BCS) were low impact. Other than the CIP-002-5.1 requirement to identify assets containing low impact BCS, a control which is documentation in nature, there were no other controls for low impact BCS in effect until April 1, 2017, which was nine months after this noncompliance started. The controls that did become effective on April 1, 2017, was for CIP-003-6 R2, Attachment 1 Sections 1 and 4, Cyber Security Awareness and Cyber Security Incident Response, are non-technical in nature so their absence did not represent any increased exposure to cyber security threats. Additionally, the number of assets not identified was limited to seven. No harm is known to have occurred.</p> <p>MRO reviewed the Entity's compliance history and determined that it should not serve as a basis for applying a penalty.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) performed an extent of condition review to determine if any other instances of missed assets to which none were found; 2) added missing assets to its documented list; and 3) created and enacted a new BES Asset List, including the consideration of any assets that are third-party owned and directly connected to its system. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021270	CIP-005-5	R1	[REDACTED] (the Entity)	[REDACTED]	09/16/2018	09/19/2018	Self-Log	5/31/2020 Expected Date
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 10, 2019, the Entity submitted a Self-Log stating that as a [REDACTED], it was in noncompliance with CIP-005-5 R1.</p> <p>The Entity received an alert, from its Security Information and Event Management (SIEM) system, that allowed the Entity to determine that a hard drive had failed on its Network Intrusion Detection System (NIDS) (Cyber Asset). This Cyber Asset is used for detecting known or suspected malicious communications for both inbound and outbound communications at its primary high impact Control Center as required by Requirement Part 1.5.</p> <p>The cause of the noncompliance was that the Entity lacked a process for assuring continuity of its ability to detect known or suspected malicious communications for both inbound and outbound communications in the event of a failure of a hard drive on the NIDS Cyber Asset.</p> <p>The noncompliance began on September 16, 2018, when the hard drive on the NIDS failed, and ended on September 19, 2018, when a replacement NIDS was put into service.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because by configuring its SIEM to perform an automated internal detective control, the loss of the Entity's NIDS was detected and alerted within 24 hours of occurrence and the total duration of the issue was limited to four days. Additionally, the requirement to have at least one method for detecting known or suspected malicious communications for both inbound and outbound communications is one of two mandated security measures for protecting the Electronic Security Perimeter (ESP). Therefore, for the duration of the noncompliance, the Entity had an active security measure, which was protecting the ESP, namely the Entity's mechanism for limiting inbound and outbound access through the Electronic Access Point to that which is explicitly granted, with all other access denied by default. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) replaced the failed NIDS; and 2) approved purchase request for new Cyber Asset <p>To mitigate this noncompliance, the Entity will complete the following mitigation activities by May 31, 2020:</p> <ol style="list-style-type: none"> 1) will commission new Cyber Asset as an additional NIDS, establishing redundancy. <p>The expected date of completion takes into account the time between the purchase request approval and the procurement time, shipping/receiving of the new hardware, configuring and testing of the hardware, and scheduling a go-live date that is compatible with other anticipated system activities.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021447	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	07/18/2018	12/06/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. This Self-Log included three instances of noncompliance for changes that deviate from the existing baseline configurations; it failed to update the baseline configuration as necessary within 30 calendar days of completing the change as required by Part 1.</p> <p>In the first instance of noncompliance, the Entity discovered on October 29, 2018, while performing an informal review of baselines, it discovered that changes that deviated from the existing baseline configuration for four high impact Physical Access Control Systems (PACS) had not been updated within 30 days of the most recent change per Part 1.3. The cause of the noncompliance was that the Entity's baseline review process lacked sufficient detail on documenting and tracking the action items for managing any findings from the baseline review. The noncompliance began on October 11, 2018, which was the 31st day after the most recent update, and it ended on October 29, 2018, when the baseline changes were approved for the affected PACS.</p> <p>In the second instance of noncompliance, the Entity discovered on August 1, 2018, when its change management tool ran its comparison, the Entity discovered that one intermittently accessible open port for one high impact PACS had not been added to the baseline configuration as required by Part 1.1. This port is active only during the patching cycles. The cause of the noncompliance was that the Entity's procedure was deficient as it did not verify intermittently used ports during onboarding the device and updating the baseline configuration. The noncompliance began on July 18, 2018, when the baseline configuration was not updated during the onboarding process, and ended on August 1, 2018, when the baseline configuration was updated to reflect the dynamic port for the effected PACS.</p> <p>In the third instance of noncompliance, the Entity discovered on December 6, 2018, while performing patching on a high impact PACS, that two intermittently accessible needed ports had not been added to the baseline configuration. These ports are active only during the patching cycles. The cause of the noncompliance was that the Entity's procedure was deficient as it did not verify intermittently used ports during onboarding the device and updating the baseline configuration. The noncompliance began on July 18, 2018, when the baseline configuration was not updated during onboarding process, and ended on December 6, 2018, when the baseline configuration was updated to reflect the dynamic ports for the effected PACS.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance was minimal because the issue was limited to four PACS, which do not directly impact the Bulk Electric System. The duration of the issue was limited to 19 days, and the resolution for the issue was limited to submitting a change request; the removal of the patch was required for secure operation of the PACS device. Additionally, the issue was discovered by an internal review which was more robust than required by the Standard, and the employees who had access to the PACS had completed Personnel Risk Assessments (PRA) and training. Lastly, the PACS resided inside a Physical Security Perimeter (PSP), and the access is restricted and required authentication to access the device.</p> <p>The second instance was minimal because the issue was limited to one PACS and one open port. There was no direct impact the Bulk Electric System, and the duration was limited to 15 days. The employees who had access to the PACS had completed Personnel Risk Assessments (PRA) and training. The PACS resided inside a PSP, and the access is restricted and required authentication to access the device. Additionally, the resolution of the issue was limited to updating the baseline configuration; the intermittent port was required during the patching cycle. Lastly, this port was already approved and identified as required on other similar system baselines.</p> <p>The third instance was minimal because the issue was limited to one PACS and two open ports, which do not directly impact the Bulk Electric System. The employees who had access to the PACS had completed Personnel Risk Assessments (PRA) and training. The PACS resided inside a PSP, and the access is restricted and required authentication to access the device. Additionally, the resolution of the issue was limited to updating the baseline configuration; the intermittent port was required during the patching cycle. Lastly, this port was already approved and identified as required on other similar system baselines.</p> <p>No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated and approved the baseline; 2) developed a tool to track the action items for managing any findings from the baseline review; 3) formalized the baseline review process to ensure that the reviews are performed in a consistent manner; and 					

4) added steps to a [REDACTED] meeting to address assigned investigators and completion dates.

To mitigate the second and third instances of noncompliance, the Entity:

- 1) updated the baseline configuration with intermittently opened ports;
- 2) had its EMS team discuss, create awareness, and provide training for individuals on intermittent ports;
- 3) compared the baseline for both servers and documented the differences;
- 4) compared the baseline differences and ensured they were updated for both servers: and
- 5) added additional steps to its NERC CIP change work sheet (a tool used when onboarding or making changes to a CIP asset) to compare to existing like devices for potential intermittent 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
MRO2019022029	CIP-004-6	R4	[REDACTED] (the Entity)	[REDACTED]	10/03/2018	07/22/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 9, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED]</p> <p>On April 19, 2019, the Entity discovered that there was missing information in its access review process that resulted from software changes after a firewall upgrade. The firewall created two files for import into the access management system. The access management system can import only a single file, which resulted in partial quarterly account access reviews (there was missing electronic access authorization information in the second file that was not imported). After correcting the import process, during its manual review of updated firewall entitlements comparing entitlements with the prior quarter, the Entity identified two entitlements that had been granted electronic access without an authorization record as per Part 4.1. The prior quarterly review failed to identify these two individuals as required by Part 4.2 due to the import failure.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process to authorize electronic access, which resulted in two individuals having unauthorized access. Additionally, the Entity's quarterly review process lacked sufficient detail, resulting in the two employees, who had unauthorized access, not being identified.</p> <p>The noncompliance began on October 3, 2018, when the two individuals were provided access without authorization, and ended on July 22, 2019, when the individual's access were authorized.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the issue was limited to two individuals, who were current employees of the Entity and had other CIP authorization entitlements, including access to other firewalls. Additionally, the two individuals of issue were current with their Personnel Risk Assessment (PRA) and CIP training. Lastly, the issue of missing data for quarterly reviews was discovered during an internal spot-check, which limited the missed quarterly reviews to one cycle. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) authorized access for the employees of issue; 2) combined both files created by the firewall and updated the access management system to provide accurate information for quarterly reviews; 3) had its IT security administrator review all the access requirements and did not find any additional missing access authorization information; 4) updated procedures for new/added entitlements to include the need for uploading a single file to the access management system and defined a communication approach for changes or modifications made by the application owner, to ensure that authorizations are covered by proper authorization records; and 5) updated the quarterly review process to add a requirement that its IT Security Administrator will send information, prior to quarterly access reviews, containing high-level entitlement counts per application. Discrepancies will be identified by the entitlement owner, who will work with the firewall team to timely resolve the issues. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022030	CIP-004-6	R5	[REDACTED] (the Entity)	[REDACTED]	04/06/2019	07/05/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 9, 2019, the Entity submitted a Self-Log stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R1. [REDACTED] The Self-Log contained four instances of noncompliance; [REDACTED]</p> <p>In the first instance of noncompliance, the Entity determined that when a contract employee was terminated on June 7, 2019, the contractor’s firm failed to inform the Entity to remove the unescorted physical access and the Interactive Remote Access (IRA) as required by CIP-004-6 R5.1. The contractor had turned in his electronic and physical access keys on the last day he worked on site; however, continued to work off-site for 15 more days until terminated. The cause of the noncompliance was that the contractor firm failed to follow the Entity’s process to submit the off-boarding forms in a timely manner for removal of access permissions on contractor termination. Additionally, the Entity’s contracts supervisor (who had previously been made aware of the contractor’s planned termination) failed to follow the Entity’s process to ensure that the contractor’s off-boarding forms were received in a timely manner for removal of access permissions on contractor termination. Lastly, the Entity’s service vendor contract template included incorrect information concerning termination notification timeframes. The noncompliance began on June 8, 2019, which was 24 hours after contractor was terminated, and ended on June 13, 2019, when access was revoked.</p> <p>In the second instance of noncompliance, the Entity determined that when another contract employee was terminated on June 14, 2019, the contractor’s firm did not inform that Entity until June 19, 2019. Additionally, the contractors firm failed to inform the Entity to remove the unescorted physical access and the Interactive Remote Access (IRA) as required by CIP-004-6 R5.1. The contract employee was working as a relay testing engineer and subsequently began working as regional director for the same firm. The cause of the noncompliance was that the Entity’s contractor firm failed to follow the Entity’s process to timely report the contractor’s termination. The noncompliance began on June 15, 2019, which was 24 hours after contractor was terminated, and ended on June 19, 2019, when access was revoked.</p> <p>In the third instance of noncompliance, the Entity determined that it had not been notified by a contracting firm when a contract employee had been terminated. The Entity received an email update of completion of standards of conduct training for this contractor; however, when the Entity contacted the contracting firm about the contractor, there were notified that the contractor was no longer employed with the contracting firm. The Entity promptly instructed the [REDACTED] to remove the unescorted physical access and the Interactive Remote Access (IRA) as required by CIP-004-6 R5.1. The cause of the noncompliance was that the Entity’s contractor firm failed to follow the Entity’s process to timely report the contractor’s termination. The noncompliance began on April 6, 2019, which was 24 hours after the contractor was terminated, and ended on June 13, 2019, when access was revoked.</p> <p>In the fourth instance of noncompliance, as part of its physical security services validation of access revocation review, the Entity identified that two contractor resources whose contracts were terminated on still had unescorted physical access to Entity’s BES Cyber Systems. The cause of the noncompliance was that the Entity failed to follow its process for removal of access permissions on contractor termination. The began on July 2, 2019, which was 24 hours after the first contractor was terminated, and ended on July 5, 2019 when access was revoked for both contractors.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance was minimal because the contractor had turned in his electronic and physical access keys on the last day he worked on site, which removed the unescorted physical access and the IRA access. It was confirmed that the contractor did not attempt to gain access to BCAs, the contractor was current on his personnel risk assessment (PRA) and CIP training, and had read-only access to the SCADA system. Lastly, the contractor termination was not for cause, which reduces the risk of malicious use.</p> <p>The second instance was minimal because it was confirmed that the contractor did not attempt to gain access to BCAs during the time of noncompliance. They did not attempt to gain access to any of the Entity’s substations, and prior to accessing the PSP at the substation, the individual would have had to access the exterior gate, for which access was not provisioned. Additionally, the contractor was current on his PRA and CIP training. Lastly, the contractor termination was not for cause, which reduces the risk of malicious use.</p> <p>The third instance was minimal because it was confirmed that the contractor did not attempt to gain physical access to the EMS SCADA room, primary control center, or communications room during the time of noncompliance. The contractor did not have logical access and during this noncompliance, and it was confirmed that the contractor did not attempt to gain access to BCAs. Additionally, the contractor was current on his PRA and CIP training. Lastly, the contractor termination was not for cause, which reduces the risk of malicious use.</p>					

	<p>The fourth instance was minimal because it during this noncompliance, it was confirmed that the contractors did not attempt to gain access to CIP restricted locations. The contractors were current on their PRA, and CIP training and the contractor’s termination were not for cause, which reduces the risk of malicious use.</p> <p>No harm is known to have occurred.</p>
<p>Mitigation</p>	<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked unescorted physical access, CIP access, and logical access for the contractor of issue; 2) contacted the contractor to remind them of details and importance of following the Entity off-boarding processes.; and 3) reminded its technical consultant assistant and contracts supervisor of CIP-004-6 compliance requirements, including the [REDACTED] and the importance of the 24-hour access removal procedure; and 4) updated the service vendor contract template with current access removal timeframes as required by CIP-004-6. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked unescorted physical access, CIP access, and logical access for the contractor of issue; 2) reminded the consultant about the contractually agreed requirements to timely report the termination within 12 hours and the Entity’s CIP compliance self-reporting policy; and 3) updated the service vendor contract template with current access removal timeframes as required by CIP-004-6. <p>To mitigate the third instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked unescorted physical access and CIP access for the contractor of issue; 2) contacted the contractor to remind them about the contractually agreed requirements to timely report terminations; and 3) updated the service vendor contract template with current access removal timeframes as required by CIP-004-6. <p>To mitigate the fourth instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked unescorted physical access and CIP access for the contractors of issue; 2) sent a procedural reminder to its managers about the steps to be taken and required timeframe to revoke CIP access upon employee/contractor termination. This communication also referenced two earlier emails sent about the access removal timeframes and possible disciplinary actions if the managers do not adhere to this process; and 3) created schedule for ongoing training on expectation of timely submission of [REDACTED] for contractors and employees.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022031	CIP-007-6	R5	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	08/22/2019	Self-Log	03/31/2020 Expected Date
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</p>			<p>On August 9, 2019, the Entity submitted a Self-Log stating that as a [REDACTED] [REDACTED] The Self-Log contained four instances of noncompliance; [REDACTED]</p> <p>In the first instance of noncompliance, there were two issues: one was a firmware update issue and the other was associated with Cyber Vulnerability Assessments (CVA). For the first issue, the Entity discovered during a firmware update at two medium impact substations that passwords on six digital meter devices had not been changed from the default of “no password” per CIP-007-6 R5.4. The cause of the noncompliance was that Entity field technicians failed to follow the Entity’s processes regarding inventory of new accounts and changing of known default passwords (per Cyber Asset capability). The noncompliance began on March 15, 2018, the day the first device was installed, and ended on December 21, 2018, when the last password was changed.</p> <p>For the second issue of the first Self-Logged instance of noncompliance, the Entity discovered that while performing an annual Cyber CVA that an additional eleven devices in one of the medium impact substations and seven devices in the second medium impact substation did not have passwords changed from the default of “no password”. The cause of the noncompliance was that Entity field technicians failed to follow the Entity’s processes regarding inventory of new accounts and changing of known default passwords (per Cyber Asset capability). The noncompliance began on March 15, 2018, the day the first device was installed, and ended on May 8, 2019, when the passwords were changed.</p> <p>In the second instance of noncompliance, during the Entity’s annual CVA, it discovered two devices password [REDACTED] had not been changed as required by CIP-007-6 R5.4. These devices resided in a medium impact substation. The cause of the noncompliance was the Entity’s process was deficient in that it did not specify that the contents of the CVA device worksheet should be compared to the CVA password worksheet for verification of all required passwords that also included [REDACTED] access level passwords. The noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on February 28, 2019, when the [REDACTED] access level passwords were changed from the default passwords.</p> <p>In the third instance of noncompliance, the Entity discovered that the media access control (MAC) address of two network interface (NIC) cards in the Physical Access Control System (PACS) panels did not match the MAC addresses recorded in the Entity’s panel inventory and had a default password that had not been changed in accordance with CIP-007-6 R5.4. The cause of the noncompliance was that the Entity failed to follow its processes related to changing known default passwords (per Cyber Asset capability) and for failing to notify the PACS server support team when equipment was replaced so the default passwords could be changed. Additionally, the Entity’s process was deficient in that it did not ensure communication between all affected departments when repairs/replacements were made for PACS equipment. The noncompliance began on December 7, 2018, the day the NIC cards were replaced, and ended on June 14, 2019, when the default passwords had both been changed.</p> <p>In the fourth instance of noncompliance, the Entity discovered that a Technical Feasibility Exception (TFE) [REDACTED] [REDACTED] had not been updated to reflect the replacement(s) reported in the third instance of noncompliance. Further investigation showed that the TFE had not been updated to reflect the addition of a [REDACTED] which had been added since March 6, 2019. This is a noncompliance of CIP-007-6 part 5.7, as the TFE is for the ability to limit unsuccessful login attempts. The cause of the noncompliance was that the Entity’s process was deficient in that it did not ensure communication between all affected departments when repairs/replacements are made to PACS equipment and default passwords should be changed or a TFE should be filed. The noncompliance began on March 6, 2018, 60 days after the change was made, and ended on August 22, 2019, when the Entity submitted the material change report to update the TFE [REDACTED].</p>					
<p>Risk Assessment</p>			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance was minimal because to successfully exploit the noncompliance, in addition to the knowledge of the password, an attacker would be required to either bypass the Entity’s multi-factor authentication scheme or bypass the physical protections of the Physical Security Perimeter (PSP) where the devices were located. This greatly reduces the likelihood that an intruder could access the devices. Additionally, each affected device resides within an Electronic Security Perimeter (ESP) and a PSP and thus required an Intermediate System for Interactive Remote Access. The issues were limited to substations and did not impact control centers. Lastly, the noncompliance was discovered during a firmware upgrade and annual CVA (secondary control).</p> <p>The second instance was minimal because the devices did not have external routable connectivity; they are serially connected to ethernet external transceivers and the transceivers were protected and updated. The passwords on lower access levels, which must be successfully accessed prior to being able to access the [REDACTED] level, had been changed in accordance with applicable CIP-007-6 Part 5</p>					

	<p>requirements; this greatly reduces the likelihood that an intruder could access the [REDACTED] level. Additionally, each affected device resides within an ESP and a PSP and were protected in accordance with the Entity's standards for devices residing within a substation ESP and PSP. Lastly, the issue was limited to a substation and did not impact the Entity's control centers.</p> <p>The third instance was minimal because the Entity's PACS server and NICs are protected behind a firewall and are on a separate virtual local area network (VLAN) which provides segmentation from other parts of the network. Additional knowledge such as make and model of the NIC, the password, IP address, and port number is needed to access the NICs. To gain remote access the attacker needs to know username and password for another login server. Additionally, all affected devices were protected in accordance with the Entity's standards for devices residing within a [REDACTED]. Lastly, all affected NICs were located in substations, and none of the affected equipment resided in a control center.</p> <p>The fourth instance was minimal because there was an existing TFE for [REDACTED]; the noncompliance was a failure to update the existing TFE. Additionally, the affected devices were protected in accordance with the Entity's standards for devices residing within a [REDACTED]. Lastly, an extent of condition analysis was performed, which did not find any additional instances.</p> <p>No harm is known to have occurred.</p>
Mitigation	<p>To mitigate the issues included in the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) added complex passwords to vendor default accounts. <p>Additionally, to mitigate the issues included in the first instance of noncompliance, the Entity will complete the following mitigation activities by March 31, 2020 as part of a phased plan:</p> <ol style="list-style-type: none"> 1) simplify the vendor change form without diminishing required evidentiary information. This will help field technicians who do not routinely work within CIP substations; 3) incorporate a secondary verification (peer review) to validate security controls and evidence documentation in change control workbooks; 4) develop tools to aid field technicians; and 5) implement a process to have the CIP Analyst perform checks on password changes. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated passwords on all affected devices; and 2) updated the device passwords again to complex [REDACTED] character passwords. <p>To mitigate the third instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) changed the passwords; 2) had its security vendor and internal personnel responsible for password changes and inventory updates discuss the importance of communication when replacing NIC which included the importance of detailed records for all work performed to ensure that all changes are understood, documented, and communicate to all relevant parties. <p>To mitigate the fourth instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) submitted a material change report to update the TFE; 2) performed an extent of condition analysis and did not find any [REDACTED] to be added to the TFE; 3) discussed methods to improve communications between the teams; and 4) updated the procedures to improve the communications between the teams which included: <ul style="list-style-type: none"> • sending an email to the PACS server team from [REDACTED] team to notify them of the change when updates are made to [REDACTED] inventory sheet; • having the [REDACTED] team update the spreadsheet stored in SharePoint site with version history describing the changes made; and • modify properties of the access panel inventory sheet to automatically send an email to the team when the spreadsheet is updated.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022037	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	08/01/2017	02/28/2019	Self-Log	12/31/2020 Expected Date
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 9, 2019, the Entity submitted a Self-Log stating that as a [REDACTED] [REDACTED] The Self-Log contained two instances of noncompliance; [REDACTED]</p> <p>In the first instance of noncompliance, during an internal review of devices with synchrophasors in a substation, one of the Entity's CIP analyst discovered six microprocessor relays that each had authorized port information not recorded within the Entity's baseline documentation. All six devices are BES Cyber Assets (part of a medium impact BES Cyber system) with External Routable Connectivity (ERC) and Interactive Remote Access (IRA). The cause of the noncompliance was that the Entity's baseline document was deficient in that all enabled ports were not listed in the baseline tool. Additionally, the baseline process was deficient because the Entity maintained baselines by device rather than by group of devices. This created complexity and proved to be unsustainable for large number of devices. This noncompliance began on August 1, 2017; the day after the mitigation plan for a prior noncompliance [REDACTED] was completed, and ended on February 1, 2019, when the Entity updated the baseline document with authorized port information.</p> <p>In the second Self-logged instance of noncompliance, the Entity's CIP Compliance team discovered during a review of devices, which had been previously installed in a medium impact substation, that for six SCADA meters the firmware versions installed were the approved current versions. However, the Entity could not locate the change control documentation to evidence the change and the baseline changes were not updated as required by Part R1.3. The field personnel who originally installed the meters noticed the screen locking for five of the meters three days after the installation. The field personnel contacted the manufacturer who recommended that the Entity install a new firmware update on the meters. The Entity then installed new firmware on the five new meters and on one additional pre-existing meter. When the new firmware version was installed on the five new devices, the team failed to update the firmware version on the change control paperwork and also failed to submit change control paperwork for the additional pre-existing device. Additionally, the Entity classified three of the meters as medium impact BCAs with ERC and IRA and the other three meters as Cyber Assets. The cause of the noncompliance was due to inadequate or incomplete training. The Entity's substation technicians failed to follow the Entity's processes to update device baselines within 30 days of completing a change to the baseline. Additionally, the Entity did not have a process for a CIP analyst or an engineer to validate a manufacturer's advice before proceeding to act on that advice to implement device changes such as firmware upgrades. This process deficiency allowed field personnel to contact the manufacturer directly and install the firmware on the devices without the validation from a CIP analyst or an engineer. This noncompliance began on November 15, 2018, 31 days after the meter firmware was updated, and ended on February 28, 2019, when the Entity updated the baseline documentation.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance was minimal because the resolution of the issue was limited to updating baseline documentation; all three open ports were required for operation and there were no ports open that should have be closed. Additionally, the issue was limited to six BES Cyber Assets.</p> <p>The second instance was minimal because the meters had current firmware updates, baselines existed, and the issue was limited to updating the baseline documentation. Additionally, during the current year cyber vulnerability assessment, it verified that all other required security measures had been implemented. Lastly, the issue was discovered by an internal review that MRO considered to be more robust than required by the Standard.</p> <p>No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the baseline document; 2) revised the baseline instruction and communication process for field technicians to include additional training and clear instructions for ports and services baselines; and 3) completed training on baseline instruction and communication process for all the field technicians. 					

Additionally, to mitigate this noncompliance, the Entity will complete the following mitigation activities by December 31, 2020:
1) update the ports and service database to be managed by group (device type) rather than by individual Cyber Asset. The reason for the delayed date is that this is the last step as part of phased implementation.

To mitigate the second instance of noncompliance, the Entity:

- 1) updated the baseline document;
- 2) provided CIP compliance training sessions to all relay technicians and electrician specialists groups to understand the CIP deliverable and baseline document; and
- 3) developed a process for validating manufacturer's advice with a CIP analyst or an engineer before proceeding to act on the advice of the manufacturer for changes such as firmware upgrades.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022378	CIP-010-2	R3	[REDACTED] (the Entity)	[REDACTED]	02/01/2019	02/20/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 2, 2019, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R3. [REDACTED]</p> <p>The Entity reported that while performing a scheduled cyber vulnerability assessment (CVA) on May 5, 2019, the Entity discovered that it had not performed a CVA on two of its six Electronic Access Control or Monitoring System (EACMS) as required by CIP-010-2 R3.</p> <p>The cause of the noncompliance was that the Entity's process was deficient it was not clear when the next scheduled 15 month CVA should be performed.</p> <p>The noncompliance began on February 1, 2019, which was the day after the 15-calendar month period to perform the next CVA lapsed, and ended on February 20, 2019, when CVA was completed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the noncompliance was limited to two EACMS. The system is an EACMS, not a BES Cyber Asset (BCA), and the EACMS does not directly provide any access to Cyber Assets [REDACTED]. Additionally, the duration of the noncompliance was limited to 20 days. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed the CVA; 2) created EACMS CVA automated calendar updates to provide more reminders to SMEs performing CVA scheduling. These updates provide more specific information and provide greater clarity on the next CVA due date; and 3) created a CVA tracking tool spreadsheet to ensure CVAs are completed within the required time frame. The tracking tool provides increases oversight and information across all of the systems with more eyes watching the due dates. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020763	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	09/27/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], MRO determined that the Entity, as a [REDACTED], was in noncompliance with CIP-010-2 R1.</p> <p>It was discovered that [REDACTED] sampled medium impact BES Cyber Assets [REDACTED] had incomplete baseline information. After an extent of condition analysis, MRO found that specifically, the Entity failed to develop a baseline configuration that included version tracking for [REDACTED] software. The Entity used scripts to gather its baseline information during this time from the Windows registry that did not include versions for this software. The Entity performed an extent of condition and determined that this issue affected [REDACTED] that had [REDACTED] installed, and [REDACTED] that had [REDACTED] installed.</p> <p>The cause of the noncompliance was that the Entity's process did not include a method to check baselines for versions that where not in the Windows registry.</p> <p>The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable, and ended on September 27, 2018 when the Entity updated the baselines to include these versions.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. This issue is minimal risk because the Entity's Control Center only contains medium impact BES Cyber Systems and only facilities containing low impact BES Cyber Systems are controlled and/or monitored by this Control Center. The Entity utilizes [REDACTED] software to collect hash values of related files to detect when changes have occurred to software versions. The Entity configured the system to alert the Entity to these changes that the Entity would have subsequently investigated. Additionally, the issue was limited to the documentation of two specific software versions in the baselines and not the entire Cyber Asset application. Lastly, the resolution of this issue was to add this information to the existing baselines, and changes to the BCAs were not required. No harm is known to have occurred.</p> <p>The Entity does not have any relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) added the impacted software versions to its baselines; and 2) changed its process to have a more thorough review from [REDACTED] which includes a process to manually update versions in the baselines whenever a hash difference for executables occurs and a review to verify that versions are included for all new and existing software. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020764	CIP-007-6	R5	[REDACTED] (the Entity)	[REDACTED]	07/25/2016	09/27/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], MRO determined that the Entity, as a [REDACTED], was in noncompliance with CIP-007-6 R5.</p> <p>It was determined that the Entity had a process that was in conflict with itself. The Entity's Operating procedure states the CIP-007-6 R5.5 requirement for a minimum eight character length complexity. However, later on the same page, the Entity states a minimum six character length complexity. During a review of the potential impacted systems it was found that a single medium impact BCA was impacted by this and only had the six character complexity required.</p> <p>The cause of the noncompliance was that the Entity's process had inconsistencies requiring different password length complexity.</p> <p>The noncompliance began on July 25, 2016, when a single MIBCA was deployed utilizing a configuration file that only required six character password complexity, and ended on September 27, 2018, when the configuration file was updated to require password complexity of eight characters.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the Entity's Control Center only contains medium impact BES Cyber Systems; only facilities containing low impact BES Cyber Systems are controlled and/or monitored by this Control Center. Additionally, the password requirements in the configuration file met the three character-type complexity requirement and met the previous requirement for six-character complexity limiting the potential risk for unauthorized access. Lastly, this issue impacted a single MIBCA. No harm is known to have occurred.</p> <p>The Entity does not have any relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated the impacted devices configuration file to require eight character length password complexity; and 2) updated its operating process documentation to require the eight character length password complexity. <p>MRO has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019131	CIP-006-6	R1.	[REDACTED]	[REDACTED]	07/01/2016	11/10/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 6, 2018, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it had discovered on October 19, 2017 that it was in noncompliance with CIP-006-6 R1. (1.3., 1.4., 1.5., 1.8., 1.9., 1.10). The entity had two instances of noncompliance failing to implement one or more documented physical security plans.</p> <p>The first instance of noncompliance was discovered on October 19, 2017. Entity subject matter experts raised concerns of a possible noncompliance after conducting a Cyber Vulnerability Assessment. This noncompliance started on July 1, 2016 when the entity failed to implement its physical security plan for two (2) PCAs associated with a High Impact BES Cyber System. The noncompliance ended on November 10, 2017 when the entity removed both PCAs from the Electronic Security Perimeter (ESP) rendering them no longer subject to CIP Standards.</p> <p>Specifically, two PCAs were located in two separate rooms that lacked two-factor authentication, physical access logging, and physical access alarming. The PCAs were deployed in these locations due to wiring distance constraints. [REDACTED]</p> <p>The root cause of this instance was an oversight by personnel when installing the PCAs.</p> <p>The second instance of noncompliance was discovered on September 27, 2017 when the entity's compliance manager was alerted of a compliance issue. The noncompliance involved two PSP Cabinets containing two BES Cyber Assets (BESCA) at a Medium Impact facility with External Routable Connectivity (ERC). This noncompliance started on April 1, 2017 when the entity failed to monitor two (2) PSP Cabinets for unauthorized access and issue an alarm or alert in response to detected unauthorized access. The noncompliance ended on October 20, 2017 when the entity installed direct alarms.</p> <p>The root cause of this instance was internal miscommunication and a failure to successfully transition from CIP V3 to CIP V5. Prior to the BES CAs coming online, the entity had installed locks on the cabinets. However, the BES CAs were overlooked during the Version 3 to Version 5 site review which resulted in a failure to alarm and detect unauthorized access. In addition, internal miscommunication caused the cabinets not to be alarmed prior to the devices coming on-line.</p>					
Risk Assessment			<p>These two instances of noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, not ensuring that physical security plans have been implemented for applicable Cyber Assets could lead to an unauthorized individual gaining physical access. This access could then be used to render the device unavailable, degraded, or misused due to the noncompliance.</p> <p>Instance 1 The entity reduced the risk of unauthorized physical access. [REDACTED] If the PCAs were compromised, the associated High Impact BES Cyber Systems would continue to function as the PCAs do not have an impact on the reliable operation of the BES.</p> <p>Additionally, in the event that a malicious actor were able to 'hijack' the network connection of the PCAs, the entity's [REDACTED] and the entity would follow its incident response plan upon receiving an alert. The entity also has [REDACTED]</p> <p>Instance 2 The entity reduced the risk of unauthorized physical access by limiting access to the devices via [REDACTED] Additionally, the substation security system was active for the entire substation. The keys for the device locks were secured in a PSP which has [REDACTED] The BES CAs also had unique passwords that only authorized personnel could access. The entity only allows authorized personnel and contractors unescorted physical access to the Substation.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC reviewed the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the devices from the ESP rendering them no longer subject to the CIP standards; 2) reclassified the devices in the Cyber Asset List; 3) verified secondary source synchronization was successful after PCAs were removed; 					

- | | |
|----------------------|---|
| 4)
5)
6)
7) | updated the server configuration to point to the new network the PCAs are being moved to;
updated the ESP Diagram to reflect the new configuration; updated firewall rules to accept data from PCAs in their new location;
installed alarms for unauthorized access on both cabinets; and
developed a new process that requires a checklist of activities and updated Cyber Asset forms being completed prior to installing, replacing or removing an asset. |
|----------------------|---|

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019022244	CIP-011-2	R1.	[REDACTED]	[REDACTED]	02/05/2019	05/15/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 24, 2019, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-011-2 R1 (1.2). In two separate instances, the entity failed to follow its procedures for protecting and securely handling the transmission of BES Cyber System Information (BCSI).</p> <p>The entity's data classification policy has four data classifications. The highest two data classification levels are NERC Confidential and NERC Restricted.</p> <p>The first instance of noncompliance occurred on February 5, 2019, when an entity employee emailed a collection of procedures related to CIP-002 and a file classified as NERC Confidential was inadvertently included to fellow internal entity recipients. The confidential file was included unintentionally when selecting multiple files for inclusion in the email. The entity failed to follow its procedure to protect the file with encryption and password protection. Later that day, entity personnel noticed that the confidential file had been sent and informed management who contacted the entity's internal NERC compliance department for guidance. The entity's NERC compliance department responded with instructions for deleting the files from the email inboxes of all the recipients. The noncompliance ended once all emails were purged on April 4, 2019.</p> <p>The second instance of noncompliance occurred on April 30, 2019. Another employee sent an email with a Mitigation Plan Extension Request to the entity's internal NERC compliance department. A member within the recipients identified that the attachment failed to include the same protections (encryption and password protection) and notified the entity's NERC compliance department. A follow-up email was sent to the recipients on May 13, 2019 advising them to purge the email. The noncompliance ended once all emails were purged on May 16, 2019.</p> <p>In both instances, the sources were aware of the procedure for protecting and security handling BCSI, but failed to follow the internal procedure. The cause of this noncompliance was human error due to a lack of controls and training.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to follow its procedure to secure BCSI in transit could result in unauthorized users viewing or accessing BCSI and then exploit any vulnerabilities in the associated systems and affect the reliability of the Bulk Power System.</p> <p>However, all individuals who received the files (in both instances) were internal employees and are CIP-trained and authorized for access of this information sent. Further reducing the risk, the associated system exists in an isolated environment that is not directly connected to the internet. [REDACTED] are employed to identify and prevent any unauthorized access in the associated systems. Finally, the emails were purged in a timely manner and there was no indication of interception by a malicious actor.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>The entity has relevant compliance history. NPCC determined the entity's compliance history is not aggravating because the root cause of the previous noncompliance and the root cause of the instant noncompliance are unrelated. In addition, the mitigating actions and actions to prevent recurrence in the previous noncompliance would not have addressed the cause of the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> developed an IPP Training Supplement to increase awareness of the program; required all those with NERC CIP access to review the training; administered a self-directed IPP Training Supplement; imposed more restrictive procedures on document classifications and required protections when transmitting CIP-related information; removed all NERC Confidential and NERC Restricted content from areas that do not conform to BCSI Storage oversight protections; amended monthly reports to add supplemental information that includes IPP Guidelines about the proper methods for handling, storage, and transit of sensitive information; changed policy to require any individuals that inadvertently transmit protected files to retake training, followed by additional repercussions for further offenses; and explored email screen mechanisms designed to catch keywords or phrases that imply protected files are included. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019109	CIP-006-6	R1.	[REDACTED]	[REDACTED]	07/01/2016	11/10/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 6, 2018, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it had discovered on October 19, 2017 that it was in noncompliance with CIP-006-6 R1. (1.3., 1.4., 1.5., 1.8., 1.9., 1.10). The entity failed to implement a physical security plan for Protected Cyber Assets (PCAs).</p> <p>The noncompliance was discovered on October 19, 2017. Entity subject matter experts raised concerns of a possible noncompliance after conducting a Cyber Vulnerability Assessment. This noncompliance started on July 1, 2016 when the entity failed to implement its physical security plan for two (2) PCAs associated with a High Impact BES Cyber System. The noncompliance ended on November 10, 2017 when the entity removed both PCAs from the Electronic Security Perimeter (ESP) rendering them no longer subject to CIP Standards.</p> <p>Specifically, two PCAs were located in two separate rooms that lacked two-factor authentication, physical access logging, and physical access alarming. The PCAs were deployed in these locations due to wiring distance constraints. [REDACTED]</p> <p>The root cause of this instance was an oversight by personnel when installing the PCAs.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, not ensuring that physical security plans have been implemented for applicable Cyber Assets could lead to an unauthorized individual gaining physical access. This access could then be used to render the device unavailable, degraded, or misused due to the noncompliance.</p> <p>The entity reduced the risk of unauthorized physical access. [REDACTED] If the PCAs were compromised, the associated High Impact BES Cyber Systems would continue to function as the PCAs do not have an impact on the reliable operation of the BES.</p> <p>Additionally, in the event that a malicious actor were able to 'hijack' the network connection of the PCAs, the [REDACTED] and the entity would follow its incident response plan upon receiving an alert. The entity also has [REDACTED].</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC reviewed the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the devices from the ESP rendering them no longer subject to the CIP standards; 2) reclassified the devices in the Cyber Asset List; 3) verified secondary source synchronization was successful after PCAs were removed; 4) updated the server configuration to point to the new network the PCAs are being moved to; 5) updated the ESP Diagram to reflect the new configuration; 6) updated firewall rules to accept data from PCAs in their new 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
NPCC2018019265	CIP-004-6	R4.	[REDACTED]	[REDACTED]	10/01/2016	03/31/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 27, 2018, [REDACTED] (the entity) submitted a Self-Report stating that as a [REDACTED] it was in noncompliance with CIP-004-6 R4 (4.2). The entity determined that although quarterly reviews were being performed, the reviews did not verify that individuals with active electronic access or unescorted physical access have authorization records.</p> <p>While developing the RSAW for CIP-004-6, the entity identified the issue, that although the entity conducted quarterly reviews since the Standard became mandatory and enforceable, the reviews were deficient. The reviews consisted of lists from the provisioning system, Physical Access lists, and various Cyber systems, but they did not compare the provisioned physical access system of record with the entity's database of authorized user access.</p> <p>This noncompliance started on October 1, 2016 when the entity failed to reconcile individuals with active electronic access or unescorted physical access with actual authorization records. The noncompliance ended on March 31, 2018 when the quarterly reviews were performed correctly.</p> <p>The root cause of this noncompliance was incomplete process documentation for execution of a process to verify electronic and physical access records once a quarter.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, not verifying at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records could lead to unauthorized individuals having access to applicable Cyber Assets. Unauthorized access could be used to render Cyber Assets unavailable, degraded, or misused due to the noncompliance.</p> <p>The entity reduced the risk of unauthorized individuals gaining access by performing quarterly reviews on the individual provisioning system and the access lists for physical and electronic access. All individuals with electronic or physical access were found to have authorization records. The entity requires all CIP access through an access provisioning system. Any physical access to a BES Cyber System would require an active badge.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>The entity has relevant compliance history. NPCC determined the entity's compliance history is not aggravating because the root cause of the previous noncompliance and the root cause of the instant noncompliance are unrelated. In addition, the mitigating actions and actions to prevent recurrence in the previous noncompliance would not have addressed the cause of the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) conducted a quarterly review that verified electronic and physical access; 2) updated process to perform quarterly reviews that verify individuals with active electronic access or unescorted physical access have authorization records; and 3) reminded applicable SMEs of CIP-004 requirements verbally. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021141	CIP-004-6	R5	[REDACTED]	[REDACTED]	10/17/2018	11/8/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 22, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5. On November 5, 2018, during a routine access review of a CIP information storage location, the entity discovered that a contractor was listed as having access to the CIP information storage location after the contractor had been off-boarded from the project work that required the access. The contractor's contract expired on October 15, 2018, and was not renewed by the entity. Accordingly, the entity should have removed access by the end of the next calendar day. However, the entity did not remove access until November 8, 2018, or 23 days late.</p> <p>The root cause of this noncompliance was a breakdown in the process for removing access to this particular CIP information storage location, [REDACTED]. In this case, the responsible entity employee [REDACTED] failed to notify the vendor to remove the contractor's access. This root cause involves the management practices of external interdependencies, because the access at issue was for a contractor, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on October 17, 2018, when the entity should have removed access for the contractor and ended on November 8, 2018, when the entity actually removed access for the contractor.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The potential risk posed by failing to remove access for a contractor is that the contractor could utilize that access for an improper purpose after termination. This risk was mitigated in this case by the following factors. First, the entity quickly identified the issue through effective internal controls, minimizing the length of time that the access remained active. Second, the contractors had up-to-date CIP training, a valid Personnel Risk Assessment, and left the project on good terms. ReliabilityFirst notes that the contractor did not attempt to access his account during the time the issue persisted, and that the contractor did not have physical access to any assets. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) provided evidence from revocation of the terminated contractor's access to the [REDACTED] CIP information storage location; 2) sent an awareness email to entity performers and their supervisors from the [REDACTED] project team, who are responsible for granting and removing access to this [REDACTED] CIP information storage location. This email described the issue of a failure to revoke access to a [REDACTED] CIP information storage location in a timely manner and reinforced the behavior to [REDACTED]; 3) conducted a meeting to reinforce requirements for fulfilling manual requests. Meeting invitees will include: [REDACTED] and [REDACTED]; 4) created and distributed a job aid for access removal to the [REDACTED] CIP information storage location to entity performers [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
RFC2019021140	CIP-004-6	R5	[REDACTED]	[REDACTED]	10/17/2018	11/8/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 22, 2019, the entity submitted a Self-Report stating that [REDACTED] it was in noncompliance with CIP-004-6 R5. On November 5, 2018, during a routine access review of a CIP information storage location, the entity discovered that a contractor was listed as having access to the CIP information storage location after the contractor had been off-boarded from the project work that required the access. The contractor's contract expired on October 15, 2018, and was not renewed by the entity. Accordingly, the entity should have removed access by the end of the next calendar day. However, the entity did not remove access until November 8, 2018, or 23 days late.</p> <p>The root cause of this noncompliance was a breakdown in the process for removing access to this particular CIP information storage location, [REDACTED]. In this case, the responsible entity employee [REDACTED] failed to notify the vendor to remove the contractor's access. This root cause involves the management practices of external interdependencies, because the access at issue was for a contractor, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on October 17, 2018, when the entity should have removed access for the contractor and ended on November 8, 2018, when the entity actually removed access for the contractor.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The potential risk posed by failing to remove access for a contractor is that the contractor could utilize that access for an improper purpose after termination. This risk was mitigated in this case by the following factors. First, the entity quickly identified the issue through effective internal controls, minimizing the length of time that the access remained active. Second, the contractors had up-to-date CIP training, a valid Personnel Risk Assessment, and left the project on good terms. ReliabilityFirst notes that the contractor did not attempt to access his account during the time the issue persisted, and that the contractor did not have physical access to any assets. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> provided evidence from revocation of the terminated contractor's access to the [REDACTED] CIP information storage location; sent an awareness email to entity performers and their supervisors from the [REDACTED] project team, who are responsible for granting and removing access to this [REDACTED] CIP information storage location. This email described the issue of a failure to revoke access to a [REDACTED] CIP information storage location in a timely manner and reinforced the behavior to [REDACTED]; conducted a meeting to reinforce requirements for fulfilling manual requests. Meeting invitees will include: [REDACTED] and [REDACTED]; created and distributed a job aid for access removal to the [REDACTED] CIP information storage location to entity performers [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
RFC2019021145	CIP-004-6	R5	[REDACTED]	[REDACTED]	10/17/2018	11/8/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 22, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5. On November 5, 2018, during a routine access review of a CIP information storage location, the entity discovered that a contractor was listed as having access to the CIP information storage location after the contractor had been off-boarded from the project work that required the access. The contractor's contract expired on October 15, 2018, and was not renewed by the entity. Accordingly, the entity should have removed access by the end of the next calendar day. However, the entity did not remove access until November 8, 2018, or 23 days late.</p> <p>The root cause of this noncompliance was a breakdown in the process for removing access to this particular CIP information storage location, [REDACTED]. In this case, the responsible entity employee [REDACTED] failed to notify the vendor to remove the contractor's access. This root cause involves the management practices of external interdependencies, because the access at issue was for a contractor, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on October 17, 2018, when the entity should have removed access for the contractor and ended on November 8, 2018, when the entity actually removed access for the contractor.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The potential risk posed by failing to remove access for a contractor is that the contractor could utilize that access for an improper purpose after termination. This risk was mitigated in this case by the following factors. First, the entity quickly identified the issue through effective internal controls, minimizing the length of time that the access remained active. Second, the contractors had up-to-date CIP training, a valid Personnel Risk Assessment, and left the project on good terms. ReliabilityFirst notes that the contractor did not attempt to access his account during the time the issue persisted, and that the contractor did not have physical access to any assets. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) provided evidence from revocation of the terminated contractor's access to the [REDACTED] CIP information storage location; 2) sent an awareness email to entity performers and their supervisors from the [REDACTED] project team, who are responsible for granting and removing access to this [REDACTED] CIP information storage location. This email described the issue of a failure to revoke access to a [REDACTED] CIP information storage location in a timely manner and reinforced the behavior to [REDACTED]; 3) conducted a meeting to reinforce requirements for fulfilling manual requests. Meeting invitees will include: [REDACTED] and [REDACTED]; 4) created and distributed a job aid for access removal to the [REDACTED] CIP information storage location to entity performers [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
RFC2019021236	CIP-006-6	R1	[REDACTED]	[REDACTED]	11/26/2018	11/26/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On March 8, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-006-6 R1.</p> <p>On November 26, 2018, at 4:45 PM the entity deployed an HVAC contractor and a general contractor to support data center personnel in the delivery of two Control Room Air Conditioning units into the [REDACTED] datacenter. At 5:03 PM, datacenter personnel contacted the [REDACTED] and informed them that the Physical Security Perimeter (PSP) double doors in the [REDACTED] had to be propped open in order to get the air conditioning units inside the PSP. The [REDACTED] staff person asked what the duration of the opened double door period would be and datacenter personnel informed [REDACTED] that it would be in excess of an hour. [REDACTED] deactivated the open door alarms at that time, and did not reactivate the open door alarms until 7:59 PM, when datacenter personnel contacted [REDACTED] to inform them that the air conditioning delivery was completed and both doors would be latched and closed.</p> <p>On November 27, 2018, the entity reviewed video for the period when the doors were open and the door open alarms were disabled. During this review, the entity discovered 49 entries into the PSP by five persons with authorized unescorted physical access, who were entering and exiting the PSP to deliver the air conditioning units, without properly badging and entering their PIN. While they were performing this work, the entity had a security guard at the PSP door to control access.</p> <p>The root cause of this noncompliance was inadequate communication and improper training resulting in IT personnel assuming that obtaining [REDACTED] approval to deactivate alarms and stationing a security guard at the PSP door was sufficient to control access to the PSP.</p> <p>This noncompliance involves the management practices of work management and workforce management. Work management is involved because the entity failed to adequately foresee the complexities and impacts of air conditioning unit installation and its impacts on PSP protection. Workforce management is involved because entity staff were not adequately trained to continue to badge-in when the door open alarm was turned off, additionally the ESOC and datacenter personnel did not communicate effectively regarding responsibilities during the period which the door open alarm was deactivated.</p> <p>This noncompliance started on November 26, 2018 at 5:03 PM, when the entity disabled the door open alarm and ended on November 26, 2018, at 7:59 PM when the entity enabled the door open alarm.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to utilize proper physical controls for the PSP is that an unauthorized individual could gain access and carry out malicious activity with the potential to physically or electronically impact systems and communications in the PSP. The risk in this case is mitigated by the following factors. First, the five employees involved were trusted employees with work history, who were performing work on a narrowly scoped project. Second, all of the employees and contractors involved had current NERC training and current Personal Risk Assessments. Third, [REDACTED] personnel were aware of the work being performed and a security guard was posted at the door to control access, minimizing the likelihood that any potential unauthorized person could gain access. Fourth, the entity identified the issue within one day, minimizing the risk of potential impact. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because while the result of the prior noncompliance was arguably similar, the prior noncompliance arose from a different cause.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) provided counseling to both affected IT personnel regarding badging when entering and existing propped open doors in PSPs and to ensure adequate communications with validation of any assumptions; 2) discussed badging issue with project general foremen and supervisor emphasizing better communications is needed when working inside NERC PSPs regardless of doors propped open or not. The entity also emphasized why badging is required whenever PSPs doors are propped open; and 3) developed datacenter script or checklist to provide guidance on NERC rules for door badging and escorting when planning major project work that could involve NERC PSPs. The entity notified staff members of new document. Script/Checklist will also include the following requirement: [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
RFC2019021142	CIP-004-6	R5	[REDACTED]	[REDACTED]	10/17/2018	11/8/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 22, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5. On November 5, 2018, during a routine access review of a CIP information storage location, the entity discovered that a contractor was listed as having access to the CIP information storage location after the contractor had been off-boarded from the project work that required the access. The contractor's contract expired on October 15, 2018, and was not renewed by the entity. Accordingly, the entity should have removed access by the end of the next calendar day. However, the entity did not remove access until November 8, 2018, or 23 days late.</p> <p>The root cause of this noncompliance was a breakdown in the process for removing access to this particular CIP information storage location, [REDACTED]. In this case, the responsible entity employee [REDACTED] failed to notify the vendor to remove the contractor's access. This root cause involves the management practices of external interdependencies, because the access at issue was for a contractor, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on October 17, 2018, when the entity should have removed access for the contractor and ended on November 8, 2018, when the entity actually removed access for the contractor.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The potential risk posed by failing to remove access for a contractor is that the contractor could utilize that access for an improper purpose after termination. This risk was mitigated in this case by the following factors. First, the entity quickly identified the issue through effective internal controls, minimizing the length of time that the access remained active. Second, the contractors had up-to-date CIP training, a valid Personnel Risk Assessment, and left the project on good terms. ReliabilityFirst notes that the contractor did not attempt to access his account during the time the issue persisted, and that the contractor did not have physical access to any assets. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) provided evidence from revocation of the terminated contractor's access to the [REDACTED] CIP information storage location; 2) sent an awareness email to entity performers and their supervisors from the [REDACTED] project team, who are responsible for granting and removing access to this [REDACTED] CIP information storage location. This email described the issue of a failure to revoke access to a [REDACTED] CIP information storage location in a timely manner and reinforced the behavior to [REDACTED]; 3) conducted a meeting to reinforce requirements for fulfilling manual requests. Meeting invitees will include: [REDACTED] and [REDACTED]; 4) created and distributed a job aid for access removal to the [REDACTED] CIP information storage location to entity performers [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
RFC2019021827	CIP-011-2	R2	[REDACTED]	[REDACTED]	11/11/2017	2/21/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On July 16, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-011-2 R2.</p> <p>The entity discovered multiple instances where personnel did not follow the entity's procedures for CIP asset reuse and disposal. The procedures require entity technicians to document the data storage media removed from an asset, including recording the serial numbers. The entity discovered that technicians removed hard drives from six Physical Access Control Systems (PACS) and processed those hard drives for destruction without documenting the serial numbers for the hard drives. Because the technicians failed to document the serial numbers, the entity has no record of destruction for these specific hard drives. The entity properly followed all other steps for CIP asset reuse and disposal except for documenting the serial numbers.</p> <p>The entity discovered this noncompliance in April 2019 when the entity conducted a [REDACTED] [REDACTED] revealed no hardware destruction reports exist that correlate to the hard drives removed from the PACS. The entity believes that disposal of the hard drives likely occurred on February 21, 2018 which was the first disposal date after the PACS servers were removed from service on November 11, 2017.</p> <p>This noncompliance involves the management practices of work management, workforce management, and reliability quality management. [REDACTED]</p> <p>[REDACTED] Therefore, the detailed evidence tracking the serial number of the hard drives to a specific PACS server was not documented as would have been if the CIP workflow was used. The root cause of this noncompliance was that the technician used the wrong workflow due to ineffective training. Additionally, the entity did not have an effective internal control in place to ensure the right workflow was used.</p> <p>This noncompliance started on November 11, 2017, when the entity was required to have disposed of the hard drives after they were removed from service and ended on February 21, 2018, when the entity disposed of the hard drives.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by not properly disposing of CIP assets is that improper disposal increases the risk that Bulk Electric System Cyber System Information (BCSI) could be obtained from the CIP assets and exploited by unauthorized individuals. The risk is minimized because both [REDACTED] hard drives are disposed of in almost exactly the same way. The only difference is the recording of serial numbers for CIP hard drives which did not occur in this noncompliance. The entity followed every disposal step correctly except for documenting the serial numbers. This is primarily a documentation issue. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> reinforced to the impacted team members regarding the correct change model to use for Cyber Asset disposal, ensuring the CIP process is followed in its entirety and with the correct level of documentation within the service management system; and implemented a quarterly review process, beginning with the end of the 2nd quarter 2019, of all CIP change tickets that were entered for asset disposal. This was completed as part of a quality assurance (QA) check, performed by the Manager and/or Supervisor of the team(s) handling the asset disposal. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021308	CIP-002-5.1	R1	[REDACTED]	[REDACTED]	7/1/2016	2/18/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On March 28, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-002-5.1 R1. On July 24, 2018, while performing a gap analysis, the entity discovered that a redundant pair of firewalls at a medium impact facility was not included on its CIP-002 Bulk Electric System (BES) Categorization list. However, the entity confirmed that this was only a documentation issue because the firewall pair was still afforded all of protections required for BES Cyber Assets.</p> <p>The root cause of this noncompliance was the failure to effectively coordinate and communicate with plant personnel during the asset identification and verification process. Specifically, the entity failed to include the relevant subject matter experts in the reconciliation process to ensure the asset list was complete and accurate. This root cause involves the management practice of verification, in that the entity failed to properly verify the information on the asset list.</p> <p>This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-002-5.1 R1 and ended on February 18, 2019, when the entity completed a full physical inventory and validation of the BES Cyber Asset list. (The entity did not identify any other assets missing from the BES Cyber Asset list.)</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to properly identify BES Cyber Assets is that the entity may not properly protect omitted assets. This risk was mitigated in this case by the fact that the entity confirmed that it was properly protecting the redundant firewall pair despite not including them on its BES Cyber Asset list. Additionally, the redundant firewall pair was the only asset that was missing from the BES Cyber Asset list, indicating that this was an isolated issue. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) developed a simplified BES Cyber Asset validation process; 2) trained personnel on the inventory and validation process, reporting identified differences, and establishing a mechanism for timely follow-up; 3) included the asset tag and description of BES Cyber Asset in change management process as a secondary check; and 4) executed a full physical inventory and validation of BES Cyber Asset list at Medium impact plants. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021309	CIP-002-5.1a	R2	[REDACTED]	[REDACTED]	10/1/2017	2/18/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On March 28, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-002-5.1a R2. On July 24, 2018, while performing a gap analysis, the entity discovered that a redundant pair of firewalls at a medium impact facility was not included on its CIP-002 Bulk Electric System (BES) Categorization list. However, the entity confirmed that this was only a documentation issue because the firewall pair was still afforded all of protections required for BES Cyber Assets. While investigating the cause of the missed identification issue, the entity discovered that it failed to perform a full and complete 15-calendar month review and verification of the BES Cyber Asset list, which would have identified the missing firewall pair.</p> <p>The root cause of this noncompliance was a lack of training on the asset list verification process. Specifically, responsible personnel lacked clear understanding regarding roles and responsibilities in the process. This root cause involves the management practice of workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on October 1, 2017, when the entity was required to have completed its first 15-calendar month review and verification of the BES Cyber Asset list and ended on February 18, 2019, when the entity completed a full physical inventory and validation of the BES Cyber Asset list. (The entity did not identify any other assets missing from the BES Cyber Asset list.)</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to perform a 15-calendar month review and verification of the BES Cyber Asset list is that the entity may not identify changes to its inventory. The risk was mitigated in this case by the following factors. First, the redundant firewall pair was the only asset that was missing from the BES Cyber Asset list, indicating that this was an isolated issue. Second, the entity confirmed that it was properly protecting the redundant firewall pair despite not including them on its BES Cyber Asset list. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) developed a simplified BES Cyber Asset validation process; 2) trained personnel on inventory and validation process, reporting identified differences, and establishing a mechanism for timely follow-up; 3) included asset tag and description of BES Cyber Asset in change management process as a secondary check; and 4) executed a full physical inventory and validation of BES Cyber Asset list at Medium impact plants. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019020929	CIP-004-6	R4	[REDACTED]	[REDACTED]	1/29/2018	7/2/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On January 9, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R4.</p> <p>On June 18, 2018, the entity discovered unauthorized access during the performance of its quarterly entitlement review. The entity mistakenly provided unauthorized [REDACTED] production server access to 11 individuals who should not have had access to the [REDACTED] production server. The entity commissioned the new [REDACTED] servers on January 29, 2018 and during the project cutover process, the entity added the access list to the entitlement review list, which placed it in the queue for entitlement review for the first time in the second quarter of 2018. The entity identified this error while performing the second quarter entitlement review on June 18, 2018.</p> <p>The unauthorized [REDACTED] access occurred because the entity relied on the wrong list (directory) of users as the valid login group. The production and failover servers for the [REDACTED] application used the [REDACTED] Active Directory (AD) users as the valid login group. However, there is a separate AD group for the [REDACTED] Production server which should have been used as the user login group for the [REDACTED] production server instead of the staging server AD group. Therefore, since the incorrect AD group was used during [REDACTED] onboarding, 11 individuals were incorrectly provided access to the [REDACTED] production server.</p> <p>The root cause of this noncompliance was the entity's failure to validate that the proper AD group was used for commissioning.</p> <p>This noncompliance involves the management practices of validation and implementation. Validation is involved in this noncompliance because the entity failed to validate that the proper AD group was attached to the [REDACTED] production server during onboarding. Implementation is involved in this noncompliance because the [REDACTED] AD group failure occurred during the implementation of various [REDACTED] servers.</p> <p>This noncompliance started on January 29, 2018, when the [REDACTED] production server was commissioned and unauthorized access was granted. The noncompliance ended on July 2, 2018, when the entity revoked the unauthorized access and changed to the proper AD group.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (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 Bulk Electric System Cyber Assets and associated systems. The risk is minimized because all 11 individuals who were incorrectly provided access to the [REDACTED] production server had current Personnel Risk Assessments (PRAs). Further minimizing the risk, the 11 individuals were authorized to access similar staging [REDACTED] servers. The entity also notes that upon reviewing the logs of individuals who accessed the [REDACTED] production server during the timeframe in questions, none of the 11 individuals logged into the server. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances involved different facts and circumstances and root causes than the instant noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) revoked access from the unauthorized users; 2) met to discuss the issue; 3) reviewed the issue at the CIP Senior Manager meeting; 4) reviewed the self-report at the CIP Senior Manager meeting; 5) developed access controls to monitor [REDACTED] servers to ensure only Production access is implemented. [REDACTED] 6) implemented automated access and monitoring controls to replace manual monitoring of servers to reduce the risk of a recurrence; and 7) trained applicable personnel on the new access monitoring 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
RFC2019020928	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/17/2018	7/24/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On January 9, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-010-2 R1.</p> <p>On July 17, 2018, after an approved change to disable domain services on a system was placed into production, a [REDACTED] team member at the entity determined that the priority order for the traffic path on the Electronic Access Control or Monitoring System (EACMS) was not properly configured, which had resulted in certain internal systems being unreachable using two-factor authentication. In order to restore the service, entity personnel modified the order of the priority of traffic on those systems. This order of priority modification was performed without an approved change request, meaning it was unauthorized as it relates to CIP-010-2 R1.</p> <p>After the change was implemented, between the period of July 17, 2018 and July 24, 2018, [REDACTED] personnel contacted the [REDACTED] [REDACTED] team to validate the change approach. At that time, it was discovered that the changes to the systems were placed into production without an approved change request.</p> <p>The root cause of this noncompliance was inadequate training and a lack of emphasis on adhering to the company's change management process which led to the technician in charge modifying the order of the priority of traffic without executing a change ticket request.</p> <p>This noncompliance involves the management practices of asset and configuration management and workforce management. Asset and configuration management is involved because the entity failed to adhere to its own asset and configuration management policy to ensure that changes were not made in the production environment without prior approval. Workforce management is involved because entity staff were not adequately trained on the details and importance of the entity's change management policy.</p> <p>This noncompliance started on July 17, 2018, when the entity made changes to the production environment without an approved change request and ended on July 24, 2018, when the entity approved the change request.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The risk posed by making an unapproved change to a server without proper change management documentation is that the unapproved change could negatively affect security controls and thus the BPS. The risk here is minimized because the work, while unscheduled, was necessary to restore services. Additionally, the entity's change management process allows these types of changes under an emergency change process in which the change implementer documents their work, and in this instance the documentation simply was not completed. Lastly, the entity identified, assessed, and corrected this noncompliance in just seven days. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances involved different facts and circumstances and root causes than the instant noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) reviewed the technical change and validated it matched with restoration of services [REDACTED] personnel were provided instructions on the proper change approach in this instance and had a refresher on the proper change management approach overall; 2) reviewed the issue at the CIP Senior Manager meeting; 3) reviewed the self-report at the CIP Senior Manager meeting; 4) developed training course content for [REDACTED]; 5) piloted and refined a presentation of [REDACTED] and refined both job aids based on feedback. (The proposed job aids will allow for timely and consistent decisions, reducing service restoration delays and increasing proper change behavior.); 6) implemented the job aids; and 7) conducted "train the trainer" on [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
RFC2019021144	CIP-004-6	R5	[REDACTED]	[REDACTED]	10/17/2018	11/8/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 22, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5. On November 5, 2018, during a routine access review of a CIP information storage location, the entity discovered that a contractor was listed as having access to the CIP information storage location after the contractor had been off-boarded from the project work that required the access. The contractor's contract expired on October 15, 2018, and was not renewed by the entity. Accordingly, the entity should have removed access by the end of the next calendar day. However, the entity did not remove access until November 8, 2018, or 23 days late.</p> <p>The root cause of this noncompliance was a breakdown in the process for removing access to this particular CIP information storage location, [REDACTED]. In this case, the responsible entity employee [REDACTED] failed to notify the vendor to remove the contractor's access. This root cause involves the management practices of external interdependencies, because the access at issue was for a contractor, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on October 17, 2018, when the entity should have removed access for the contractor and ended on November 8, 2018, when the entity actually removed access for the contractor.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The potential risk posed by failing to remove access for a contractor is that the contractor could utilize that access for an improper purpose after termination. This risk was mitigated in this case by the following factors. First, the entity quickly identified the issue through effective internal controls, minimizing the length of time that the access remained active. Second, the contractors had up-to-date CIP training, a valid Personnel Risk Assessment, and left the project on good terms. ReliabilityFirst notes that the contractor did not attempt to access his account during the time the issue persisted, and that the contractor did not have physical access to any assets. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) provided evidence from revocation of the terminated contractor's access to the [REDACTED] CIP information storage location; 2) sent an awareness email to entity performers and their supervisors from the [REDACTED] project team, who are responsible for granting and removing access to this [REDACTED] CIP information storage location. This email described the issue of a failure to revoke access to a [REDACTED] CIP information storage location in a timely manner and reinforced the behavior to [REDACTED]; 3) conducted a meeting to reinforce requirements for fulfilling manual requests. Meeting invitees will include: [REDACTED] and [REDACTED]; 4) created and distributed a job aid for access removal to the [REDACTED] CIP information storage location to entity performers [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
RFC2019021143	CIP-004-6	R5	[REDACTED]	[REDACTED]	10/17/2018	11/8/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 22, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5. On November 5, 2018, during a routine access review of a CIP information storage location, the entity discovered that a contractor was listed as having access to the CIP information storage location after the contractor had been off-boarded from the project work that required the access. The contractor's contract expired on October 15, 2018, and was not renewed by the entity. Accordingly, the entity should have removed access by the end of the next calendar day. However, the entity did not remove access until November 8, 2018, or 23 days late.</p> <p>The root cause of this noncompliance was a breakdown in the process for removing access to this particular CIP information storage location [REDACTED]. In this case, the responsible entity employee [REDACTED] failed to notify the vendor to remove the contractor's access. This root cause involves the management practices of external interdependencies, because the access at issue was for a contractor, and workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on October 17, 2018, when the entity should have removed access for the contractor and ended on November 8, 2018, when the entity actually removed access for the contractor.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The potential risk posed by failing to remove access for a contractor is that the contractor could utilize that access for an improper purpose after termination. This risk was mitigated in this case by the following factors. First, the entity quickly identified the issue through effective internal controls, minimizing the length of time that the access remained active. Second, the contractors had up-to-date CIP training, a valid Personnel Risk Assessment, and left the project on good terms. ReliabilityFirst notes that the contractor did not attempt to access his account during the time the issue persisted, and that the contractor did not have physical access to any assets. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> provided evidence from revocation of the terminated contractor's access to the [REDACTED] CIP information storage location; sent an awareness email to entity performers and their supervisors from the [REDACTED] project team, who are responsible for granting and removing access to this [REDACTED] CIP information storage location. This email described the issue of a failure to revoke access to a [REDACTED] CIP information storage location in a timely manner and reinforced the behavior to [REDACTED]; conducted a meeting to reinforce requirements for fulfilling manual requests. Meeting invitees will include: [REDACTED] and [REDACTED]; created and distributed a job aid for access removal to the [REDACTED] CIP information storage location to entity performers [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
RFC2019022536	CIP-011-2	R1: P1.2	[REDACTED]	[REDACTED]	1/30/2019	3/8/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On June 30, 2019, the entity submitted a self-log stating that, [REDACTED], it was in noncompliance with CIP-011-2 R1.2. More specifically, on January 30, 2019, an individual in the entity's legal department inadvertently sent a cyber security incident response handbook to an external law firm via an e-mail attachment.</p> <p>The root causes of this noncompliance were employee oversight and a lack of preventative controls. The entity utilizes a tool [REDACTED] relating to Bulk Electric System Cyber System Information (BCSI). At the time of this noncompliance, the tool was [REDACTED]. And, in this case, the tool [REDACTED].</p> <p>This noncompliance involves the management practice of risk management. The entity recognized a risk associated with the transmission of BCSI and, therefore, implemented [REDACTED]. But, in this case, the [REDACTED] did not function as intended, demonstrating the importance of mitigating risk through layered controls to prevent and detect issues.</p> <p>This noncompliance started on January 30, 2019, when BCSI was inadvertently shared and ended on March 8, 2019, when the entity confirmed that the law firm destroyed the BCSI.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Inadvertently sharing BCSI could lead to misuse of the information and corresponding harm to the BPS. Here, the risk was minimized because the handbook was a general, "high level" document that does not contain detailed BCSI. It does not contain information that could be used to gain unauthorized access, and it was only sent to one e-mail address that belonged to an individual working at an outside law firm. The entity confirmed that the outside law firm deleted the handbook. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) deleted the copy of the handbook from outlook and the local drive; 2) confirmed that the external entity destroyed physical and electronic copies of the handbook and accompanying email as well as electronic copies from the system backup; 3) researched the capability of the tool [REDACTED]; 4) researched how to use the tool [REDACTED]; 5) researched capability to prevent confidential documents from being sent via email as attachments; 6) researched moving electronic storage locations; and 7) implemented appropriate and reasonable solutions identified through its research. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022537	CIP-004-6	R4: P4.1	[REDACTED]	[REDACTED]	10/22/2018	2/13/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On June 30, 2019, the entity submitted a self-log stating that, [REDACTED] it was in noncompliance with CIP-004-6 R4.1. Per the entity's access management program, only authorized individuals can approve requests for electronic access, physical access, or access to storage locations for Bulk Electric System (BES) Cyber System Information (BCSI). The entity has a process for tracking such authorizers. In this case, during an annual review, entity personnel discovered that unauthorized individuals had approved requests for access to BCSI repositories. The entity investigated and discovered that the authorized approval group for one electronic BCSI repository included two incorrect authorizers, and the authorized approval group for two physical BCSI repositories had one incorrect authorizer. This noncompliance involves the latter incorrect authorizer who approved 24 requests for access that resulted in 15 individuals obtaining access to the physical BCSI repositories, which were staging areas for future BES Cyber Assets. By the time the entity discovered the issue, nine of the 15 individuals had used the provisioned access.</p> <p>The root causes of this noncompliance were: (a) entity personnel did not fully complete the process of creating and populating approved authorizers for the affected BCSI repositories; (b) entity personnel incorrectly approved a request for additional, incorrect authorizers due to difficulty in distinguishing various groups; and (c) a lack of sufficient detective controls beyond the annual review that led to the discovery of this noncompliance.</p> <p>This noncompliance implicates the management practices of workforce management and information management. Workforce management involves, in part, properly managing employee access permissions. And, effective information management includes the protection of information assets through physical, technical, and administrative controls.</p> <p>This noncompliance started on October 22, 2018, when the entity authorized access without following all of the requirements of its process and ended on February 13, 2019, when the entity removed all of the incorrectly provisioned access so that it could re-authorize access in accordance with its process.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious and substantial risk to the reliability of the bulk power system (BPS). Unauthorized access could be exploited or misused and cause corresponding harm to the BPS. Here, the risk was minimized based upon the following facts. This noncompliance was largely a documentation issue that involved a missed procedural step. All 15 of the individuals who obtained access had a legitimate business need for that access, had previously completed cyber security training, and were subjected to required background checks. Further, a supervisor for each of the 15 individuals had previously approved the requested access. Lastly, the individuals only obtained access to a staging area for future assets. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed the incorrect authorizers; 2) removed 15 entitlements that were approved by the incorrect authorizers so that the entity could re-authorize access in accordance with its process; 3) performed an extent of condition on all authorizers to identify any additional, incorrect authorizers (note: no additional, incorrect authorizers were found); 4) implemented a new control [REDACTED]; 5) completed a configuration change [REDACTED]; 6) reinforced expectations and review the new control with the responsible group; 7) updated its access control and management procedure to add a preventive control [REDACTED]; and 8) communicated the new approval process and set expectation that the process is to be followed for all authorized approver group requests. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022538	CIP-002-5.1	R1	[REDACTED]	[REDACTED]	7/1/2016	9/13/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On June 30, 2019, the entity submitted a self-log stating that, [REDACTED] it was in noncompliance with CIP-002-5.1 R1. While reviewing its asset inventory, the entity identified three [REDACTED] Bulk Electric System Cyber Assets (BCAs) (i.e., [REDACTED]) that were not in its BCA inventory and did not have documented baselines. The assets are located a facility that is shared with another company. During its initial cyber asset identification process, the entity incorrectly concluded that the other company owned the assets. The entity performed an extent of condition to confirm correct cyber asset ownership at facilities that it shares with the other company and identified two additional [REDACTED] that were not in its BCA inventory and did not have documented baselines.</p> <p>The root causes of this noncompliance were: (a) a lack of proper investigation during the entity's initial cyber asset identification process; and (b) a lack of sufficient controls in the walkdown and post-walkdown processes that would have assisted in identifying and resolving such issues. This noncompliance implicates the management practice of asset and configuration management. Entities must ensure that assets are properly inventoried, monitored, managed, and controlled.</p> <p>This noncompliance started on July 1, 2016, when the entity did not account for the assets in its BCA inventory and ended on September 13, 2019, after the entity completed an extent of condition, added the assets to its BCA inventory, and documented baselines for the assets.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Failing to account for cyber assets could lead to a corresponding failure to implement appropriate safeguards to protect those assets, which could have an adverse impact on the reliability and resilience of the BPS. Here, the risk was minimal based upon the following facts. The assets [REDACTED] do not have external routable connectivity. Moreover, even though the entity did not include the assets in its inventory or document baselines, further investigation revealed that the entity was still protecting the assets (e.g., current firmware, up-to-date patching, and port management), thereby rendering this noncompliance mostly a documentation issue. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) discussed cyber asset identification and lessons learned on the [REDACTED] walkdown process, including post-walkdown action items, with responsible engineers; 2) updated its asset inventory and created baselines; 3) updated the relevant maintenance procedure to clarify roles and responsibilities for [REDACTED] ownership at shared facilities with the other company; 4) created a control that confirms all post-walkdown action items are addressed; and 5) performed an extent of condition to confirm correct cyber asset ownership at similar shared facilities and took appropriate follow-up action. The entity found two additional assets as set forth in the description of 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
SERC2018020796	CIP-014-2	R6, P6.3	[REDACTED]	[REDACTED]	08/15/2016	06/11/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 11, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-014-2 R6, P6.3. The Entity failed to modify its evaluation or security plan consistent with the recommendation or document the reason for not doing so within 60 calendar days of the completion of an unaffiliated third-party review.</p> <p>On June 15, 2016, the Entity received recommendations from an unaffiliated third-party reviewer, which the Entity hired to evaluate CIP-014-2 R4 and R5. Their recommendations, administrative in nature, pertained only to the structure or documentation conveyed in the reports and did not affect the Entity's current physical security design or equipment to be implemented at any of the [REDACTED] CIP-014 sites in-scope. At that time, the CIP-014 Project Manager issued an email to [REDACTED] senior management requesting acceptance of the recommendations.</p> <p>On October 31, 2016, the Entity updated its CIP-014-2 R4 and R5 documents based upon the accepted third-party reviewer recommendations, which was 78 days after the required due date of August 14, 2016.</p> <p>For the Entity's [REDACTED] sites that are in-scope for CIP-014, the Entity conducted an extent-of-condition assessment and discovered another three recommendations from a site's 30-month review, dated April 4, 2018, that was not documented within the 60-day timeframe in accordance with P6.3. The update to the security plan was completed on June 11, 2018, 68 days after the completion of the 30-month review, and eight days after the required due date of June 3, 2018. The three recommendations were also administrative in nature and had no effect on the security approach for the affected location.</p> <p>This noncompliance started on August 15, 2016, when the Entity failed to implement the recommendations of the unaffiliated third-party review within 60 days of completion, and ended on June 11, 2018, when the Entity updated its final documents, as recommended by the unaffiliated third-party review, dated April 4, 2018.</p> <p>The cause of this noncompliance was a management oversight for failing to implement a procedure that documented roles and responsibilities and controls to ensure compliance with CIP-014 R4-R6.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to implement the third-party evaluation recommendations created a potential for inadequate physical security plans or an insufficient evaluation of the potential threats and vulnerabilities of a physical attack that covers their respective [REDACTED]. However, in this instance, the recommendations were administrative in nature and did not impact the physical security design or equipment. Additionally, there were no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential violation. No harm is known to have occurred.</p> <p>SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity</p> <ol style="list-style-type: none"> 1) implemented the changes recommended by the third-party reviewer into the R4 and R5 documentation for all [REDACTED] CIP-014-2 in-scope sites; 2) developed a versioning table in the CIP-014 R4 and R5 documentation, and [REDACTED] took control of the R4 and R5 master documents from the third-part reviewer; 3) developed an internal program management procedure for compliance with CIP-014 R4-R6 in order to document roles and responsibilities and controls for [REDACTED]; 4) provided training to applicable [REDACTED] employees on CIP-014 R4-R6; and 5) developed a mechanism to track and monitor compliance timelines for CIP-014 R4-R6. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2019022268	CIP-004-6	R4, P4.1	[REDACTED]	[REDACTED]	06/06/2019	07/08/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 26, 2019, the Entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-004-6 R1, P 4.1. The Entity granted 12 employees unescorted physical access into Physical Security Perimeters (PSPs) that was not needed.</p> <p>On June 6, 2019, an Entity employee who had authorized unescorted physical access to PSPs left his corporate-issued badge at home. As a result, the Entity issued the employee a temporary corporate badge with the same access rights as his corporate-issued badge pursuant to the Entity’s operating procedures. However, the Entity failed to utilize the “set to expire” field for the access rights, therefore, the unauthorized physical access rights on the temporary corporate badge did not automatically deactivate when the employee returned the badge later that day. On June 7, 2019, the same temporary badge was reissued to twelve personnel who were not authorized for unescorted physical access. The Entity discovered the issue on July 8, 2018 and immediately deactivated the temporary corporate badge.</p> <p>The Entity conducted an extent-of-condition that consisted of a review of the internal access-related logs and information for the timeframe from June 7, 2019 to July 8, 2019. The 12 employees who retained the temporary corporate badge did not enter any PSPs, as they were not made aware of the additional access rights provisioned on the temporary corporate badge.</p> <p>This noncompliance started on June 6, 2019, when the Entity failed to deactivate the access rights on the temporary badge, and ended on July 8, 2019, when the badge access rights were deactivated.</p> <p>The cause for this noncompliance was inadequate training. The training covered the required tasks in the procedures but the quality of training was inadequate to fully address work methods and expectations of personnel.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. There was no indication that the employees were aware of the additional access rights provisioned on the temporary corporate badge, and none of the employees attempted to access a PSP. Furthermore, the PSPs, which the temporary badge provided access to, were protected with one or more of the following access and monitoring related protections: (i) ingress and egress logging; (ii) 24/7 physical presence within the PSP; (iii) PSP entrances were monitored by camera; (iv) Cyber Assets within PSPs required additional electronic access authorizations; (v) 24/7 security guard monitoring; and (vi) PSPs protected within secured outer perimeter. No harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1. removed the unescorted physical access rights from the temporary corporate badge; 2. temporarily suspended the practice to add unescorted physical access rights to corporate temporary badges while reviewing identified issue; all personnel were notified of the suspended practice; 3. notified all personnel of the official change in practice regarding the addition of unescorted physical access rights to corporate temporary badges. The change includes: <ol style="list-style-type: none"> (i) If an employee forgets a badge at home and is in a critical position or access is time sensitive, as determined by the employee’s direct supervisor, the employee can contact the [REDACTED] to have a new replacement badge issued. The old badge will be disabled and returned to the [REDACTED] the following business day for destruction. (ii) If an employee forgets the badge at home and does not need access to a PSP that day, the employee should relocate to a non-PSP location within the campus to complete work ; (iii) In all other instances, the employee should return home and retrieve their badge; and 4. evaluated related procedural documentation and revised as necessary; and 5. trained responsible personnel on the revised documentation and general awareness of the Entity’s responsibility under CIP-004. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019022217	CIP-004-6	R2	[REDACTED] (the "Entity")	[REDACTED]	09/01/2018	02/11/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 16, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R2.3. According to the Entity, for one individual, it failed to require completion of the training specified in CIP-004-6 R2.1 at least once every 15 calendar months.</p> <p>This noncompliance started on September 1, 2018, which is the first day that is more than one calendar day after the 15 calendar month deadline was reached and ended on February 11, 2019, when the user completed the Entity's CIP-004-6 R2.1 training.</p> <p>The root cause of this noncompliance was a deficient technical control. The Entity has technical controls in place notify staff responsible for revoking access when training has expired. Due to a logic error in the Entity's technical control a situation could occur where a revocation notice is not sent for users with expired training. This situation occurred and subsequently resulted in a failure to revoke access.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk in failing to require the completion of CIP-004-6 R2.1 training content at least once every 15 calendar months is users may be unaware of changes to the Entity's cyber security policies, physical access controls, electronic access controls, visitor control program, the handling of BES Cyber System Information, Cyber Security Incident response plan, recovery plans, response to Cyber Security Incidents, and Cyber Security risks associated with Transient Cyber Assets or Removable Media.</p> <p>Aggravating risk factors as they relate to the Entity:</p> <ol style="list-style-type: none"> 1) The Entity owns [REDACTED] Control Centers that each contain High Impact BES Cyber Systems; 2) The Entity's system includes elements of a [REDACTED]; 3) The Entity's [REDACTED]; 4) The Entity [REDACTED]; and 5) The Entity [REDACTED] to provide voltage control. <p>The risk posed by these instances of noncompliance is reduced by the following factors:</p> <p>The mitigating factors as they relate to the Entity:</p> <ol style="list-style-type: none"> 1) The Entity's service territory is divided into [REDACTED]. 2) The Entity's UFLS Load [REDACTED]. <p>The mitigating factors as they relate to the issues:</p> <ol style="list-style-type: none"> 1) The user had been approved for CIP access; 2) The user had received CIP-004-6 R2.1 training in the past; and 3) The user had a current Personnel Risk Assessment. <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity completed a Mitigation Plan with the following actions:</p> <ol style="list-style-type: none"> 1) to end the noncompliance the Entity required the user to complete the Entity's CIP-004-6 R2.1 training; 2) to prevent recurrence of this noncompliance the Entity modified the workflow associated with access revocation; 3) to prevent recurrence of this noncompliance the Entity now performs a quarterly comparison of CIP training reports to access reports to identify users approaching the 15 month training deadline; and 4) to prevent recurrence of this noncompliance the Entity made additional modifications to its technical controls and tested them with CIP access request categories. <p>Texas RE has verified the completion of all mitigation activity associated with the Mitigation Plan.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2020022797	CIP-004-6	R5: P 5.3	[REDACTED]	[REDACTED]	08/04/2019	8/5/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On August 30, 2019, the entity submitted a Self-Log stating that, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R5. Specifically, the entity did not revoke an individual's access to one Bulk Electric System (BES) Cyber System Information (BCSI) storage location by the end of the next calendar day after the employee terminated employment. On August 2, 2019 when the individual terminated employment, neither the former employee's supervisor nor their manager correctly completed the entity's documented access revocation process. Per the entity's documented process, the employee's manager should have initiated the revocation request in the entity's access management system. Instead, the supervisor sent an internal communication to an email address that was not continuously monitored. This issue began on August 4, 2019, when the time frame permitted to complete revocation expired and ended on August 5, 2019, when the entity revoked the terminated employee's access.</p> <p>The root cause of the issue was attributed to a knowledge-based error. Specifically, the terminated employee's supervisor and manager were not adequately trained to submit the revocation request in accordance with the entity's documented access revocation program.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to adequately implement its access revocation program when it failed to revoke one employee's access by the end of the next calendar day following the effective date of the termination action as required by CIP-004-6 R5 Part 5.3.</p> <p>Failure to timely complete access revocation could have resulted in an attempt by the terminated employee to access the BCSI storage location by contacting the entity's technical support team and requesting assistance to remotely access the BCSI. However, the former employee's physical access badge, laptop computer, electronic keys, and all company property was collected prior to their departure. Additionally, the former employee voluntarily terminated employment, and did not attempt to enter the facility after terminating employment. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) revoked the terminated employee's access to the BCSI storage location; 2) provided individualized training to the supervisor and manager; and 3) provided written training to refresh employee familiarity with termination actions and the appropriate steps for performance. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020231	CIP-002-5.1	R1: P1.1; P1.2; P1.3	[REDACTED]	[REDACTED]	7/1/2016	5/2/2018	Spot Check	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>During a Spot Check conducted [REDACTED] WECC determined [REDACTED] as a [REDACTED] had a potential noncompliance with CIP-002-5.1 R1 and R2. Specifically, [REDACTED] had a contractual agreement with another entity (entity A) to perform [REDACTED] functions and the compliance responsibilities for the associated BES Cyber System (BCS), [REDACTED]. During that time, entity A failed to implement its documented process to identify an appropriate impact rating for the BES Cyber System(s) in its [REDACTED], including backup Control Center and associated data centers, as prescribed by R1.i, for the purposes of Parts 1.1 through 1.3. by July 1, 2016, when the Standard and Requirement became mandatory and enforceable.</p> <p>Due to [REDACTED] being registered as a [REDACTED] even though the BCS functions and compliance responsibilities were contractually provided by entity A, a potential noncompliance was identified against [REDACTED] [REDACTED] contractually assumed the [REDACTED] function and compliance responsibility of the [REDACTED] generating units and switched the [REDACTED] functions to [REDACTED] High Impact BCS (HIBCS), which was already determined to be compliant with CIP-002-5.1, thereby ending the noncompliance.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). At the time of the issue, entity A was contractually responsible for performing the [REDACTED] function for [REDACTED] utilizing entity A's BCS. The failing of entity A to correctly identify the impact rating of its BCS resulted in entity A not appropriately implementing protective security measures, commensurate with their impact, which could have led to inadequate or non-existent cyber security controls (CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, and CIP-011-2) and resulted in the compromise or misuse of the BCS.</p> <p>[REDACTED]</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance:</p> <p>On [REDACTED] [REDACTED] assets and responsibilities as a [REDACTED]. As such, the [REDACTED] function is now performed by a new HIBCS owned and operated by [REDACTED] is compliant with CIP-002-5.1 R1.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020232	CIP-002-5.1	R2: P2.1; P2.2	████████████████████	████████	7/1/2016	5/2/2018	Spot Check	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>During a Spot Check conducted ██████████, WECC determined ██████████, as a ██████████ had a potential noncompliance with CIP-002-5.1 R1 and R2. Specifically, ██████████ had a contractual agreement with another entity (entity A) to perform ██████████'s ██████████ functions and the compliance responsibilities for the affected systems, from ██████████. During that time, entity A failed to review the identifications in CIP-002-5.1 R1 and its parts (and update them if there were changes identified) and have its CIP Senior Manager or delegate approve the identifications as required by CIP-002-5.1a R2 Parts 2.1 and 2.2. by July 1, 2016, when the Standard and Requirement became mandatory and enforceable.</p> <p>Due to ██████████ being registered as a ██████████, even though the system functions and compliance responsibilities were contractually provided by entity A, a potential noncompliance was identified against ██████████. ██████████ contractually assumed the ██████████ function and compliance responsibility of the ██████████ generating units and switched the ██████████ functions to ██████████'s High Impact BCS (HIBCS), which was already determined to be compliant with CIP-002-5.1, thereby ending the noncompliance.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). At the time of the noncompliance, ██████████ was a ██████████ of approximately ██████████. Failing to correctly identify the impact rating of its BES Cyber System resulted in ██████████ not appropriately implementing the protective measures, commensurate with their impact, which lead to inadequate or non-existent cyber security controls (CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, and CIP-011-2) that could have led to compromise or misuse those systems.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance:</p> <p>On ██████████. ██████████ assets and responsibilities as a ██████████. As such, the ██████████ function is now covered by a new BES Cyber System owned and managed by ██████████ is compliant with CIP-002-5.1 R2.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021588	CIP-003-6	R1: P1.2	[REDACTED]	[REDACTED]	09/01/2018	03/14/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On May 20, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-003-6, R1.</p> <p>Specifically, the entity did not obtain CIP Senior Manager review and approval of its CIP Low Impact BES Cyber Security (LIBCS) policy at least once every 15 calendar months. Following the most recent review and approval of its LIBCS policy on May 26, 2017, the entity failed to set a schedule reminder to alert responsible personnel of the need to conduct the review by August 31, 2018. Responsible personnel were not aware of the 15-month review requirement and did not understand the need to timely conduct a review and obtain approval in the absence of a scheduled reminder. This issue began on September 1, 2018, when the LIBCS policy should have been approved and ended on March 14, 2019, when the policy was reviewed and approved.</p> <p>The root cause of the issue was attributed to lack of appropriate scheduling and lack of adequate awareness by responsible personnel.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to review and obtain CIP Senior Manager approval at least once every 15 calendar months of its LIBCS policy for assets identified in CIP-002-5.1 as required by CIP-003-6 R1 Part 1.2.</p> <p>Failure to review and obtain approval could have resulted in cyber security policies that are outdated and do not address new vulnerabilities or risks not addressed by previous versions. However, this was an administrative issue and therefor inherently low risk. The entity continued to implement the policy consistent with CIP-003-6 despite not obtaining the required review and approval in a timely manner. Additionally, the entity owns and operates [REDACTED] containing LIBCS. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) obtained CIP Senior Manager approval of its LIBCS policy; 2) established an Outlook calendar reminder to alert personnel responsible for the review, that the review and approval of the current policy is due; 3) scheduled the annual review as a recurring maintenance task in the entity's management system for December 1 of every calendar year; and 4) reinforced awareness of the 15-month requirement and the company's 12-month cycle through an email to impacted personnel and the CIP Senior Manager. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020164	CIP-010-2	R4	[REDACTED]	[REDACTED]	04/01/2017	01/31/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On July 30, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in potential noncompliance with CIP-010-2 R4. Specifically, on January 24, 2018, the entity discovered that it had not implemented its documented plan to manage [REDACTED] Transient Cyber Assets (TCA). In preparation for the initial performance date of April 1, 2017, the entity documented a process designed to use the automated functionality of its Identity and Access Management (IAM) tool to manage TCAs and track authorizations. However, due to staff changes, the necessary upgrades to the system were not completed in time; instead, the entity implemented a manual process to manage TCAs and did not update its documented plan to reflect its actual strategy to manage and authorize TCAs. This issue began on April 1, 2017, when the Standard and Requirement became mandatory and enforceable and ended on January 31, 2019, when the entity updated its documented plan, for a duration of 671 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls. Specifically, the entity did not implement detective and preventative controls sufficient to identify that its documented plan did not align with the entity's implementation.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to implement its documented plan including the sections in Attachment 1, for [REDACTED] TCAs, as required by CIP-010-2 R4.</p> <p>Such failure could have resulted in employees referencing inaccurate procedural documentation for guidance on how TCAs should be managed and authorized. However, the entity implemented malicious code prevention on all corporate laptops, including TCAs, to reduce the risk of introducing malware to the Cyber Assets to which the TCA would connect. Additionally, the entity required two-factor authentication for access to Physical Security Perimeters associated with High and Medium Impact BES Cyber Systems, which limited access to only authorized individuals. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) updated its documented plan to reflect the manual process used to manage TCAs and the that the use of Removable Media is prohibited in High and Medium Impact BES Cyber System; and 2) created a reminder to annually review all documentation associated with TCAs and Removable Media. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020396	CIP-009-6	R3: P3.1.2; P3.1.3	[REDACTED]	[REDACTED]	09/29/2017 01/30/2018	10/22/2018 02/27/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>During a Compliance Audit conducted [REDACTED], WECC determined that the entity, as a [REDACTED], was in potential noncompliance with CIP-009-6 R3, Part 3.1, subparts 3.1.2 and 3.1.3.</p> <p>Specifically, regarding the first issue identified, the entity conducted a June 30, 2017 test of its [REDACTED] recovery plan that resulted in documented lessons learned. Although required by subparts 3.1.2 and 3.1.3 to update the [REDACTED] recovery plan with the documented lessons learned and notify personnel with roles defined in the plan of the updates within 90 days of the test (September 28, 2017), the entity did not do so until October 22, 2018, for a total of 389 days.</p> <p>For the second issue identified, the entity conducted an October 31, 2017 test of its Supervisory Control and Data Acquisition (SCADA) recovery plan that resulted in documented lessons learned. Although required by subparts 3.1.2 and 3.1.3 to update the SCADA recovery plan with the documented lessons learned and notify personnel with roles defined in the plan of the updates within 90 days of the test (January 29, 2018), the entity did not do so until February 27, 2018, for a total of 29 days.</p> <p>The root cause of the issues was attributed to supervision that did not take the appropriate actions to monitor the task progress or status, exacerbated by the team lead position being vacant for approximately 11 months at the time the noncompliance occurred.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to update two recovery plans to include documented lesson learned and failed to notify personnel with defined roles in the recovery plans of the updates within 90 days following recovery plan tests that resulted in documented lessons learned, as required by CIP-009-6 R3 Part 3.1 subparts 3.1.2 and 3.1.3.</p> <p>Such failure could have resulted in the entity not having recovery procedures that reflect all steps necessary to restore operations, resulting in delays in resuming services. However, as compensation, recovery plans were in place and the violations were primarily matters of documentation. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) updated both recovery plans and notified personnel that updates were made; 2) provided CIP-009 training to all information technology personnel; and 3) hired a new team lead with responsibility for testing and updating recovery plans and notifying personnel of updates. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019020954	CIP-009-6	R3: P3.1.2; P3.1.3			09/29/2017 01/30/2018	10/22/2018 02/27/2018	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 violation.)			<p>On January 16, 2019, the entity submitted a Self-Report stating that, as a _____, it was in potential noncompliance with CIP-009-6 R3. Specifically, regarding the first issue identified, the entity conducted a June 30, 2017 test of its _____ recovery plan that resulted in documented lessons learned. Although required by subparts 3.1.2 and 3.1.3 to update the _____ recovery plan with the documented lessons learned and notify personnel with roles defined in the plan of the updates within 90 days of the test (September 28, 2017), the entity did not do so until October 22, 2018, for a total of 389 days.</p> <p>For the second issue identified, the entity conducted an October 31, 2017 test of its Supervisory Control and Data Acquisition (SCADA) recovery plan that resulted in documented lessons learned. Although required by subparts 3.1.2 and 3.1.3 to update the SCADA recovery plan with the documented lessons learned and notify personnel with roles defined in the plan of the updates within 90 days of the test (January 29, 2018), the entity did not do so until February 27, 2018, for a total of 29 days.</p> <p>The root cause of the issues was attributed to supervision that did not take the appropriate actions to monitor the task progress or status, exacerbated by the team lead position being vacant for approximately 11 months at the time the noncompliance occurred.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to update two recovery plans to include documented lesson learned and failed to notify personnel with defined roles in the recovery plans of the updates within 90 days following recovery plan tests that resulted in documented lessons learned, as required by CIP-009-6 R3, Part 3.1, subparts 3.1.2 and 3.1.3.</p> <p>Such failure could have resulted in the entity not having recovery procedures that reflect all steps necessary to restore operations, resulting in delays in resuming services. However, as compensation, recovery plans were in place and the violations were primarily matters of documentation. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) updated both recovery plans and notified personnel that updates were made; 2) provided CIP-009 training to all information technology personnel; and 3) hired a new team lead with responsibility for testing and updating recovery plans and notifying personnel of updates. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019020953	CIP-009-6	R3: P3.1.2; P3.1.3			09/29/2017	10/22/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On January 16, 2019, the entity submitted a Self-Report stating that, as a _____, it was in potential noncompliance with CIP-009-6 R3.</p> <p>Specifically, the entity conducted a June 30, 2017 test of its _____ recovery plan that resulted in documented lessons learned. Although required by subparts 3.1.2 and 3.1.3 to update the recovery plan with the documented lessons learned and notify personnel with roles defined in the plan of the update within 90 days of the test (September 28, 2017), the entity did not do so until October 22, 2018, for a total of 389 days.</p> <p>The root cause of the issue was attributed to supervision that did not take the appropriate actions to monitor the task progress or status, exacerbated by the team lead position being vacant for approximately 11 months at the time the noncompliance occurred.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to update a recovery plan to include documented lesson learned and failed to notify personnel with defined roles in the recovery plan of the update within 90 days following a recovery plan test that resulted in documented lessons learned, as required by CIP-009-6 R3, Part 3.1, subparts 3.1.2 and 3.1.3.</p> <p>Such failure could have resulted in the entity not having recovery procedures that reflected all steps necessary to restore operations, resulting in delays in resuming services. However, as compensation, a recovery plan was in place and the violation was primarily a matter of documentation. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) updated the recovery plan and notified personnel that the update was made; 2) provided CIP-009 training to all information technology personnel; and 3) hired a new team lead with responsibility for testing and updating recovery plans and notifying personnel of updates. 					

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	MRO2019022432	Yes	Yes	Yes	Yes									Category 2 – 12: 2 years
2	MRO2019022436			Yes	Yes									Category 2 – 12: 2 years
3	MRO2019021529			Yes	Yes									Category 2 – 12: 2 years
4	SPP2018019308			Yes	Yes									Category 2 – 12: 2 years
5	MRO2019022107			Yes	Yes									Category 2 – 12: 2 years
6	MRO2019022026			Yes	Yes									Category 2 – 12: 2 years
7	MRO2019021947			Yes	Yes					Yes				Category 2 – 12: 2 years
8	SERC2018019455			Yes	Yes					Yes				Category 2 – 12: 2 years
9	SERC2018019512	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
10	NCEA2019022275			Yes	Yes					Yes				Category 2 – 12: 2 years
11	NCEA2019022276			Yes	Yes									Category 2 – 12: 2 years
12	NCEA2019022278			Yes	Yes									Category 2 – 12: 2 years
13	NCEA2019022279			Yes	Yes				Yes					Category 2 – 12: 2 years
14	NCEA2019022313			Yes	Yes					Yes				Category 2 – 12: 2 years
15	NCEA2019022280			Yes	Yes				Yes	Yes				Category 2 – 12: 2 years
16	NCEA2019022281			Yes	Yes				Yes					Category 2 – 12: 2 years
17	NPCC2019022250			Yes	Yes						Yes			Categories 3 – 4: 2 years Category 10: 3 years
18	NPCC2019021859	Yes		Yes	Yes									Category 1: 3 years Categories 3 – 4: 2 years
19	NPCC2019021860	Yes		Yes	Yes									Category 1: 3 years Categories 3 – 4: 2 years
20	NPCC2019021861	Yes		Yes	Yes									Category 1: 3 years Categories 3 – 4: 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)
21	RFC2019021685	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years.
22	RFC2019022483	Yes	Yes	Yes	Yes									Category 1: 3 years; Category 2-12: 2 years.
23	RFC2019021565	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years.
24	RFC2018019699	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 years
25	RFC2018019700	Yes		Yes	yes						Yes			Category 1: 3 years; Category 2 – 12: 2 years
26	RFC2018019697	Yes		yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 years
27	RFC2018019701	Yes		Yes	Yes	Yes					Yes			Category 1: 3 years; Category 2 – 12: 2 years
28	SERC2018019031			Yes	Yes					Yes				Category 2 – 12: 2 year
29	SERC2018020055			Yes	Yes								Yes	Category 2 – 12: 2 year
30	SERC2019021812			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
31	SERC2019022069			Yes	Yes					Yes				Category 2 – 12: 2 year
32	SERC2018019635			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
33	SERC2018019988			Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
34	TRE2019020987			Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
35	TRE2019020986		Yes	Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
36	TRE2017018200	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
37	TRE2019022152			Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
38	TRE2019022153			Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
39	TRE2017017973			Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 year
40	TRE2018019891			Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
41	TRE2018019887			Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
42	TRE2018019888			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)
43	TRE2018019889			Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
44	TRE2018019890	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
45	WECC2018019193	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
46	WECC2018020218	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
47	WECC2018020219	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
48	WECC2018020220	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
49	WECC2018020265	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
50	WECC2019020887	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
51	WECC2018019297			Yes	Yes									Category 2 – 12: 2 years
52	WECC2018019298			Yes	Yes									Category 2 – 12: 2 years
53	WECC2019021157			Yes	Yes									Category 2 – 12: 2 years
54	WECC2019022288			Yes	Yes						Yes			Category 2 – 12: 2 years
55	WECC2019022289			Yes	Yes						Yes			Category 2 – 12: 2 years
56	WECC2019022350			Yes	Yes					Yes				Category 2 – 12: 2 years
57	WECC2018019547			Yes	Yes					Yes				Category 2 – 12: 2 years
58	WECC2018019411			Yes	Yes									Category 2 – 12: 2 years

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022432	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	03/25/2019	07/30/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. [REDACTED] and included three instances of noncompliance where the Entity failed to authorize and document changes that deviate from the existing baseline configuration as required by Part 1.2.</p> <p>For the first instance of noncompliance, the Entity reported that during team discussions, a Subject Matter Expert (SME) identified that for an Electronic Access Control or Monitoring Systems (EACMS) that only performs monitoring function, the Java version was upgraded without proper authorization. The SME was part of an application support group and did not have proper authorization to create the change request. The cause of the noncompliance was that the Entity's process was deficient that it did not ensure to assign the SME to applicable support group, and the SME did not follow the Entity's process for installing the java program. This noncompliance began on March 25, 2019 when Java was upgraded without proper authorization, and ended on March 28, 2019 when the change request was submitted and approved by the manager.</p> <p>For the second instance of noncompliance, that Entity reported that an SME, who was new to working with the product, configured a monitoring application [REDACTED] on a new EACMS application server. As part of the process, the SME was prompted to add domain controller devices (also classified as EACMS) to the application. This involved opening a new port for the newly installed agent to use in communications between the application server and the domain controller devices. On the following day, the Entity's change management system detected the newly opened port and created a task to validate the change. When the validation was performed by the SME responsible for domain controller devices, it was determined that no change request had been approved for the configuration changes to domain controllers. The SME subsequently created a change request on April 9, 2019 that was approved on April 10, 2019. The cause of the noncompliance was that the SME installing the new application server was new to this complex product, and due to inadequate or incomplete training did not follow the Entity's process to open the new ports. This noncompliance began on April 8, 2019, when the ports were opened on the domain controller without proper authorization, and ended on April 10, 2019 when the change request was approved.</p> <p>For the third instance of noncompliance, an Entity SME installed security patches [REDACTED] on one EACMS device and opened a previously submitted change request to document the implementation update. The SME noticed that the submitted change request to install the latest security patches for 25 EACMS devices had not been approved. The cause of the noncompliance was that the SME did not follow the Entity's process for installing the security patches. This noncompliance began on July 30, 2019, when SME installed the security patches on one EACMS, and ended on July 30, 2019, when the change request was approved for all the 25 EACMS.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance was minimal risk because the EACMS device was limited to performing monitoring function, and thus do not perform electronic access controls. Additionally, the issue was limited to one EACMS. Lastly, the resolution for the issue was limited administrative in nature as the Java update was required for secure operation of the device.</p> <p>The second instance was minimal because the EACMS devices were limited to performing monitoring functions and do not perform electronic access controls. Additionally, the issue was limited to two EACMS. Lastly, the resolution of the issue was limited to updating baseline documentation where all the open ports were required for operation, and there were not any open ports that should have been closed</p> <p>The third instance was minimal because the EACMS devices were limited to performing monitoring functions and do not perform electronic access controls. Additionally, the security patches were assessed for applicability and approved for updating the servers. Lastly, the resolution of the issue was limited to updating baseline documentation and the security patch update was required for secure operation of the server.</p> <p>No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) submitted and approved a change request for the Java upgrade; 2) created a combined support group for SME's that support both device and applications and assigned the SME's to the combined group. This allowed the application support SME's to submit the change request; 					

<p>3) had supervisor train the affected SMEs on how the combined support group would work and follow the NERC CIP change workflow; 4) reviewed all support groups and devices for shared responsibilities and assigned them to the new combined support group; and 5) had the application support group update the NERC CIP Process document to address situations in which a change on one device required a change on other devices.</p> <p>To mitigate the second instance of noncompliance, the Entity:</p> <p>1) submitted and authorized a change request to document the update to the EACMS of issue; 2) had a manager review the Entity's baseline update instruction and communication process with the SMEs; 3) had a manager send a follow-up email to the SMEs to confirm the baseline update instruction and communication process discussions; and 3) had the SMEs create new documentation to address the installation procedure for this complex product and clarified that a separate, approved change request is required for the agent installation to any domain controller device.</p> <p>To mitigate the third instance of noncompliance, the Entity:</p> <p>1) approved the submitted change request for the 25 security patches; and 2) distributed email communication to SME's reinforcing that they are responsible to verify that change requests are approved before implementing a change and to follow the workflows.</p>

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022436	CIP-006-6	R1	[REDACTED] (the Entity)	[REDACTED]	07/26/2019	07/29/2019	Self-Log	3/31/2020 Expected Date
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R1. [REDACTED]</p> <p>The Entity reported that a security guard was performing a periodic random patrol within a data center that contains Physical Security Perimeters (PSPs) and found he was able to access a cabinet when he pulled on one of the door handles. The PSPs consist of lockable equipment cabinets with alarms that are activated if a door is opened without using a key. When the guard pulled the cabinet door, it opened and initiated a "forced open" alarm. The guard then reported the incident.</p> <p>The cause of the noncompliance was that a Subject Matter Expert (SME) failed to follow the process of firmly closing and then testing whether the door was locked and fully secured before leaving the area.</p> <p>The noncompliance began on July 26, 2019, when the SME accessed the PSP cabinet door and did not push the door forcefully enough for the locking mechanism to engage, and ended on July 29, 2019, when the door was secured by the guard.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk is minimal because this impacted only one factor (Cabinet door), while the other factor (Data Center entry) was still enforced. The door in question was nested within a data center, which has controlled access; this limits the potential for unauthorized access to any PSP cabinets. Additionally, when the PSP cabinet door was opened, it initiated a forced open alarm alert. Lastly, review of the logs and video recordings from the duration of the noncompliance showed no unauthorized access attempts. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) secured the cabinet door (done by the security guard); and 2) reminded staff about the need to close cabinet doors firmly and then test the lock before leaving the area. <p>To mitigate this noncompliance for reoccurrence, the Entity will complete the following mitigation activity by March 31, 2020:</p> <ol style="list-style-type: none"> 1) will either decommission or move to the PSP cage, the NERC CIP devices currently residing in the PSP cabinet. This will eliminate the possibility of the PSP cabinet door being closed but not secured. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021529	CIP-007-6	R5	[REDACTED] (the Entity)	[REDACTED]	11/03/2017	9/24/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5. [REDACTED] The Self-Log contained two instances of noncompliance.</p> <p>In the first instance of noncompliance, the Entity reported that on September 24, 2018, its System Protection team discovered that for one medium impact BES Cyber Assets (BCA), one password on one access level was not changed within the 15-month time required by CIP-007-6 R5. This device has a hierarchical access scheme whereby access to level two cannot be attempted until access to the previous access level has been successfully achieved. In this instance, the password was last changed on August 3, 2016, and should have been changed on or before November 3, 2017, the next required 15-month password change interval per CIP-007-6 Part 5.6. Passwords on two of three access levels in the device were successfully changed; the third (level two) was not changed. The cause of this instance of noncompliance was a combination of a software error in an application used to automatically change passwords and a failure to review the results of the application, and the Entity failed to follow its documented process regarding password changes as required by CIP-007-6 Part 5.6. This noncompliance began on November 03, 2017, when the password should have been changed, and ended on September 24, 2018, when the password was changed.</p> <p>In the second instance of noncompliance, the Entity also reported that on March 28, 2019, for two Protected Cyber Assets associated with a medium impact BCS residing in a substation, the Entity failed to change four out of eight passwords on hierarchical access levels. The cause of this instance of noncompliance was that during the commissioning of two PCAs, a technician failed to follow the documented process to change default passwords on all levels of a device with a hierarchical password scheme as mandated by CIP-007-6 Part 5.4. This noncompliance began on March 8, 2019, when PCAs were placed in service and ended on March 11, 2019, when the passwords were changed.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>For the first instance, the device at issue was a medium impact device (a protective relay) located in a substation and not a control center. The unchanged level two password at issue had been successfully changed in a previous password change cycle, thus it was not a default password. Additionally, to successfully exploit the noncompliance, knowledge of the level two password was needed, the previous access level password is needed, and one would need the ability to be able to bypass the Entity's multi-factor authentication scheme as well as an Intermediate system or be able to bypass the physical protections protecting the PSP in which the device was located.</p> <p>For the second instance, the PCAs at issue (protective relays) were located in a substation and not a control center. To successfully exploit the noncompliance, knowledge of the password at issue was needed, passwords for two other access levels were needed, and one would need the ability to be able to bypass the Entity's multi-factor authentication scheme as well as an Intermediate System or be able to bypass the physical protections protecting the PSP in which the device was located.</p> <p>No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) changed the affected password; 2) conducted an extent of condition to identify other possible instances and identify the combination of factors which caused the password application to fail; 3) opened a support ticket with the application vendor of the application that failed; 4) updated its operating procedures; 5) added process to ensure that an SME verifies all password changes; and 6) provided guidance on how reviews of annual password changes are to be performed. <p>To mitigate second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) changed the affected passwords; 2) updated departmental operating procedures to include guidance on changing passwords; and 3) held a post-issue review and lessons learned discussion with commissioning and substation maintenance personnel about details of this issue and the procedural changes to operating procedures. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2018019308	CIP-010-2	R3: P3.1	[REDACTED] (the Entity)	[REDACTED]	07/01/2017	05/29/2018	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 28, 2018, the Entity submitted a Self-Certification stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R3, P3.1. [REDACTED]</p> <p>The Entity states that it did not conduct an active or paper vulnerability assessment within the 15 calendar month timeframe as required by R3.1.</p> <p>The cause of the noncompliance was that the Entity failed to follow its documented process to perform a paper or active vulnerability assessment by the initial performance date required by CIP-010-2 P3.1.</p> <p>This noncompliance began on July 1, 2017, when the standard became enforceable, and ended on May 29, 2018, when the vulnerability assessment was completed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per the Entity, the noncompliance did not impact any High Impact BES Cyber Systems. The Entity states that the impacted Medium Impact BES Cyber Systems were protected by all relevant CIP controls at the time of the noncompliance and the duration of the noncompliance was less than one monitoring period. Additionally, per the Guidelines and Technical Basis for CIP-010-2, the rationale for Requirement R3 is to "act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems." CIP-010-2 R3 specifies detective security controls rather than preventive controls. Short-term risks associated with a failure to exercise detective controls are lower than risks associated with a failure to exercise preventive controls. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) created an internal mitigation plan describing the current issue and planned mitigation; 2) performed an active vulnerability assessment; 3) created a plan to address issues discovered by the vulnerability assessment; 4) provided training to affected staff and subject matter experts on applicable policies and procedures; and 5) assigned permanent resources to tasks associated with CIP-010-2 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
MRO2019022107	CIP-006-6	R2	[REDACTED] (the Entity)	[REDACTED]	08/14/2019	08/14/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 22, 2019, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-006-6 R2.</p> <p>The Entity reported that an employee was escorting a guest that did not have authorized unescorted physical access to the BCC. Further, the Entity discovered the employee and guest both entered the PSP, the employee left the PSP on a couple of occasions, leaving the guest to perform IT work in the BCC Server Room which is located within the BCC Physical Security Perimeter (PSP) without an escort.</p> <p>The cause of the noncompliance was that the Entity failed to follow its CIP-006-6 R2.1 process to continuously escort visitors (individuals who are provided access but are not authorized for unescorted physical access) within each PSP.</p> <p>The noncompliance began on August 14, 2019, when the Entity failed to have an individual that was not authorized for unescorted physical access continuously escorted within the Physical Security Perimeter, and ended on the August 14, 2019, after the incident occurred.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity determined this to be minimal risk because the visitor of concern was an employee of the company performing expected work with an authorized individual (escort) who was intermittently leaving (noncontiguous escort) to aid in performing this work. The Entity has third party monitoring to alert for any downtime of the system, which did not occur during the unescorted access. Network ports not in use are disabled, preventing any logical access by the visitor during unescorted access. No deviations from the baselines occurred as a result of this issue. No antivirus notification for malicious code happened as a result of this issue. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) sent quarterly email to all employees with unescorted physical access to medium and high impact Facilities with a reminder of the CIP-006-6 R2.1 Visitor Control Program policy; and 2) held a focused training session to review this event and reinforce the Visitor Control Program policy with all employees who have unescorted 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
MRO2019022026	CIP-007-6	R5	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	03/05/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 12, 2019, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-007-6 R5. The Self-Report included two instances of noncompliance.</p> <p>In the first instance of noncompliance, the Entity reported that it failed to provide protections or 12 Cyber Assets (CA), per R5.7, when a Technical Feasibility Exception (TFE) was submitted, but not approved by the Regional Entity (RE). The Entity had submitted two TFEs for different CA types but for the same requirement subparts and did not realize the RE had requested the Entity to merge the TFEs into one. Because the two TFEs were not combined, only one of the TFEs was approved by the RE. The Entity discovered the issue when gathering evidence for an upcoming Compliance Audit. The cause of this noncompliance was that the Entity failed to follow its process for submitting TFEs when it failed to review the approval and disapproval notifications from the RE. This noncompliance began on July 1, 2016, when the CIP Version 5 standards became enforceable, and ended on March 5, 2019, when the TFE was revised and submitted for approval with all applicable CAs.</p> <p>In the second instance of noncompliance, the Entity reported that it failed to provide protections, per CIP-007-6 R5.1, R5.6, and R5.7, for one CA when it did not add the CA to three existing TFEs upon identifying it as a Physical Access Control System (PACS). The cause of this noncompliance was that the Entity failed to follow its process for updating an existing TFE when a new applicable CA was commissioned but not added to an existing approved TFE. This noncompliance began on May 1, 2018, when the CA was implemented, and ended on March 1, 2019, when the Entity submitted an update to all existing TFEs for approval to its RE.</p>					
Risk Assessment			<p>The noncompliances posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk for both instances was minimal because the Entity determined the mitigating measures described within the TFEs were implemented for all CAs of issue for the duration of the noncompliance. Additionally, for both instances, the noncompliance was documentation-in-nature and were resolved through the update of documentation, rather than implementation of a change to the system. Lastly, the Entity's Control Centers contain medium impact BES Cyber System, and only control and monitor assets that contain low impact BES Cyber Systems. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) submitted and gained approval of an update to TFE which included the CAs of issue; and 2) provided training to Subject Matter Experts (SMEs) on its TFE process including but not limited to applicable TFE standards, TFE request and update process, and responsibilities of the request and update process. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) submitted and gained approval of an update to TFE which included the CA of issue; and 2) provided training to SMEs on its TFE process including but not limited to applicable TFE standards, TFE request and update process, and responsibilities of the request and update 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
MRO2019021947	CIP-010-2	R2	██████████ (the Entity)	██████████	09/15/2018	12/09/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 19, 2019, the Entity submitted a Self-Log stating that, as a ██████████, it was in noncompliance with CIP-010-2 R2. The Self-Log contained two instances of noncompliance where the Entity failed to monitor at least every 35 days for changes to the baseline configuration as required by Part 2.1.</p> <p>For the first instance of noncompliance, the Entity reported that it failed to review the baseline for ██████████ host devices classified as high impact BES Cyber Assets (BCA), which hosted ██████████ providing core energy management system (EMS) services. The cause of the noncompliance was that the Entity’s process did not include sufficient controls to ensure that baseline monitoring was occurring at least every 35 days.</p> <p>This noncompliance began on September 15, 2018, after the 35-day window lapsed, and ended on September 30, 2018, when the baseline configurations were reviewed.</p> <p>For the second instance of noncompliance, the Entity reported that it failed to review the baselines again for the same four virtual machine host devices as in prior instance. The cause of the noncompliance was that the Entity’s process did not include sufficient controls to ensure that baseline monitoring was occurring at least every 35 days.</p> <p>This noncompliance began on December 8, 2018, after the 35-day window lapsed, and ended on December 9, 2018, when the baseline configurations were reviewed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In both instances, the risk was minimal because there was a limited number ██████████ of BCAs impacted. The total duration for the two instances combined was 18 days, which would have limited the exposure risk if an unauthorized change were to have occurred. Additionally, the servers were configured to operate in a “locking mode”, where remote configuration changes cannot be made, unless first allowed through changes made at the physical console. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate both instances of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) performed baseline monitoring of the devices; 2) created a recurring ticket within its change management software to serve as a reminder to perform the baseline review during the 35-day window; 3) created an automated task reminder to remind the assigned individual to perform the review; and 4) built an additional escalation process into the automated task reminder process to ensure increased awareness of approaching due dates. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019455	CIP-002-5.1	R2; R2.1	██████████ (the Entity)	██████████	12/15/2016	1/9/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On March 30, 2018, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-002-5.1 R2.1. The Entity did not update the identifications of Bulk Electric System (BES) Cyber Systems required by CIP-002-5.1a R1 after repurposing ██████████ Protected Cyber Assets (PCAs) to function as BES Cyber Assets (BCAs).</p> <p>On May 6, 2016, the Entity repurposed ██████████ PCAs as ██████████ operator consoles, resulting in a need to reclassify the Cyber Assets as BCAs, but the Entity did not reclassify the PCAs to BCAs on the Entity's CIP Asset Identification List. On December 15, 2016, the Entity conducted its 2016 annual asset review, but did not identify the misclassifications. Consequently, the Entity did not correctly classify these Cyber Assets on the approved 2016 BES Cyber System list, thus failing to update the BES Cyber System list as required. On December 12, 2017, the Entity conducted its 2017 annual asset review, identified the misclassification, and reclassified the Cyber Assets from PCAs to BCAs. On January 9, 2018, the CIP Senior Manager approved the updated BES Cyber System list.</p> <p>The root cause of this noncompliance was a lack of clarity in the newly documented asset review and classification processes, which resulted in failures to adequately review and update the classification of Cyber Assets after changes were made.</p> <p>This noncompliance started on December 15, 2016, when the Entity completed its 2016 annual review and did not update the identifications of the PCAs to BCAs, and ended on January 9, 2018, when the Entity's CIP Senior Manager approved the updated identifications of BES Cyber Systems required by CIP-002-5.1a R1.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to update the identifications to reflect that the PCAs had been repurposed into BCAs could have resulted in the Entity failing to provide the BCAs all required protections under the CIP Standards. However, the Entity provides all of its CIP assets the same level of protection as it does to BCAs, thereby ensuring that the misclassified devices received the required protections. In addition, the Cyber Assets constituted ██████████ of the Entity's CIP assets at the time of the noncompliance. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, ██████████ determined that the Entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliance involved Cyber Assets that were not identified as devices subject to the CIP Standards and thus were not afforded the protections required by the CIP Standards, and a separate failure to conduct an annual review entirely. In this instance, the Entity misclassified the Cyber Assets despite reviewing them annually, but afforded the Cyber Assets the protections required by the CIP Standards.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) Completed an asset review, reclassified the ██████████ Cyber Assets from PCAs to BCAs, updated the BES Cyber System list, and had the CIP Senior Manager sign and approve the updated list; 2) Updated its annual asset review procedure to require documentation of how the Cyber Asset supports reliability and the reason for a 15 minute impact; 3) Updated its CIP asset classification change procedure to address the steps for the reclassification of existing CIP Cyber Assets that have been repurposed; and 4) Notified impacted staff of the updates to the two procedures and had them complete a read-and-sign acknowledgement. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019512	CIP-004-6	R5; Part 5.4	██████████ (the Entity)	██████████	7/1/2016	4/5/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 6, 2018, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-004-6 R5, Part 5.4. The Entity did not remove a contractor's non-shared user account within 30 calendar days of the effective date of the termination action.</p> <p>On March 3, 2015, a contractor was terminated but the contractor's read-only ██████████ account was not removed. The Entity removed the contractor's access to this account, revoked the contractor's unescorted physical access, terminated the contractor's VPN account, and collected the contractor's entity-issued laptop. These actions had the effect of preventing any physical or logical access to all the accounts.</p> <p>The Entity created a work order to remove the account, but the technician assigned the task was unable to locate the account with the group/role access combination as listed in the work order. The technician assumed the account did not exist and marked the ticket complete without deleting the account. The Entity discovered the read-only account during its quarterly review of user access and removed the account on April 5, 2018.</p> <p>The root cause of this noncompliance was a combination of unclear instructions of what to do in the event a ticket had incomplete or conflicting information and an incorrect assumption that closing the ticket without following up with the requester was an acceptable course of action.</p> <p>This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on April 5, 2018, when the Entity completed removal of the contractor's read-only account.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to remove the contractor's read-only account within 30 days of the termination could have allowed an individual to use the account for unauthorized or malicious purposes. However, the contractor's VPN account was terminated and his Active Directory domain account was disabled, preventing him from electronically accessing the read-only account. The contractor's unescorted physical access had also been removed and his entity-issued laptop had been retrieved at the time of his termination, preventing him from physically accessing a computer required to electronically access the account. In addition, the account in question was read-only, limiting the harm that could be done with the account. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, ██████████ determined that the Entity's compliance history should not serve as a basis for applying a penalty because this was an isolated instance in which the Entity missed one step in the removal of access from the contractor while removing most avenues to gain access to the account in question, significantly limiting the potential harm that could occur, and is not indicative of a broader programmatic failure.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) Removed the contractor's account that provided access to the application; 2) Completed a work ticket to add a form involving service requests for the account type in question to the terminations service request system; 3) Updated a process document for access revocation for terminations to include steps conducted by the Entity's compliance group to verify all work orders pursuant to a termination are complete and evidence is attached to the work order, and had relevant staff complete a read and sign acknowledgment; and 4) Added a note to the internal procedure to clarify expected actions needed to be taken by technicians in cases where there is incomplete or conflicting information in the access removal request forms, specifically that the technicians should notify the approver to submit a new request and cancel the initial request, and had relevant staff complete a read and sign acknowledgment. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NCEA2019022275	CIP-004-6	R5; Part 5.1	██████████ (the Entity)	██████████	5/9/2019	5/22/2019	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 27, 2019, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-004-6 R5, Part 5.1. The Entity did not complete the removal of an individual's ability for Interactive Remote Access within 24 hours of a termination action.</p> <p>The Entity sponsor of a contractor failed to notify the Entity's human resources (HR) group of the impending termination of a contractor in time to meet the requirements of the Standard. On April 25, 2019, the company employing the contractor notified the Entity sponsor that the contractor would be voluntarily terminating employment with the company. On May 8, 2019, the individual voluntarily left employment with the contractor. On May 21, 2019, during a discussion unrelated to the contractor, the Entity sponsor realized the contractor had left the company and that the sponsor had not notified the Entity's HR group. On May 22, 2019, the Entity removed the contractor's logical access to ██████████ Bulk Electric System Cyber Assets (BCAs). The contractor did not have any physical access to BCAs. The Entity confirmed that there was no logical access by the contractor during the noncompliance.</p> <p>The root cause of this noncompliance was an oversight by the Entity sponsor of the contractor and a failure to follow documented policy. Although the Entity sponsor had timely notification of the termination of the contractor, he failed to notify the Entity's HR group of the impending termination in time to meet the requirements of the Standard.</p> <p>This noncompliance started on May 9, 2019, 24 hours after the contractor was terminated and the contractor's logical access had not been removed, and ended on May 22, 2019, when the Entity removed the contractor's logical access.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to complete the removal of a contractor's logical access within 24 hours of a termination action could have allowed an individual to use the logical access for malicious purposes. However, the contractor did not access any system during the noncompliance. The individual was a trusted contractor who voluntarily left the company doing work for the Entity. The contractor possessed a current personnel risk assessment and had completed security awareness and CIP Standards training. The Entity employs multiple methods, such as host-based malware prevention and intrusion prevention systems to detect, prevent, and alert on identified malicious activity. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, ██████████ determined that the Entity's compliance history should not serve as a basis for applying a penalty because this was an isolated instance involving a single individual voluntarily leaving their position, with a short duration of 13 days, and is not indicative of a broader programmatic failure.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) Removed the contractor's logical access; 2) Counseled the sponsor of the contractor regarding their responsibility as a sponsor to perform due diligence and immediately notify HR when notified of a contractor's termination; and 3) Had the sponsor read and acknowledge the Entity's policy regarding sponsor responsibilities for physical and logical access for non-Entity 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
NCEA2019022276	CIP-006-6	R1; Part 1.8	[REDACTED] (the Entity)	[REDACTED]	8/7/2019	8/7/2019	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 27, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-006-6 R1, Part 1.8. The Entity did not log entry of each individual with authorized unescorted physical access into each Physical Security Perimeter (PSP).</p> <p>On August 7, 2019, an employee who was authorized for unescorted physical access to the PSP followed a tour group into the PSP without swiping his badge and entering his personal identification number (PIN) at the access control system's badge reader before entering the PSP, and was not logged as a visitor. A few minutes after entering the PSP, the employee realized this issue and notified the security guard of this issue.</p> <p>The root cause of this noncompliance was insufficient attention to documented procedures by the employee.</p> <p>This noncompliance started on August 7, 2019, when the employee did not swipe his badge and enter his PIN before entering the PSP, and ended on August 7, 2019, when the employee notified the security guard of the issue.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to log the entry of an employee into a PSP could result in decreased physical security for Bulk Electric System Cyber Systems and make it difficult to identify potentially responsible individuals if an incident occurred within the PSP. However, the employee was authorized for unescorted physical access to the PSP, had been trained, and had a current personnel risk assessment on file. The employee quickly realized that he did not follow the required procedures after entering the PSP and notified a security guard. The employee's identity as well as date and time of entry into and exit from the PSP was confirmed by security video. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, [REDACTED] determined that the Entity's compliance history should not serve as a basis for applying a penalty because this was an isolated instance in which a single individual authorized for unescorted physical access to the PSP following a tour group into the PSP without first swiping his badge and entering his PIN, and is not indicative of a broader programmatic failure.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) Counseled the employee regarding the need to use two-factor authentication when entering a PSP and the prohibition on tailgating into a PSP; and 2) Had the employee complete the PSP access training as a refresher. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NCEA2019022278	CIP-006-6	R2; Part 2.2	██████████ (the Entity)	██████████	4/8/2019	6/21/2019	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 27, 2019, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-006-6 R2, Part 2.2. The Entity did not document all the required information in its visitor logs.</p> <p>In five separate instances, security guards outside of a Physical Security Perimeter (PSP) failed to complete various portions of a visitor's log, specifically the visitor's entry time and name of the escort. The security guards were trained and aware of the expected procedures. The Entity discovered these issues via a regular review of visitor logs by the Entity's compliance group.</p> <p>The root cause of this noncompliance was a lack of familiarity with a newly implemented automated logging system that caused confusion for those logging visitors and a lack of a mechanism to check for errors or omitted information.</p> <p>This noncompliance started on April 8, 2019, the first instance in which the Entity did not document all required information in its visitor logs, and ended on June 21, 2019, the last instance in which the Entity did not document all required information in its visitor logs.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to document all required information in its visitor logs could have resulted in the delayed identification of or inability to identify individuals visiting a PSP if needed during an investigation of a malicious or suspicious event. However, in all instances, the visitors were continuously escorted by an individual with authorized, unescorted physical access for the duration of the visit. The Entity was able to determine the time of entry into and exit from the PSP in each instance using security video and was able to determine escort names using logs for visitor escort within the Entity's office building. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, ██████████ determined that the Entity's compliance history should not serve as a basis for applying a penalty because this noncompliance was identified via an internal control in which the Entity's compliance group was reviewing all visitor logs on a regular basis, occurred shortly after the Entity implemented a new automated logging system in order to reduce the likelihood of future logging failures, and is not indicative of a broader programmatic failure.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) Removed one of the security guards from his post and dismissed him from working at the Entity; 2) Counseled another security guard regarding due diligence when logging visitors and the consequences of failing to do so; 3) Simplified the visitor management system's interface by consolidating multiple escort fields into a single escort field in the system to eliminate confusion; 4) Installed monitors at the PSP security desks that allow security guards to ask escorts to review and confirm that visitor and escort information entered into the visitor logging system is correct; and 5) Had security guards complete read-and-sign tasks of new post orders. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NCEA2019022279	CIP-007-6	R2; Part 2.2	██████████ (the Entity)	██████████	3/11/2019	3/25/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 27, 2019, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-007-6 R2, Part 2.1. ██████████ determined that the noncompliance was more appropriately addressed under CIP-007-6 R2, Part 2.2. The Entity did not evaluate security patches for applicability for a single Protected Cyber Asset (PCA) server at least once every 35 calendar days.</p> <p>On February 8, 2019, the Entity changed the status of a PCA in its asset management system to decommissioned. On February 11, 2019, the Entity changed the status of the PCA in its baseline configuration tool to decommissioned. However, the Entity did not actually decommission the PCA and remove it from the Electronic Security Perimeter (ESP) on either date. The Entity last evaluated security patches for applicability for the PCA on February 3, 2019, meaning that the Entity should have evaluated security patches for applicability that had been released since the last evaluation again within 35 calendar days, or by March 10, 2019. Due to its decommissioned status in the baseline configuration tool, the Entity did not evaluate security patches for applicability for the PCA within the required timeframe. On March 25, 2019, the Entity discovered the issue during a monthly CIP asset verification, an internal control, and removed the PCA from the network the same day.</p> <p>The root cause of this noncompliance was a lack of clarity regarding the order of steps needed for decommissioning assets, which resulted in tasks being completed in the wrong order and other systems showing the asset as decommissioned when it was still in the ESP.</p> <p>This noncompliance started on March 11, 2019, one day after the Entity exceeded the 35 calendar day limit to evaluate the applicability of security patches for the PCA, and ended on March 25, 2019, when the Entity decommissioned the PCA.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The Entity’s failure to evaluate security patches for applicability at least once every 35 calendar days for a PCA could result in security vulnerabilities going unpatched or otherwise unmitigated. However, this asset was a PCA with only monitoring capabilities and was not critical to the reliability of the BPS. The duration of the missed patch assessment was only 14 days. The asset was located within the ESP, which is a tightly controlled network with a number of defense-in-depth measures in place on the network. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, ██████████ determined that the Entity’s compliance history should not serve as a basis for applying a penalty because this noncompliance was an isolated instance discovered via a monthly internal control and the Entity corrected the issue on the same day it was discovered. This noncompliance had a short duration of 14 days and is not indicative of a broader programmatic failure.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) Decommissioned the PCA and removed it from the ESP network; 2) Revised its server decommission procedure to require that assets are shut down and removed from the ESP network before completing the remaining tasks. The revised procedure assigns the responsibility for removing an asset from the asset management system and baseline configuration tool to the Entity’s ██████████ group. The Entity’s decommission tickets now include a task for the assigned group to verify that the server has been removed from the ESP and then update the asset status in the asset management system to “decommissioned.” Once complete, the assigned group notifies the requester on the ticket and/or the baseline owner, if not the same, of the updated status. These revisions ensure that the assigned group verifies that the asset has been decommissioned and removed from the ESP before it is also removed from the asset management system and the baseline configuration tool; and 3) Informed relevant staff of the revised procedure and required them to complete a read-and-sign task. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NCEA2019022313	CIP-007-6	R2; Part 2.3	██████████ (the Entity)	██████████	3/12/2019	3/15/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 4, 2019, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-007-6 R2, Part 2.3. The Entity did not create a dated mitigation plan within 35 calendar days of completing the evaluation of the security patch and determining that it could not apply the security patch within the required timeframe.</p> <p>On February 4, 2019, the Entity assessed a security patch that was applicable to ██████ Bulk Electric System (BES) Cyber Assets. The security patch could not be applied to the Cyber Assets within 35 calendar days because other needed software on the Cyber Assets did not support the new version of software, requiring the Entity to document a mitigation plan that mitigated the vulnerabilities addressed by the security patch within 35 days of completing the evaluation. Thus, the Entity had until March 11, 2019 to document its mitigation plan, but it did not document a mitigation plan by that date. On March 15, 2019, the Entity discovered the noncompliance via a weekly script that provides outstanding patches that need to be applied for each Cyber Asset. On the same day, the Entity completed its documentation of a security patch mitigation plan.</p> <p>The root cause of this noncompliance was a lack of clarity regarding less frequent tasks such as documenting a security patch mitigation plan compared to routine activities, and thus Entity staff did not modify how they performed the required task in a timely manner.</p> <p>The noncompliance started on March 12, 2019, one day after the Entity exceeded the 35 calendar day window to document a security patch mitigation plan, and ended on March 15, 2019, when the Entity documented a security patch mitigation plan.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity’s failure to document a security patch mitigation plan within the required timeframe could delay the application of steps to mitigate identified vulnerabilities and thereby increase the risk that a malicious actor could exploit those vulnerabilities. The security patch mitigation plan’s steps were in place during the time in which the dated mitigation plan was not documented. ██████████ of the Entity’s BES Cyber Assets were affected. The duration of noncompliance was only three calendar days. The Entity has a number of defense-in-depth measures in place on its network. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, ██████ determined that the Entity’s compliance history should not serve as a basis for applying a penalty because this was an isolated instance discovered via a weekly internal control and the Entity corrected the issue on the same day it was discovered. This noncompliance had a short duration of three days and is not indicative of a broader programmatic failure.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) Documented a security patch mitigation plan for the applicable security patch; 2) Updated its security patch assessment template to prompt Entity employees who perform security patch assessments to contact appropriate staff for a security patch mitigation plan number when a security patch mitigation plan is required and implemented a new control requiring information technology staff to review and approve all security patch assessments before the Entity’s monthly patch assessment period ends; and 3) Trained relevant employees on the changes at an in-person training session. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NCEA2019022280	CIP-010-2	R1; Part 1.3	██████████ (the Entity)	██████████	2/25/2019	2/25/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 27, 2019, the Entity submitted a Self-Report stating that, as a ██████████ it was in noncompliance with CIP-010-2 R1, Part 1.3. The Entity did not update the baseline configuration for ██████ Protected Cyber Asset (PCA) and ██████ Electronic Access Control or Monitoring System (EACMS) within 30 calendar days of making changes that deviated from the existing baseline configuration.</p> <p>On January 25, 2019, the Entity made changes to ██████ PCA and ██████ EACMS that deviated from the existing baseline configurations and required the Entity to update the baseline configurations by February 24, 2019. The Entity uses a control report that is produced weekly to show baseline configurations that need to be reviewed and updated. On Monday, February 25, 2019, the Entity’s control report informed subject matter experts that the deadline for updating the baselines was Sunday, February 24, 2019. The Entity subsequently updated the baseline configurations on February 25, 2019.</p> <p>The root cause of this noncompliance was a failure to clearly assign responsibility for completing the update on the particular assets involved and a lack of an escalation process to management to ensure the work was done on time.</p> <p>This noncompliance started on February 25, 2019, one day after the Entity exceeded the 30 calendar day limit to update the baseline configurations for the Cyber Assets, and ended on February 25, 2019, when the Entity updated the baseline configurations for the Cyber Assets.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity’s failure to update the baseline configuration for the ██████ Cyber Assets within the required timeframe could result in the failure to identify unauthorized changes to the Cyber Assets or delays in the restoration of the Cyber Assets’ full functionality during recovery procedures. However, the Entity discovered the noncompliance a day after it began via an internal control used on a weekly basis, limiting the potential duration of the noncompliance. After discovering the noncompliance, the Entity promptly updated the baseline configurations the same day. Although there was a delay in the administrative step of promoting the baselines, the changes were expected and approved prior to the deadline. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, ██████ determined that the Entity’s compliance history should not serve as a basis for applying a penalty because this noncompliance was an isolated instance discovered via a weekly internal control and the Entity corrected the issue on the same day it was discovered. This noncompliance had a short duration of less than one full day and is not indicative of a broader programmatic failure.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) Updated the baseline configurations for the ██████ Cyber Assets; 2) Implemented an enhanced and automated escalation process improvement in which responsible staff receive daily notifications when there is a baseline exception that is 15 calendar days or older and needs to be processed. These automatic notifications are sent to affected employees and, based on the timeline, will also be sent to the employee’s manager, director, ██████████ CIP Senior Manager, and the compliance group; and 3) Notified impacted staff of these changes. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NCEA2019022281	CIP-010-2	R2; Part 2.1	[REDACTED] (the Entity)	[REDACTED]	3/2/2019	3/25/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On September 27, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-010-2 R2, Part 2.1. The Entity did not monitor at least once every 35 calendar days for changes to the baseline configuration for a single Protected Cyber Asset (PCA) server within an Electronic Security Perimeter (ESP).</p> <p>On February 8, 2019, the Entity changed the status of a PCA in its asset management system to decommissioned. On February 11, 2019, the Entity changed the status of the PCA in its baseline configuration tool to decommissioned. However, the Entity did not actually decommission the PCA and remove it from the ESP on either date. The Entity last monitored the PCA for changes to its baseline configuration on January 25, 2019, meaning that the Entity should have monitored it again within 35 calendar days, or by March 1, 2019. Due to its decommissioned status in the baseline configuration tool, the Entity did not monitor the PCA for changes to its baseline configuration within the required timeframe. On March 25, 2019, the Entity discovered the issue during a monthly CIP asset verification, an internal control, and removed the PCA from the network the same day.</p> <p>The root cause of this noncompliance was a lack of clarity regarding the order of steps needed for decommissioning assets, which resulted in tasks being completed in the wrong order and other systems showing the asset as decommissioned when it was still in the ESP.</p> <p>This noncompliance started on March 2, 2019, one day after the Entity exceeded the 35 calendar day limit to monitor the PCA for changes to the baseline configuration, and ended on March 25, 2019, when the Entity decommissioned the PCA.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The Entity’s failure to monitor at least once every 35 calendar days for changes to the baseline configuration for a PCA could result in intentional or inadvertent changes to the baseline configuration going unnoticed and uninvestigated for an extended period. However, this asset was a PCA with only monitoring capabilities and was not critical to the reliability of the BPS. The duration of the missed monitoring of the baseline configuration was limited to 23 days, and there were no changes applied to the asset during that time. The asset was located in the ESP, which is a tightly controlled network with a number of defense-in-depth measures in place on the network. No harm is known to have occurred.</p> <p>The Entity has relevant compliance history. However, [REDACTED] determined that the Entity’s compliance history should not serve as a basis for applying a penalty because this noncompliance was an isolated instance discovered via a monthly internal control and the Entity corrected the issue on the same day it was discovered. This noncompliance had a short duration of 23 days and is not indicative of a broader programmatic failure.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) decommissioned the PCA and removed it from the ESP network; 2) revised its server decommission procedure to require that assets are shut down and removed from the ESP network before completing the remaining tasks. The revised procedure assigns the responsibility for removing an asset from the asset management system and baseline configuration tool to the Entity’s [REDACTED] group. The Entity’s decommission tickets now include a task for the assigned group to verify that the server has been removed from the ESP and then update the asset status in the asset management system to “decommissioned.” Once complete, the assigned group notifies the requester on the ticket and/or the baseline owner, if not the same, of the updated status. These revisions ensure that the assigned group verifies that the asset has been decommissioned and removed from the ESP before it is also removed from the asset management system and the baseline configuration tool; and 3) informed relevant staff of the revised procedure and required them to complete a read-and-sign task. 					

Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019022250	CIP-005-5	R1.3	[REDACTED]	[REDACTED]	07/18/2018	09/25/2019	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted per an existing multi-region registered entity agreement from [REDACTED], NPCC determined that [REDACTED] (the entity), as a [REDACTED], was in noncompliance with CIP-005-5 R1 (1.3). The entity failed to provide the reason for granting access of inbound and outbound access permissions.</p> <p>The entity failed to include a reason for granting access of inbound and outbound access permissions for eight access permissions and did not provide a clear reason for two additional access permissions. In July 2018, the entity performed an upgrade of its Electronic Access Control or Monitoring System (EACMS) that required the addition of hundreds of new firewall policies to support the new EACMS infrastructure.</p> <p>This noncompliance started on July 18, 2018, when the entity added new firewall policies to support new EMS infrastructure. The noncompliance ended on September 25, 2019, when the entity added justifications to the firewall policies that were missing and clarified the ones that were unclear.</p> <p>The root cause of this noncompliance was an insufficient document control process. The entity did not have a system in place that technically required justifications when configuring new firewall policies and there was no system in place to review the justifications once completed.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, failing to provide justifications (or clearly stated justifications) for access permissions may lead to misunderstandings about what systems are intended to communicate with other systems, allowing rogue connections to penetrate undetected.</p> <p>However, this noncompliance was largely a documentation issue. The missing and insufficient justifications did not impact the firewall policies to operate as intended. All active firewall policies were required and in effect despite the noncompliance.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) performed an extent of condition review by reviewing all firewall policies; 2) added justifications to each of the firewall policies that were missing; 3) clarified the policies that had unclear justifications; 4) designed system to technically require justifications for firewall policies; 5) trained employees on detail levels required in justifications; and 6) established an automated system to peer review all firewall policies for completeness and accuracy in a tracking system. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021859	CIP-010-2	R1.	[REDACTED]	[REDACTED]	11/08/2018	04/02/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 19, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-010-2 R1 (1.2, 1.3, 1.4). The entity failed to document changes that deviated from an existing baseline configuration and did not update the baseline configuration within 30 days of the change. The entity also failed to determine cyber security controls that could be impacted by the change or verify that the controls were not adversely affected by the change.</p> <p>As part of a planned system upgrade between November and December of 2018, a change was initiated to open an additional logical network accessible port on devices located within its medium impact substations. The entity opened a new port on its devices in order to communicate with the new system and then de-commissioned the original port. At the time of the configuration change, it was not recognized by the engineer that the devices' baseline was affected. Therefore, the entity's change management process was not followed. The engineer had obtained approval to open the port but did not use the process to fully document the baseline changes.</p> <p>The change management process is utilized on its medium impact Cyber Assets only when it is anticipated that a change will result in a modification to the baseline configuration at a medium substation. Since this newly hired engineer did not anticipate that the baseline needed changing, the engineer did not initiate the process.</p> <p>This noncompliance started on November 8, 2018, when the entity failed to document changes that deviated from the baseline configuration. The noncompliance ended on April 2, 2019, when the entity made its final baseline configuration and documented it.</p> <p>The root cause of this noncompliance was inadequate direction, training and peer reviews provided to a newly hired engineer. Configuration changes to these particular devices had not previously required the use of the change management process to remedy connectivity and troubleshooting activities and lacked the same peer review process as their BES Cyber Asset (BCA) counterparts. The result was a peer check of work that was less than adequate and lacked the necessary controls to prevent a change from moving forward without peer review. Policy guidance and expectations were not well defined or understood and the consequences associated with the change were not adequately reviewed.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The entity's failure to document changes that deviate from the existing baseline or verify its impacts could have led to a degradation in organized control and situational awareness of applied configurations at eight substations.</p> <p>However, the devices in scope [REDACTED] [REDACTED] If the devices were inoperable, reliability would not be affected as RTUs could provide real time assessments.</p> <p>Since this work was planned, approved and performed by in-house engineering, this noncompliance was primarily a process and documentation issue with minimal consequences. All physical and electronic security controls were in place and functioning during the changes to these Cyber Assets. Only planned ports were opened and once this work was completed, the previously opened ports were closed, returning the overall number of open ports to the original number in the baselines for these facilities. The Cyber Assets are also protected behind an Electronic Security Perimeter (ESP) that has restrictive firewall rules that are subject to an access request process. All firewall changes for these devices followed the configuration change management process, which is identified as a preventive control. In addition, these devices are set to send an alarm for failed login attempts operating as a detective control.</p> <p>These Cyber Assets reside within medium impact substation Physical Security Perimeters that have physical access controls. The physical controls [REDACTED] [REDACTED]. In addition [REDACTED].</p> <p>This issue was primarily a documentation issue and largely mitigated upon discovery.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) performed an extent of condition which resulted in no other assets being found as impacted; 2) initiated change management process for all approvals; 3) changed the final baseline configuration only serving the new port; 4) verified baseline configuration and documentation were completed; 5) completed a programming change to allow multiple baseline IDs for equipment that uses the same firmware but has different ports enabled; 6) updated its change management process and change management training materials to better guide new engineers performing this work; and 7) provided additional training to the new engineering resource who implemented the device port changes. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019021860	CIP-010-2	R2.	[REDACTED]	[REDACTED]	03/22/2019	03/22/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 19, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-010-2 R2 (2.1). The entity failed to monitor BES Cyber Systems at least once every 35 days for changes to the baseline configuration.</p> <p>The entity was in the process of implementing new workstations as part of a system upgrade. The entity uses a baseline monitoring tool to monitor, investigate, and document changes to the approved baseline configurations. The implementation of a specific new software should have resulted in new baselines configuration images in the baseline monitoring tool. However, the task that instructs the baseline monitoring tool to examine the baseline configuration for new software was disabled during a troubleshooting session on October 9, 2018 when it began producing errors.</p> <p>The implementation of new software was a baseline change and was documented as a part of change control and authorization. The disabling of the baseline monitoring tool task hindered accurate baseline verification of specific baseline releases (all other baseline aspects were monitored and documented). This resulted in a gap in the automated monitoring of Cyber Asset configuration baselines for the entity's environment.</p> <p>These workstations were considered Protected Cyber Assets (PCAs) from the start date of the noncompliance until January 22, 2019. After the upgrade, they were considered BES Cyber Assets (BCAs).</p> <p>This noncompliance started on November 13, 2018, 35 days from when the entity disabled the baseline monitoring tool task as part of its troubleshooting efforts. The noncompliance ended on March 22, 2019, when the entity discovered the issue and manually executed the task to resume monitoring and documenting.</p> <p>The root cause of this noncompliance was the workflow for baseline reviews needed to include better documentation specific for software baseline monitoring. While all Cyber Assets received security control testing as part of any patch or update, all features and functions of an application such as the baseline monitoring tool did not undergo formalized functional testing and acceptance as part of the change management process.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, failing to monitor at least once every 35 days for changes to the baseline configuration could result in Cyber Assets being changed without the entity's knowledge. Unknown changes could result in exploited, degraded, or inoperable Cyber Assets.</p> <p>However, at the time of the noncompliance, the assets did not perform a reliability task. Once commissioned, the assets would monitor the status of assets and handle their deployment.</p> <p>The entity performs bi-weekly reviews of baseline configurations as part of its CIP Compliance processes. This detective control identified the noncompliance and led to its correction. Additionally, electronic and physical access to these devices was controlled and all baseline changes for these devices followed the change management process.</p> <p>These cyber assets were monitored during the period of noncompliance for changes on all files on the system with the entity's baseline monitoring tool's [REDACTED]. The entity reviews and approves all file additions/changes through a separate process. The entity also employs [REDACTED] in addition to traditional antivirus and system monitoring.</p> <p>These assets reside within an access controlled building which is protected by the entity's defense in depth approach to physical access and is [REDACTED] at all access points. These assets are located within a PSP of the building [REDACTED] to gain access to the room.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) performed an extent of condition; 2) inspected and verified the baseline monitoring tool's profile triggers were functioning; 3) confirmed baseline configurations for all Cyber Assets in the production environment; 4) added additional verification steps to the security controls and functional testing after baseline monitoring tool application updates; and 5) reviewed the commissioning process establishing a QA environment for the commissioning of 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
NPCC2019021861	CIP-007-6	R5.	[REDACTED]	[REDACTED]	12/01/2018	02/26/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>On July 19, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-007-6 R5 (5.6). The entity failed to enforce password changes for four relays that were considered medium impact BES Cyber Assets every 15 calendar months.</p> <p>The entity's current password change process for applicable cyber assets is to include and perform the 15 calendar month password change activity (CIP-007-6.R5.6) as part of the "annual" cyber vulnerability assessment (CVA) per CIP-010-2 R3. The tasks were aligned due to both actions having the same required frequency and similar applicability with the goal of meeting the required time frame for both using the controls set in place.</p> <p>Historically, the entity only used serially wired relays at its Medium impact substations. These serially connected relays (without External Routable Connectivity (ERC)) were not applicable systems to the CIP standards and consequently did not require password changes per CIP-007-6.R5.6 within 15 calendar months. The legacy practice excluded relays from the password change process given they were not applicable assets. The documented approach outlining the steps to take when performing a CVA did not include guidance on actions when new assets were installed and the need to verify and validate their applicability to the standards.</p> <p>As part of a substation upgrade that began in August 2017, the entity installed four new relays at its medium impact substation [REDACTED]. These new relays were installed with ERC and therefore became applicable systems and became within scope of equipment that require password changes within every 15 months. Due to the entity's historical connectivity practice [REDACTED] these relays were inadvertently not included in the list for passwords changes due in the CVA process in 2018.</p> <p>In addition, the four relays were installed just prior to the scheduled 2018 substation CVA, their passwords were not required to be changed at that time. The exclusion of these relays in the password changes during this CVA resulted in putting their 15 month due date out of alignment with the other devices scheduled for password changes. The passwords on these four relays remained unchanged until the next scheduled 2019 CVA. Through the use of an internal control tracking system, the CVA was scheduled to occur within the 15 calendar month of the previous CVA. However, since the four relay passwords had not been changed during the 2018 CVA, the scheduling of the 2019 CVA did not occur within the 15-month interval and the passwords were not changed on time; their passwords were not changed within the 15 calendar month window allowed by the CIP-007-6 standard.</p> <p>This noncompliance started on December 1, 2018, when the first of the relays passed the 15-month requirement for a password change. The noncompliance ended on February 26, 2019, when the entity discovered the issue and changed the passwords.</p> <p>The root cause of this noncompliance was inadequate documentation and training. Another contributing factor was that the internal control tracking system focused on the substations CVA due date and not the individual device password due dates. This was because the method for generating the "list" of assets considered to be "in scope" for password changes was generated from multiple systems of record with no single list containing password ages for all in scope devices.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to change the password within the 15 month interval, if the password had been compromised, it would have been effective longer. Compromise could have led to the relays becoming unavailable, degraded or misused.</p> <p>However, the entity has a defense-in-depth approach with multiple physical and cyber defenses in place during the three-month noncompliance duration. Physical controls include [REDACTED]. There are also [REDACTED] that would have detected someone unauthorized to access the facility. Cyber controls are in place [REDACTED].</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) Performed an extent of condition; 2) Updated passwords on the four relays; 3) Updated and enhanced procedures with stronger language around how and when to change passwords and how to perform a CVA based on lists; 4) Created a process within its action tracking tool that is designed to trigger reminders of upcoming due dates for each individual device and subsequent dates automatically; and 5) Informed staff of changes through updated documentation and 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
RFC2019021685	CIP-003-6	R1	[REDACTED]	[REDACTED]	7/1/2016	12/11/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On June 11, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-003-6 R1.</p> <p>The entity had cyber security policies that addressed Cyber Security Awareness and Cyber Security Incident Response as required for assets containing low impact Bulk Electric System (BES) Cyber Systems. These were approved by the plant manager who was a designated CIP delegate by the entity's CIP Senior Manager as of July 1, 2016. The CIP Senior Manager, however, did not approve the Cyber Security Awareness and Cyber Security Incident Response policies as required by CIP-003-6 R1.</p> <p>The root cause of this noncompliance was an inadequate understanding of CIP-003-6 R1. Specifically, the entity incorrectly believed that a designated CIP delegate was sufficient to approve the Cyber Security Awareness and Cyber Security Incident Response policies. The CIP Senior manager must approve these policies.</p> <p>This noncompliance involves the management practices of reliability quality management and workforce management. Reliability quality management is involved because the entity did not properly define staff roles and responsibilities for NERC CIP compliance. Workforce management is involved because the entity's CIP Senior Manager did not understand that it was his responsibility to approve these policies.</p> <p>This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-003-6 R1 and ended on December 11, 2018, when the entity's CIP Senior Manager approved the Cyber Security Awareness and Cyber Security Incident Response policies.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The failure to have one or more approved policies that address physical security and electronic access for assets containing low impact BES Cyber Systems could result in personnel not having proper direction and guidance when creating the procedures and processes for and implementing various cyber security measures, thereby increasing the likelihood of a deficient security posture. The risk here is minimized because this is mostly a documentation issue; the entity had Cyber Security Awareness and Cyber Security Incident Response policies in place as well as approval from a designated CIP delegate for the duration of the noncompliance. The entity simply failed to have the CIP Senior Manager approve these policies. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity obtained CIP senior manager approval of the cyber security policies immediately upon becoming aware that the approval of those policies could not be delegated. The entity uses [REDACTED] software as a compliance calendar. The entity had not missed obtaining approval, but was instead unaware that the approval had to be made by the CIP senior manager and could not be delegated. The entity will continue to obtain approval once every 15 calendar months, and [REDACTED] will ensure this is complete through automated reminders.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022483	CIP-007-6	R5	[REDACTED]	[REDACTED]	4/6/2018	10/12/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On February 1, 2019, the entity submitted a self-log stating that, [REDACTED] it was in noncompliance with CIP-007-6 R5. On April 6, 2018, a failed entity Medium Impact Bulk Electric System Cyber Asset (BCA) relay (type A) was replaced, but at the time of commissioning, the two default passwords on the device were not changed. Additionally, on October 8, 2018, another relay (Type B) was installed to replace a Medium Impact BCA that failed earlier in the year, but at the time of commissioning, five of the seven default passwords on the device were not changed. Both incidents resulted from the entity failing to follow its program, and change known default passwords as required by CIP-007-6, R5.4.</p> <p>In the first instance, the Compliance group was monitoring for applicable commissioning evidence records. During the review, password change evidence was not received for the device. Following the process, the Compliance group reached out to the Engineering group for a status of the device, and for applicable documentation. The entity determined on April 15, 2018, that the group recently assigned responsibility for changing passwords at commissioning did not change either of the two relay passwords during the commissioning process. On April 19, 2018, the Engineering group changed the two default passwords on the device.</p> <p>In the second instance, the Compliance group was again monitoring for applicable commissioning evidence records. During the review, it was identified that the first level default passwords were changed as required upon commissioning on October 8, 2018, but there was not evidence indicating the change of the remaining 5 levels on this relay type. The Engineering group was contacted to evaluate the documentation, which confirmed the 2-first level passwords were changed, but the remaining 5-second level passwords were not changed. On October 12, 2018, the entity changed the five remaining default passwords.</p> <p>The root cause of the noncompliance was that the handoff of the commissioning responsibility in the entity was not clearly defined nor communicated to all the responsible personnel necessary for an error free transition. In the first instance, the personnel that performed the installation of the device were not aware of the responsibility to change the default passwords, as this was a new requirement for them. In the second instance, the responsible group did change the first level passwords, but since they hadn't been fully and clearly briefed on the program requirements, and had not received the second-level passwords, they did not update the 5-second level passwords, as required. This noncompliance involved the management practices of asset and configuration management and workforce management. Asset and configuration management is involved because the entity failed to properly protect the two Medium Impact BCA relays at the time of commissioning. Workforce management is involved because the entity did not sufficiently define the responsibilities of those who were commissioning the Medium Impact BCA relays.</p> <p>The first instance of the noncompliance began on April 6, 2018, when the entity commissioned the Medium Impact BCA relay without changing the two default passwords, and ended on April 19, 2018, when the entity changed the two default passwords. The second instance of noncompliance began on October 8, 2018, when the entity commissioned the Medium Impact BCA relay without changing five of the seven default passwords, and ended on October 12, 2018, when the entity changed the remaining five default passwords on the device.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. 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. The risk here is minimized because both instances indicate that effective internal controls were in place at the time of the incidents because they were identified and corrected quickly. Additionally, the devices are subject to several layers of protections, commensurate with such accounts on devices located within a CIP-protected environment. Specifically, the relays reside within an Electronic Security Perimeter [REDACTED]. Implemented controls in place at the time of the occurrence reduced the probability of a successful unauthorized access attempt. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) developed and incorporated a checklist for the pre-job walk downs and ensure the identification of a NERC site, and that the password change forms are included; 2) discussed and developed a formal process with training aids for exchanging relay passwords; 3) trained employees on and implemented the new formal process; and 4) conducted three random audits done on projects, performed on employees at a NERC site by relay supervision, to measure the effectiveness of the 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
RFC2019021565	CIP-007-6	R2	[REDACTED]	[REDACTED]	11/2/2018	12/5/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On May 9, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-007-6 R2.</p> <p>On December 4, 2018, the entity's patch scheduling team discovered two different patches that had not been applied within 35 calendar days of the completion of the corresponding patch evaluations. The entity also did not implement or revise a plan to mitigate the vulnerabilities addressed by the patches. The first patch was deemed applicable on September 28, 2019, and the second patch was deemed applicable on October 19, 2018. On December 5, 2018, the entity created mitigation plans for both late patches. The first patch affected six [REDACTED], and the second patch affected two [REDACTED]. All of the affected devices are classified as [REDACTED].</p> <p>The root cause of this noncompliance was the continued existence of, and allowance of access to, an older version of the entity's [REDACTED]. In both instances, after evaluating the patch, the patch analyst mistakenly entered the evaluation into [REDACTED]. The analyst responsible for monitoring the [REDACTED] and creating mitigation plans, where required, was unaware that mitigation plans needed to be created for the two patches, since the [REDACTED].</p> <p>This noncompliance involves the management practices of verification and implementation. Verification was involved because the entity failed to assure that applicable patches were: (a) applied; or (b) addressed via a mitigation plan. Implementation was involved because the entity implemented a [REDACTED] but failed to address the ongoing risks associated with the continued existence of, and access to, the [REDACTED].</p> <p>This noncompliance started on November 2, 2018, when the entity was required to apply the first patch or create or revise a plan to mitigate the vulnerabilities addressed by the patch and ended on December 5, 2018, when the entity created mitigation plans for both late patches.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. Failing to apply a patch or create or revise a plan to mitigate the vulnerabilities addressed by the patch increases the opportunity for those vulnerabilities to be exploited. The risk here was minimized because of existing security controls that were in place to prevent exploitation of the patch vulnerabilities. The controls were implemented prior to the patches being released and were documented in the subsequent mitigation plans (i.e., this noncompliance was largely a documentation issue). The security controls were: (1) firewall protections; (2) access management controls; (3) multi-factor authentication for interactive access; (4) 24/7/365 security monitoring; and (5) strict password policies that include annual password changes. Additionally, the entity quickly identified and corrected the noncompliance, thus limiting the potential for harm. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances involve different facts, circumstances, and/or causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) changed [REDACTED] to remove write access of certain individuals responsible for evaluating security patches for applicability; 2) created mitigation plans for the two patches that were not applied or assigned mitigation plans within 35 days of evaluation; and 3) removed the [REDACTED]. This will help prevent users from entering patches into [REDACTED]. 4) As an additional mitigating activity, the entity removed all remaining access to [REDACTED] for all individuals who had responsibility for evaluating and documenting patches to help prevent recurrence of this 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
RFC2018019699	CIP-007-6	R1	[REDACTED]	[REDACTED]	12/5/2017	4/18/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>[REDACTED] ReliabilityFirst determined that the entity, [REDACTED] was in noncompliance with CIP-007-6 R1 identified during a Compliance Audit [REDACTED]. During the Compliance Audit, ReliabilityFirst discovered that the entity had port ranges set to "ANY" for 4 services on one Physical Access Control Systems (PACS) server. However, only the more narrow port range was required for these services. By setting the ports to "ANY", the entity failed to enable only the logical network accessible ports that have been determined to be needed.</p> <p>The root cause of the noncompliance was an administrative oversight by personnel responsible for implementing new baselines for the PACS server. Entity personnel were aware of the proper port range, but neglected to tighten those ranges after implementing the new baselines. This root cause involves the management practice of reliability quality management, which includes maintaining a system for deploying internal controls.</p> <p>This noncompliance started on December 5, 2017, when the entity implemented the new baselines without tightening the port ranges, and ended on April 18, 2018, when the entity implemented the appropriate port ranges.</p>					
Risk Assessment			<p>ReliabilityFirst determined that the subject noncompliance posed a minimal risk to the reliability of the bulk power system based on the following factors. The risk posed by not setting the ports to the correct range created opportunities for unauthorized access through unidentified open communication channels. This risk was mitigated in this case by the following factors. First, the issue was only identified on a single PACS server, which indicates that this was an isolated oversight and not indicative of a larger issue. Second, the entity had other controls in place on the PACS server to reduce the threat of unauthorized access. For instance, the PACS server was being patched, the entity had methods in place to deter, detect, or prevent malicious code, and the entity uses an automated tool to compare actual asset configurations to baselines on a nightly basis. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity developed and implemented new port configuration for specific services. As an additional mitigating action, the entity also ensured that the updated configurations were properly entered into its automated tool for monitoring in the future.</p> <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019700	CIP-007-6	R2	[REDACTED]	[REDACTED]	7/1/2016	4/18/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>[REDACTED] ReliabilityFirst determined that the entity [REDACTED] was in noncompliance with CIP-007-6 R2 identified during a Compliance Audit [REDACTED]. During the Compliance Audit, ReliabilityFirst issued a request for the entity to provide a complete list of the patch sources being monitored. The entity provided a PDF that provided a list of patch sources and identified its Patch Management Process document where the list is maintained. ReliabilityFirst reviewed the list and discovered that [REDACTED] was not on the software security patch source list, and therefore concluded that the entity was not tracking, evaluating, and installing cyber security patches for applicable Cyber Assets containing [REDACTED].</p> <p>The root cause of the noncompliance was the entity was unaware of this software tool because it was only present on 6 workstations and was rarely used. This root cause involves the management practice of asset and configuration management, which includes controlling changes to assets and configuration items.</p> <p>This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-007-6 R2 and ended on April 18, 2018, when the entity removed the software from the affected workstations.</p>					
Risk Assessment			<p>ReliabilityFirst determined that the subject noncompliance posed a minimal risk to the reliability of the bulk power system based on the following factors. The risk posed by not having [REDACTED] on the patch source list provided the opportunity for infiltration of unauthorized network traffic into the Electronic Security Perimeter (ESP) when security patches and upgrades are not installed on Cyber Assets within the ESP. This risk was mitigated in this case by the following factors. First, software was only ever used for [REDACTED] and was only used on local workstations. Therefore, this software did not present unique attack vectors. Second, though the security patches were available, those patches did not address any significant security vulnerabilities. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) developed and implemented change with unpatched software; 2) developed and implemented change with a whitelist program to ensure that patch management process tool is better utilized to identified gaps and/or deficiencies in the process as a whole; and 3) removed the identified unpatched software. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019697	CIP-010-2	R1	[REDACTED]	[REDACTED]	7/1/2016	7/1/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>[REDACTED] ReliabilityFirst determined that the entity, [REDACTED] was in noncompliance with CIP-010-2 R1 identified during a Compliance Audit [REDACTED]. During the Compliance Audit, ReliabilityFirst identified a potential noncompliance because the entity failed to define 5 controllers as Physical Access Control Systems (PACS). Because the entity did not define these devices as PACS, the entity did not maintain baselines for these devices. Moreover, based on the information provided to ReliabilityFirst during the Compliance Audit, ReliabilityFirst also concluded that, because the entity failed to define these devices as PACS, the entity also failed to provide sufficient evidence to demonstrate that it fully implemented the controls required by other Standards as well such as, CIP-006-6 R1 (Part 1.6 and 1.7), CIP-007-6 R1 (Part 1.1, R2, R3, R4, and R5), CIP-009-6 R1, R2, and R3, and CIP-010-2 R1 (Part 1.2, 1.3, and 1.4) and R3.</p> <p>The root cause of the noncompliance was the entity's incorrect interpretation that, because the devices were serially connected to the PACS server, they did not constitute PACS controllers. This root cause involves the management practice of workforce management, which includes providing training, education, and awareness to employees.</p> <p>This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-010-2 R1 and ended on July 1, 2018, when the entity completed its Mitigation Plan.</p>					
Risk Assessment			<p>ReliabilityFirst determined that the subject noncompliance posed a minimal risk to the reliability of the bulk power system based on the following factors. The risk posed by not labeling the controllers as PACS and not conducting baselines for them is that (a) this failure could have permitted a change to be implemented that could have adversely affected system security; and, (b) the entity would not implement all of the necessary security controls for PACS. This risk was mitigated in this case by the following factors. First, since the PACS controllers are serially connected to the PACS server, someone with malicious intent would need to attack the server first, which was a declared PACS device and afforded all required protections. Second, although the entity could not provide evidence that it had implemented all of the security controls required for PACS, the entity was performing actions that helped reduce the risk. Specifically, the entity was [REDACTED].</p> <p>[REDACTED] No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) ensured that a Vulnerability Assessment has been completed on the PACS; 2) ensured that only logical network accessible ports that have been determined to be needed by the entity, including port ranges or services where needed to handle dynamic ports; 3) ensured that the entity has authorized and documented changes that deviate from the existing baseline configuration; 4) ensured that the plans/processes and systems in place are adequate to monitor each PACS for unauthorized physical access to a PACS; 5) ensured that applicable employees are familiar with Patch Management Process, Malware Protection Process, Security Event Monitoring Process, System Access Control Process; and 6) ensured that all applicable employees are familiar with all plans/processes relating to NERC Standard CIP-009-6. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019701	CIP-011-2	R2	[REDACTED]	[REDACTED]	5/22/2017	4/18/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On May 3, 2018, ReliabilityFirst determined that the entity, [REDACTED] was in noncompliance with CIP-011-2 R2 identified during a Compliance Audit [REDACTED]. During the Compliance Audit, ReliabilityFirst determined that the entity was unable to provide sufficient evidence that, after a failure, the entity destroys cyber asset devices in accordance with the Standard/Requirement.</p> <p>ReliabilityFirst identified several issues with the form the entity used when destroying a hard drive that failed at the [REDACTED]. Specifically, the form provided: (a) did not have a date on the document to establish the time it was filled out and the signature line at the bottom was left blank; (b) failed to provide a specific number in the space designated for the [REDACTED]; and, (c) did not provide an explanation of all of the data that is being provided.</p> <p>The root cause of the noncompliance was the entity's insufficient process documentation related to the destruction of cyber asset hardware. This root cause involves the management practice of reliability quality management, which includes maintaining a system for deploying internal controls.</p> <p>This noncompliance started on May 22, 2017, when the entity completed the form incorrectly and ended on April 18, 2018, when the entity completed its disposal process updates.</p>					
Risk Assessment			<p>ReliabilityFirst determined that the subject noncompliance posed a minimal risk to the reliability of the bulk power system based on the following factors. The risk posed by not properly documenting the destruction of the cyber asset hardware is that it could possibly allow unauthorized access to the Bulk Electric System Cyber System Information. This risk was mitigated in this case by the following factors. First, based on information obtained during the Compliance Audit, ReliabilityFirst was reasonably assured that the hard drive was actually destroyed, and that the only issue is failure to properly record the destruction. Second, even if an unauthorized individual had obtained the hard drive, it would have been difficult to obtain any information from it as it was non-functioning when removed. Third, the entity implemented an additional layer of security for Cyber Asset components that have failed and are slated to be destroyed. [REDACTED] This secure area is located within an existing Physical Security Perimeter that has its own security measures related to access. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) developed and implemented change to the storage location of applicable Cyber Assets prior to their destruction; 2) developed and implemented changes to IT [REDACTED] to decrease deficiencies in its disposal of Cyber Assets; and 3) developed and implemented changes to IT [REDACTED] to decrease deficiencies in its disposal of Cyber Assets including protection of the Cyber Asset before disposal, and creation of adequate records surrounding the disposal itself. <p>ReliabilityFirst has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019031	CIP-010-2	R1, P1.2	[REDACTED]	[REDACTED]	10/05/2017	11/02/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On January 22, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1, P1.2. The Entity had one instance where it failed to authorize and document changes that deviated from the existing baseline configuration.</p> <p>On October 27, 2017, during the Entity's monthly baseline comparison review, an Entity transmission cybersecurity analyst discovered an inconsistency between a documented baseline configuration and the actual configuration on an Electronic Access Control or Monitoring System (EACMS) Cyber Asset. As a result, the Entity initiated a review to determine the cause of the inconsistency. On November 2, 2017, the review ended with the following conclusions: On October 5, 2017, a contractor individual working on behalf of Entity Transmission made a software change to the EACMS asset, and installed two software packages. The contractor made the change without following the Entity's documented change management process and CIP-010-2 R1, P1.2, which required initiating a change request to authorize and document changes that deviated from the existing baseline. On November 2, 2017, the Entity revoked the contractor's electronic access and rolled back the unauthorized configuration change.</p> <p>The Entity determined the extent-of-condition through the application of the internal control utilized for compliance with CIP-010-2 R2. The Entity verified that no other in-scope CIP assets had unauthorized changes.</p> <p>The scope of affected assets in this noncompliance included [REDACTED]</p> <p>This noncompliance started on October 5, 2017, when the contractor changed a configuration without authorizing and documenting the change that deviated from the existing baseline configuration, and ended on November 2, 2017, when the Entity rolled back the configuration change.</p> <p>The cause of this noncompliance was a human performance failure to adhere to the Entity's procedure. The contractor was properly trained, but for an unexplained reason, the contractor made a change that deviated from the existing baseline without first initiating a change request and obtaining approval. The Entity did not reinstate the contractor's or contractor's employees' access, and transferred the work to an internal employee.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to authorize and document a change that deviated from the existing baseline resulted in a decrease in situational awareness of implemented configurations. These degradations could have caused EACMS monitoring to be ineffective, thus provisioning a means for malicious individuals to take over BCAs and potentially disrupt grid operations. However, both software packages installed were already in use on some existing EACMS and both were being tracked for patch management under CIP-007-6 R2. In this instance the Entity conducted a personal risk assessment and training for the contractor. Additionally, access was limited to a single Cyber Asset outside of the Electronic Security Perimeter, which was logically separated from BCAs, and, the EACMS device was running antivirus software. Furthermore, real-time monitoring and alerting was in place for any detected instances of attempted configuration changes or undefined use of ports or services. No harm is known to have occurred.</p> <p>SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked the contractor and associated employees of the contracting company with logical access; 2) conducted a meeting with the contractor, his manager, and all employees of the contractor's company to discuss the breach of procedures; 3) had the contractor and all employees of the contractor's company complete a review of the CIP-010 policies and procedures and provided an attestation; and 4) did not reinstate the contractor's or the contractor's employees' access, and transferred the work to an internal Transmission employee. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018020055	CIP-004-6	R5, P5.1, P5.3	[REDACTED]	[REDACTED]	08/13/2017	02/26/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 20, 2018 (Instance 1) and May 3, 2019 (Instance 2), the Entity submitted Self-Reports stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5, P5.1 and P5.3. The Entity failed to revoke unescorted physical access upon a termination action within 24 hours of the termination action for three employees (P5.1), and failed to revoke access to designated Bulk Electric System (BES) Cyber System (BCS) Information storage locations within 24 hours of the termination for one employee (P5.3).</p> <p>In Instance 1, on April 9, 2018, an operator (employee) involved in testing the implementation of a non-production Supervisory Control and Data Acquisition (SCADA) system, voluntarily terminated his employment with the Entity. On April 20, 2018, an Entity supervisor learned during a conversation with a co-worker that the employee at issue had resigned. The Entity immediately revoked the employee's access rights after learning of the termination, and notified the appropriate department responsible for triggering revocation of all access to the Entity's systems. During the 11th day between the employee's termination and the revocation, the employee's network credentials still existed, but the employee did not attempt to electronically or physically access the non-production SCADA system. The employee only had access to BCS Information and did not have access to a Physical Security Perimeter (PSP) or an Electronic Security Perimeter (ESP). The Entity collected the employee's laptop upon termination, which limited his access capability.</p> <p>On May 3, 2019, the Entity submitted an additional Self-Report of CIP-004-6, designated [REDACTED]. SERC determined that this noncompliance involved the same Standard and Requirement as the original July 20, 2018 Self-Report. Therefore, SERC dismissed and consolidated [REDACTED] with SERC2018020055.</p> <p>In Instance 2, on February 26, 2019, while performing an internal review of the access management program, the Entity discovered that it had not revoked an employee's physical access credentials (i.e. the functionality of his employee badge) within 24 hours of his voluntary termination, effective November 7, 2018. Entity personnel immediately revoked the employee's access credentials that same date and verified it had revoked all other access as required by the Standard. The Entity confirmed in a review of records, that access to the general office building or any PSP after his termination date did not occur with the employee's badge. The Entity revoked access 111 days late.</p> <p>To determine the extent of condition, the Entity reviewed the access rights of all terminated users and determined that it had failed to revoke access for two additional employees. The Entity determined that the two employees' credentials for BCS Information access were not revoked by the end of the next calendar day following their termination. However, their laptops were returned upon termination, which limited their access capability. The Entity revoked access six days late (terminated December 7, 2018, access revoked December 14, 2018) for one, and 12 days late for the other (terminated August 11, 2017, access revoked August 24, 2017).</p> <p>This noncompliance started on August 13, 2017, when, in Instance 2, the Entity did not revoke access to BCS Information by the end of the next calendar day following the employee's termination, and ended on February 26, 2019, when the Entity revoked access to the PSP for the last discovered instance of noncompliance.</p> <p>The cause of this noncompliance was inadequate training related to access revocation. Additional training, which included the development and circulation of a new supplemental training document, was provided to supervisors responsible for access revocation.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to revoke access for terminations within the required 24 hours could allow a terminated individual with ill intentions to make changes to BCS Information or damage equipment in a PSP, potentially impacting the reliability of the BES. However, the employee at issue in Instance 1 was in good standing prior to voluntarily terminating his employment, making it less likely that the individual would have taken actions that were hostile to the Entity's operations, or destructive to the Cyber Assets in place. Likewise, in Instance 2, the three employees at issue had current cyber security training, valid personnel risk assessments, and were in good standing with the Entity. In all instances, no access with the employees' credentials occurred between the date of termination and the revocation of access, and, the Entity negated the employees' ability to electronically access Cyber Assets after termination by collecting their laptops upon termination. In all instances, no harm is known to have occurred.</p> <p>SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked the employees' access; 2) distributed an email to all supervisors to reinforce expectations relating to supervisors' responsibility to notify Human Resources when a termination occurs; 3) developed a document further detailing managers' and supervisors' employment termination requirements. The document was attached to the email sent to managers and supervisors and uploaded to the Entity's intranet for future access by supervisors when needed; 4) communicated to respective supervisors and managers involved to discuss the implications of proper internal notification of terminations; and 5) provided training to personnel responsible for access revocation and stressed the importance of following the established procedures for evidence collection and access 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
SERC2019021812	CIP-004-6	R5, P5.1	[REDACTED]	[REDACTED]	06/28/2019	07/01/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 6, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5, P5.1. The Entity did not implement a process to initiate removal of an individual's unescorted physical access and Interactive Remote Access upon a termination action within 24 hours of the termination action.</p> <p>On July 1, 2019, while reviewing access records following a personnel action, the [REDACTED] discovered that the Entity failed to revoke access within 24 hours for a deceased employee. On July 1, 2019, the Entity revoked the deceased employee's access. On June 27, 2019, the day the employee passed away, the [REDACTED] notified the department's manager of the employee's death. However, department management did not consider death as a "termination action" that required 24-hour processing. The department manager incorrectly interpreted termination actions to only mean those initiated by the employer, even though the CIP Access Management Procedure indicated that "Termination" included termination due to a death.</p> <p>The deceased employee's access was limited to physical and electronic access [REDACTED]. The deceased employee did not have remote electronic access.</p> <p>The Entity has had no other instance where an employee with CIP access has passed away. Therefore, this noncompliance was limited to this single instance.</p> <p>This noncompliance started on June 28, 2019, when the Entity failed to revoke access within 24 hours after the employee's death, and ended on July 1, 2019, when the Entity revoked access.</p> <p>The cause of the noncompliance was ineffective training. The department manager believed that the 24-hour revocation requirement applied only to terminations initiated by the employer. However, the Entity's CIP Access Management Procedure revocation process stated that "Termination" included termination for cause, voluntary resignation, retirement, and death.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to remove physical and electronic access for one employee within 24 hours of termination could allow malicious actors to gain operational control of [REDACTED] BCAs or BCSSs, and cause a degradation in situational awareness or operate BES Elements and Facilities. However, the cause of termination of the employee was death and the employee did not have remote electronic access. As such, anyone attempting to use the employee's credentials would have had to come on-site to gain access. In addition, there was no attempted use of the deceased employee's credentials following the employee's death. Furthermore, the Entity revoked the deceased employee's access only three days after the employee's death. No harm is known to have occurred.</p> <p>SERC considered the Entity's CIP-004-6 R5 compliance history in determining the disposition track. The Entity has two relevant prior instances of noncompliance with CIP-004-6 R5. SERC determined that the Entity's CIP-004-6 R5 compliance history should not serve as a basis for applying a penalty. While the prior instances of noncompliance are relevant, the instant noncompliance poses a minimal risk and warrants Compliance Exception treatment. The mitigating actions for the prior instances of noncompliance focused on training related to employee transfers and vendor termination; therefore, the prior mitigating actions could not have prevented the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked the deceased employee's access; 2) confirmed that the Entity's procedure addresses termination of employees or contractors by death; 3) revised the Entity's training to specifically address how to handle death of an employee or contractor; and 4) trained employees on the new procedure. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2019022069	CIP-006-6	R2, P2.2	[REDACTED]	[REDACTED]	05/16/2017	08/09/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 14, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R2, P2.2. The Entity had seven instances where it did not require manual or automated logging of visitor's entry into and exit from the Physical Security Perimeter (PSP) that included 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.</p> <p>On July 17, 2019, while reviewing electronic access logs, the Entity identified an "Invalid Access Level" event that occurred on June 26, 2019, which showed that an employee not authorized for unescorted access attempted a card scan for entry into a PSP, and, eight seconds later, attempted to scan out of the PSP.</p> <p>The Entity conducted an extent-of-condition assessment by reviewing every "invalid badge read" registered by the Physical Access Control Systems (PACS) that monitored the Entity's PSPs since September 2016. The Entity identified a total of seven instances where an unauthorized employee entered and exited a PSP with an employee with authorized unescorted access ("escort"), but did not sign in or out as a visitor per the Entity's Visitor Management and Control process. These instances occurred between May 16, 2017 and August 9, 2019. The same escort was responsible in two instances, and five different escorts were responsible in the other five instances. These seven instances occurred at [REDACTED]. All persons not authorized for unescorted access to the PSPs at issue were Entity employees who did have authorized unescorted access to other PSPs.</p> <p>This noncompliance started on May 16, 2017, the first instance where the Entity failed to log a visitor into and out of the PSP, and ended on August 9, 2019, the last instance where the Entity failed to log a visitor into and out of the PSP.</p> <p>The causes of this noncompliance was ineffective internal controls and training. The escorts involved in each instance believed that since the employees they were escorting had authorized access to at least one PSP, said employees had access to the PSP at issue in their particular instance. In addition, the escorts stated that no alarm sounded when the unauthorized employee swiped his or her badge, so they proceeded into the PSP without logging a visitor.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to capture physical access logs could diminish its ability to perform forensics or evaluate possible security breaches during the investigative stage of possible misoperations and/or malicious activity. However, all unauthorized employees in the instant noncompliance swiped their badge upon entry and exit and had authorized access to other PSPs. Additionally, each unauthorized employee at issue had a current Personnel Risk Assessment on file, had received the Entity's annual cyber security training, and was participating in the Entity's quarterly security awareness program. No harm is known to have occurred.</p> <p>SERC considered the Entity's CIP-006-6 R2, P2.2 compliance history in determining the disposition track. The Entity has one relevant prior noncompliance with CIP-006-6 R2, P2.2. SERC determined that the Entity's relevant compliance history should not serve as a basis for applying a penalty. The prior noncompliance is not relevant as the circumstances and causes are unrelated to the instant noncompliance, and, the Mitigation Plan would not have prevented or detected the instant noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) enhanced its training to clarify the limits of authorization; 2) conducted training on PSP access procedures for those currently authorized for any PSP access and required this training prior to providing PSP key cards; 3) developed a report that will be given to individuals when first issued their ID cards/key cards with any physical NERC access that lists the specific PSPs to which they are authorized for unescorted access. The Entity will distribute this report to current card holders at least once a year and upon any changes to authorized access; 4) enhanced monthly review of PACS reports to evaluate all invalid reads. In addition to the monthly comparison of hard-copy visitor sign-in/sign-out sheet against PACS reports to confirm compliance with the Entity's procedures for electronic logging, the Entity will review reports to identify any cases of suspected unescorted visitors in the PSPs for all "invalid badge read" events; 5) evaluated and implemented enhanced visual and audible feedback to better alert personnel of valid and invalid reads; and 6) installed improved technology (lights and audible alarms) on PSP doors to alert users on the validity of the key card reads. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019635	CIP-010-2	R4	[REDACTED] (the Entity)	[REDACTED]	04/02/2018	04/02/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On May 3, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R4. The Entity did not follow its documented process for using only a designated Transient Cyber Assets (TCAs) to connect to a Bulk Electric System (BES) Cyber System (BCS).</p> <p>On April 2, 2018, two of the Entity’s technicians went to a [REDACTED] to take the monthly readings from [REDACTED]. Prior to departing for this monthly site visit, the technicians were reminded to use the designated TCA laptop at the substation to obtain the meter readings. Unbeknownst to one another, each technician retrieved a corporate, non-TCA, laptop and assumed the other technician had the TCA laptop. When they entered the control house, technician 1 went to the restroom, while technician 2 set up a corporate laptop. Upon returning from the restroom, technician 1 assumed that the opened laptop was the TCA and began to download the monthly readings from the meters. Technician 1 then transferred the readings from the laptop to a secure jump drive, and proceeded to transfer the readings from the jump drive to a corporate laptop when technician 1 discovered that the assumed TCA was in fact a corporate laptop. Technician 1 immediately called a supervisor to report what had occurred. When the technicians returned to the office, they provided the corporate laptop to the [REDACTED] to conduct a forensic analysis. The [REDACTED] found that the laptop had up-to-date antivirus signatures with ongoing management and security patches.</p> <p>On April 4, 2018, an engineer and a technician went to the substation to conduct a forensic investigation on all [REDACTED] and no issues were detected. The Entity also confirmed that there were no additional instances of failure to use a TCA when connecting to a BCS.</p> <p>[REDACTED]</p> <p>This noncompliance started on April 2, 2018, when the unauthorized laptop computer was connected to the BCS, and ended on April 2, 2018, when the laptop was disconnected from the BCS later the same day.</p> <p>The cause of this noncompliance was a lack of internal controls. Specifically, the Entity did not implement internal controls to distinguish designated TCA laptops from non-TCA corporate laptops. To mitigate the noncompliance, the Entity applied red laptop covers, labels, and background wallpaper clearly marking the laptops as designated TCAs.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Connecting an unauthorized laptop computer to a BCS has the potential to introduce malicious code into the BCS, which could lead to a loss of control of the connected BCAs. However, the laptop in this instance was under the Entity’s corporate control, and was found to be current on security patches and antivirus. The Entity also conducted a forensic inspection of the BCAs to which the laptop had been connected, and determined that no harm is known to have occurred.</p> <p>SERC considered the Entity’s compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1. completed a forensic examination of the substation meters and unauthorized corporate laptop and confirmed no detected issues; 2. applied red laptop covers to each TCA laptop to better differentiate TCA laptops from non-TCA (corporate) laptops; 3. applied additional “Transient Cyber Asset” labels on all laptop TCAs, including at least one that can be seen from the front when the laptop is open; 4. applied custom Transient Cyber Asset background (wall paper) for the lock screen and log-in screen on all TCA laptops; 5. updated “CIP-10 Transient Cyber Assets and Removable Media Procedure” to include details of how a TCA laptop appears with the new covers and labels; and 6. delivered training describing the new parts of the procedure and the additional visual cues for TCA laptops. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2018019988	CIP-004-6	R5	[REDACTED]	[REDACTED]	07/02/2016	05/16/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 11, 2018, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5, P5.2. The Entity did not revoke an individual's authorized physical access, by the end of the next calendar day, following the date the Entity determined the individual no longer required such access.</p> <p>On June 30, 2016, the Entity transferred an employee from the Entity's [REDACTED]. The Entity's [REDACTED] revoked the employee's unneeded physical access privileges to [REDACTED] control centers that contained [REDACTED] BES Cyber Systems (BCSs) on his badge, but did not also revoke physical access on the employee's key fob. The Entity should have revoked the employee's key fob access by the end of the next day of the employee's transfer, in accordance with the Entity's documented access revocation program. The Entity did not discover this instance until May 11, 2018, when it conducted an ad hoc review of access revocation for an upcoming audit. Upon discovery, the Entity removed all physical access privileges from the key fob on May 16, 2018.</p> <p>The extent-of-condition involved a review of all personnel who held key fobs and a review of all personnel changes within that group. No additional instances were found.</p> <p>The scope of affected Facilities included [REDACTED] facilities that contained [REDACTED] BCSs.</p> <p>This noncompliance started on July 2, 2016, the day after when the Entity should have revoked the employee's physical access, and ended on May 16, 2018, when the Entity revoked the employee's physical access.</p> <p>The cause of this noncompliance was inadequate training. [REDACTED] was not aware of the required task in the Entity's process to revoke key fobs when revoking physical access privileges.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. By not revoking a transferred employee's physical access by the end of the next calendar day, a potential window of opportunity was afforded for the employee to potentially gain access to and degrade cyber assets and bulk power system facilities and maliciously cause grid instability or mine sensitive data. However, the individual was in good standing with the Entity and remained with the Entity after this transfer with no performance issues. The individual never used or attempted to use the FOB coded for CIP access at any point after the transfer. The Entity protected the cyber assets within the sites by requiring unique log-on credentials, which this employee did not have. This limited any risk vectors to physical access, which the Entity managed using real time configuration monitoring of the Cyber Assets. The Entity also secured the CIP environments using redundant firewalls secured ESP and PSP controls, and the sites at issue were staffed at all times. The Employee was in good standing with the Entity and met clearance/training for unescorted access. No harm is known to have occurred.</p> <p>SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1. removed all physical access privileges from the key fob; 2. confirmed, by using a Physical Access Control System access usage report, that the key fob was not used at any facility during the time period between when the employee's badge access was revoked and the date his key fob access was revoked; and 3. re-trained the Entity's [REDACTED] on the PACS workstation Instruction that provides guidance for removing access from all devices, including key fobs. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019020987	CIP-011-2	R1	██████████ (the "Entity")	██████████	07/01/2016	01/15/2020	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from ██████████, Texas RE determined that the Entity, as a ██████████, was in noncompliance with CIP-011-2, R1.1. Specifically, the Entity did not identify the backups stored on the network attached storage (NAS) servers as Bulk Electric System Cyber System Information (BCSI). Additionally, the Entity did not identify the NAS servers used for backups as a designated BCSI storage location.</p> <p>The root cause of the noncompliance was that the Entity's process for identification of BCSI did not consider these fully encrypted backups located in a secured location as information that could be used to gain unauthorized access or pose a security threat to applicable BES Cyber Systems.</p> <p>This noncompliance started on July 1, 2016, when the standard became effective, and ended January 15, 2020, the earliest date by which the Entity's evidence reflects that it had added a label to all NAS storage drives to identify the contents as BCSI.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk posed by this noncompliance is that by not identifying the BCSI (and subsequently, not identifying the NAS as a storage location), the Entity may not have implemented controls that have been deemed necessary for protecting designated storage locations. However, although the Entity did not identify the backups as BCSI and did not designate the NAS servers as BCSI storage locations, the Entity used controls, such as encryption and physical protection in place to reduce the risk. Additionally, the Entity has a relatively ██████████). No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> ended the noncompliance by adding a label to all NAS storage drives to identify the contents as BCSI; and prevented reoccurrence by revising its CIP-011-2 Information Protection policy to include NAS drives utilized for BES Cyber System backups. <p>Texas RE has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019020986	CIP-004-6	R2; 2.1 and 2.2	██████████ (the "Entity")	██████████	07/01/2016	01/02/2019	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from ██████████, Texas RE determined that the Entity, as a ██████████ was in noncompliance with CIP-004-6, R2. Specifically, the Entity did not implement all the required training content specified in Part 2.1 for the cyber security training program utilized by its vendors, and the Entity granted electronic access to ██████████ employee prior to completion of the training specified in Part 2.1. Although the Entity's training program for its own personnel included all nine training elements specified in CIP-004-06, the Entity accepted vendor training in lieu of the Entity's training material for vendors.</p> <p>The root cause of the noncompliance was that the Entity did not review the vendor training to ensure all aspects of the requirement were met, prior to accepting it as a replacement for their training.</p> <p>This noncompliance started on July 1, 2016, when the standard became effective, and ended on January 2, 2019, when the Entity revoked electronic access for the vendor's personnel.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Not executing proper training for third party personnel for items such as cyber-security policies or what they should do if a cyber-security Incident is identified may lead to an unwanted compromise of the bulk power system. However, the risk posed by the noncompliance was mitigated by the following factors. To begin, the electronic access granted to ██████████ employee prior to completion of the training specified in Part 2.1 was relatively short at three days, as that training was completed on March 16, 2018, after initial access was granted March 13, 2018. Additionally, the Entity has a relatively small footprint ██████████. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked electronic access for ██████████ personnel; 2) decommissioned ██████████ SCADA/EMS system; 3) revised its Cyber Security and Annual NERC CIP Training; and 4) revised its personnel and Training Program to include that all vendors and contractors who require electronic access shall be required to complete the same level of training as the Entity's employees. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017018200	CIP-003-6	R2	██████████ (the "Entity")	██████████	04/01/2017	07/11/2017	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted per an existing multi-region registered entity agreement from ██████████, Texas RE determined that the Entity, as a ██████████ was in noncompliance with CIP-003-6 R2. Specifically, the Reliability Standard requires the Entity to test the Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing Low Impact BES Cyber Systems, at least once every 36 calendar months. The Entity scheduled the first test of its Cyber Security Incident response plan for July 2017, which was after the April 1, 2017, implementation date for CIP-003-6 R2.</p> <p>The root cause of the noncompliance was a misunderstanding of the timeline of the implementation of CIP-003-6.</p> <p>This noncompliance started on April 1, 2017, when the first testing was due under the implementation plan for the Reliability Standard, and ended on July 11, 2017, when the Entity tested its Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure by an Entity to test its Cyber Security Incident response plan can lead to the Entity not having awareness of issues with that plan. The Entity's portfolio includes a generating capacity of approximately ██████████. However, the risk of this noncompliance was lessened because the entity had a documented Cyber Security Incident response plan in place. While completion of the required testing may improve the efficiency and efficacy of the plan, the existing plan was found to be compliant. A documented Cyber Security Incident response plan, even when not tested, significantly improves security posture over not having a plan at all, or having an undocumented plan. Additionally, the Entity performed operational Security Incident Response tests prior to the compliance effective date, and included participation from personnel that manage BES Cyber Systems. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) tested its Cyber Security Incident response plan, which is applicable to Low, Medium, and High Impact BES assets, to end the noncompliance; 2) to prevent reoccurrence, implemented ██████████ toolset to track the Entity's CIP requirements, Control Procedures, etc., and to maintain regulatory compliance artifacts; 3) to prevent reoccurrence, held training for the Entity's applicable employees on CIP Low Impact BES Cyber Assets; and 4) to prevent reoccurrence, delivered NERC CIP Awareness communications to the impacted workers residing at Low Impact BES locations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019022152	CIP-004-6	R4; R4.1	██████████ (the "Entity")	██████████	08/14/2019	08/15/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 28, 2019, the Entity submitted a Self-Log stating that, as a ██████████ it was in noncompliance with CIP-004-6 R4.1. In particular, the Entity provisioned access to a designated storage location of BES Cyber System Information (BESCSI) without first authorizing the individual to access the storage location.</p> <p>The root cause of this noncompliance was a logic error in an access request and authorization workflow. The Entity's workflow was implemented in a manner where it was expected that the CIP Senior Manager would initiate access requests, and thus all access requests would already have approval from the CIP Senior Manager. In this instance of noncompliance the access request was submitted by an individual that was not the CIP Senior Manager, and as such the approvals were not present. The workflow did not contain logic to route the request to the CIP Senior Manager when this scenario occurred, and as such the request was processed and access provisioned without the documented approval of the Entity's CIP Senior Manager, which the Entity requires as part of its authorization process.</p> <p>This noncompliance started on August 14, 2019, when the user was provisioned access to the BESCSI designated storage location and ended on August 15, 2019, when the user's access to the designated storage location was revoked.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The period of noncompliance was short, lasting only one day. Additionally, the Entity verified that the user did not access the designated storage location while access was provisioned.</p> <p>Texas RE determined that the Entity's compliance history should not serve as a basis for aggravating the risk. The Entity does have a previous instance of noncompliance, however the issues have different root causes. In the previous instance of noncompliance the Entity was unable to demonstrate that it had approved ████████ individuals to have access to a Physical Security Perimeter due to a lack of procedural controls to ensure the existence of and long-term storage of authorization records. In this instance of noncompliance the Entity did not fully follow their authorization process due to a previously unencountered logic error in an automated workflow.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) to end the noncompliance the Entity revoked the user's access to the BESCSI storage location; 2) to prevent recurrence of this noncompliance the Entity reconfigured its workflow to explicitly require approval from the ██████████ before the request is routed for provisioning; and 3) to prevent recurrence of this noncompliance the Entity instructed members of ██████ to not grant access without approval by the CIP Senior Manager. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2019022153	CIP-006-6	R1; R1.9	[REDACTED] (the "Entity")	[REDACTED]	02/05/2019	02/10/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On August 28, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED] it was in noncompliance with CIP-006-6 R1.9. In particular, the Entity is unable to demonstrate that it retained physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least 90 calendar days.</p> <p>The root cause of this noncompliance was hardware failure. The Entity has configured their Physical Access Control System (PACS) to retain logs indefinitely. When the Entity discovered logs were missing the Entity contacted its vendor to determine the cause. The vendor subsequently determined that a memory corruption issue, because of a faulty memory chip, was responsible.</p> <p>This noncompliance started on February 5, 2019, which is the first day within 90 calendar days of the discovery of the issue and for which logs are missing, and ended on February 10, 2019, which is the first day after the beginning of the log issue for which the entity is in possession of logs.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The noncompliance was related to the logging function of the PACS. During the period of noncompliance the PACS continued to function as intended. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) due to the nature of the noncompliance, the noncompliance ended without user intervention, ending on the day when logs are available in the PACS; and 2) to prevent recurrence of this noncompliance the Entity has configured their PACS to send daily copies of applicable logs to a second location for retention purposes. <p>Texas RE has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017017973	CIP-004-6	R5	[REDACTED] (the "Entity")	[REDACTED]	04/01/2017 04/28/2017	04/02/2017 04/28/2017	Self-Report	06/01/2020
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 20, 2017, the Entity submitted a Self-Report stating that, as a [REDACTED] it was in noncompliance with CIP-004-6 R5. Specifically, in two instances, the Entity did not revoke an individual's authorized unescorted physical access or Interactive Remote Access within the 24-hour time limit provided in the Procedure for removing such access when an employee is terminated or has retired. In the first instance, the employee who had resigned did not have their Interactive Remote Access removed within the required timeframe. In the second instance, the retired employee did not have his Interactive Remote Access or his unescorted physical access terminated within the required timeframe.</p> <p>The root cause of this noncompliance was insufficient training on procedures for removal of access.</p> <p>This noncompliance of the first instance started on April 1, 2017, the day after the first employee resigned but did not have his or her Interactive Remote Access removed and ended on April 2, 2017, when that employee's unauthorized access was removed. The noncompliance of the second instance ended the same day it began: it began on April 28, 2017, at 10:45 AM, which was 24 hours after that employee's last day, and ended on April 28, 2017, at 3:29 PM, when unauthorized access was removed for that individual.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Neither of the two former employees attempted to gain physical or electronic access to the Entity's Physical Security Perimeters or Electronic Security Perimeters during the time after their employment ceased and before their authorized unescorted physical and/or Interactive Remote Access were revoked. Additionally, the first instance lasted only one day, and the second instance lasted only a few hours. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity took the following steps:</p> <ol style="list-style-type: none"> 1) to end the noncompliance, the Entity removed unauthorized access for both individuals; and 2) to prevent reoccurrence of the noncompliance, by June 1, 2020, the Entity will perform training on proper removal of unauthorized access of the entire [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
TRE2018019891	CIP-005-5	R1; 1.3	██████████ ("the Entity")	██████████	07/01/2016	03/28/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from ██████████, Texas RE determined that the Entity, as a ██████████), was in noncompliance with CIP-005-5 R1; 1.3. Specifically, for both the primary and backup control center configuration files, while the Entity did have inbound and outbound access permissions, the Entity did not include the reason for granting access.</p> <p>The root cause of the noncompliance was an overreliance on a third-party vendor for managing the Entity's firewall rules, and a lack of internal management comprehension of the requirements.</p> <p>This noncompliance started on July 1, 2016, the effective date of the standard, and ended on March 28, 2018, when the Entity provided updated configuration files containing justifications for granting access.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. A failure to maintain firewall access permissions has the potential to affect the reliability of the BPS by providing the opportunity for undetected compromise of Bulk Electric System (BES) Cyber Systems to occur, which could lead to misoperation or instability in the BES. However, the risk is reduced by the following factors. To begin, the firewall rules determined to be no longer necessary were very few compared to the firewall rules that were deemed necessary; in other words, while the Entity had failed to include a justification for each rule, once the Entity reviewed the rules, the vast majority of those rules were determined to be necessary, and therefore stayed in place. Additionally, the Entity has a relatively ██████████ of interconnected generation). No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) undertook a full analysis of the firewall configurations at its primary and backup Control Centers and updated firewall configurations; and 2) underwent an organizational restructuring to improve the Entity's compliance process and managerial-level expertise. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019887	CIP-010-2	R3; 3.3	[REDACTED] ("the Entity")	[REDACTED]	11/28/2017	06/24/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit from [REDACTED], Texas RE determined that the Entity, as a [REDACTED] was in noncompliance with CIP-010-2, R3. Specifically, the Entity did not, prior to adding new applicable Cyber Assets to a production environment, perform an active vulnerability assessment of the new Cyber Assets. The Entity indicated not having any additions of Cyber Assets to the production environment outside of a recent SCADA upgrade, but was unable to provide sufficient evidence of an active Vulnerability Assessment for those additions.</p> <p>The root cause of this noncompliance was an overreliance on a third-party vendor, which ran an inventory scan, but not a full vulnerability assessment on new Cyber Assets.</p> <p>This noncompliance started on November 28, 2017, when the first Cyber Assets were added after the standard became effective, and ended on June 24, 2018, when the Entity performed an active vulnerability assessment on all Cyber Assets, including those added during its SCADA upgrade.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Adding new high impact BES Cyber Assets and failing to perform and document vulnerability assessments can reduce the ability to detect potential vulnerabilities that can pose a threat to the bulk power system. However, the risk was reduced by the following factors. To begin, the duration of the noncompliance was relatively short, lasting approximately seven months. Further, the Entity demonstrated having a tool that has the capability of sending notifications for unplanned changes during the duration of the noncompliance. Lastly, the impacted devices were located inside an ESP. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) performed a new vulnerability assessment for all new Cyber Assets, including those added during the audit period; 2) underwent an organizational restructuring to improve the Entity's compliance process and managerial-level expertise; and 3) performed vulnerability assessments for new Cyber Assets in-house. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019888	CIP-010-2	R1; R1.1; R1.2; R1.3; R1.4; R1.5	[REDACTED] ("the Entity")	[REDACTED]	07/01/2016	03/01/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], Texas RE determined that the Entity, as [REDACTED] was in noncompliance with CIP-010-2 R1. Specifically, the Entity did not provide evidence of fully baselining all applicable cyber assets, authorizing and documenting all baseline changes, updating all baseline configuration deviations within 30 calendar days, documenting that required cyber security controls were not adversely affected, and testing and documenting results of test for all baseline configuration deviations.</p> <p>The root cause of the noncompliance was reliance on a tracking tool that did not have the capability of producing new baselines each month.</p> <p>This noncompliance started on July 1, 2016, when the standard went into effect, and ended on March 1, 2018, when the Entity began documenting monthly baselines for each Cyber Asset.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The lack of documenting and testing changes can lead to potential risks and reduce the ability to mitigate them. However, these risks were mitigated by the following factors. Specifically, the Entity had a process in place for each part of the requirement subject to noncompliance, and the Entity demonstrated to the Audit Team that it has a tool that has the capability of monitoring all baseline configuration changes, including operating system or firmware; commercially available or open-source application software installed; custom software installed; logical network accessible ports; and the security patches applied. However, the tool used by the Entity lacked a reporting function to provide evidence for applicable cyber assets sampled for the time frames requested. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) implemented a tool for keeping monthly baselines for each Cyber Asset; and 2) trained its applicable employees on the new tool. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019889	CIP-009-6	R2; 2.2	[REDACTED] ("the Entity")	[REDACTED]	07/01/2017	08/08/2018	Compliance Audit	03/01/2020
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED] Texas RE determined that the Entity, as a [REDACTED] was in noncompliance with CIP-009-6 R2. Specifically, the Entity did not test a representative sample of information used to recover PACS, at least once every 15 calendar months to ensure that the information is useable and compatible with current configurations.</p> <p>The root cause of the noncompliance was that the Entity did not have a test environment or extra controller for its PACS systems.</p> <p>This noncompliance started on July 1, 2017, which is 15 calendar months from the effective date of the FERC Order adopting the standard, and ended on August 8, 2018, when the Entity experienced an incident with a PACS controller and performed an actual recovery.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk of not testing a representative sample of information used to recover PACS at least once every 15 calendar months is that if there were an incident, the Entity may find that it does not have a plan that is able to recover reliability functions performed by its BES Cyber Systems, risking the continued stability, operability, and reliability of the BES. However, the risk posed by this issue was reduced by the following factors. To begin, the Entity has a [REDACTED]. Further, although the Entity had not tested a representative sample of information used to recover BES Cyber System functionality for the PACS, all other representative samples of information were tested. Additionally, the Entity has a redundant PACS system, so if one system was hindered, the Entity has the other system in place to fill in. No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity will complete the following mitigation activities by March 1, 2020:</p> <ol style="list-style-type: none"> 1) To mitigate this noncompliance, the Entity provided dated evidence of an actual incident where the PACS system was recovered; and 2) To prevent reoccurrence of this noncompliance, the Entity will install a new PACS system through a different vendor by January 31, 2020. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019890	CIP-007-6	R2; 2.2 and 2.3	[REDACTED] ("the Entity")	[REDACTED]	07/01/2016	03/29/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit from [REDACTED] Texas RE determined that the Entity, as a [REDACTED] was in noncompliance with CIP-007-6, R2. Specifically, the Entity was unable to demonstrate that, at least once every 35 calendar days, it evaluates security patches for applicability that have been released since the last evaluation from the sources identified in Part 2.1, and for any patches so evaluated, apply applicable patches within 35 calendar days.</p> <p>The root cause for the noncompliance was the Entity's inability to demonstrate compliance with the requirement. The Entity utilized a tool that lacked the functionality that would retain evidence, which could demonstrate the Entity's compliance with the requirement.</p> <p>This noncompliance started on July 1, 2016, when the standard became effective, and ended on March 29, 2018, when the Entity became up-to-date on evaluating security patches for applicability.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to evaluate and apply patches in a timely manner could have exposed the Entity's BES Cyber Systems to cyber security vulnerabilities, such as the introduction of malicious code. However, although the Entity was not able to demonstrate that it evaluated or applied patches for several sampled Cyber Assets within the required timeframe, the Entity was able to provide additional evidence that demonstrated that several patches were evaluated and applied within the required timeframe. Additionally, the Entity has a [REDACTED] No harm is known to have occurred.</p> <p>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) became up-to-date on evaluating all security patches for applicability at least once every 35 calendar days, and applied all applicable security patches within 35 calendar days; 2) [REDACTED], which serves as monthly baselines for each Cyber Asset; and 3) holds and documents monthly meetings among the IT, Engineering, and Compliance groups to review available patches. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019193	CIP-010-2	R1: P1.2; P1.3	[REDACTED]	[REDACTED]	11/01/2017	05/18/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On February 12, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in potential noncompliance with CIP-010-2 R1. For the first issue, on November 1, 2017 the entity did not update the baseline configuration of two Bulk Electric System (BES) Cyber Assets associated with its Medium Impact BES Cyber System (MIBCS) and [REDACTED] Physical Access Control Systems (PACS) associated with its High Impact BES Cyber System (HIBCS), as required by Part 1.3. Specifically, the entity implemented a change on October 1, 2017 but the entity's documented process required manual data entry to complete its automated process to update baseline configurations. The employee incorrectly input data into the tracking system which precluded the automated process from identifying that a change had been made to the Cyber Assets in scope of this issue. As such, the baseline configurations were not updated within 30 calendar days of completing the change. This issue started on November 1, 2017 when the entity did not update the baseline configuration within 30 days of completing a change and ended on May 18, 2018 when the entity updated the baseline configurations, for a duration of 199 days.</p> <p>For the second issue, the entity implemented a change to [REDACTED] PACS servers on November 8, 2017 but did not authorize the change as required by Part 1.2 nor did the entity update the baseline configuration within 30 calendar days of completing the change as required by Part 1.3. Responsibility for the patching process had been transferred to a new employee in 2017; during an internal investigation, the entity discovered that the documented process for implementing changes was incomplete and did not detail instructions for authorizing and documenting changes to the baseline configuration. Therefore, the employee completed the process as documented, however the procedure was not adequately detailed in the entity's documented process. This issue started on December 9, 2017 when the entity did not update the baseline configuration 30 days after completing a change and ended on January 23, 2018, when the entity authorized and documented all changes to the baseline configurations on the [REDACTED] PACS, for a duration of 46 days.</p> <p>The root cause of the issues was attributed to less than adequate program documentation and inadequate work package preparation. The processes for both issues were primarily automated, however, employees needed to accurately input and handle data for the process to be completed correctly.</p>					
Risk Assessment			<p>These issues 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 authorize and document changes that deviated from the existing baseline configuration as required by CIP-010-2 R1 Part 1.2 for [REDACTED] PACS and failed to update the baseline configuration as necessary within 30 days of completing a change, for changes that deviated from the existing baseline as required by CIP-010-2 R1 Part 1.3 for two BCAs and, on two additional occasions, [REDACTED] PACS.</p> <p>Failure to authorize, document changes, and update the baseline configuration could have resulted in the entity unable to restore the PACS to its most recent configuration which could have resulted in extended outages of the PACS. Additionally, these failures could have resulted in changes being authorized when they are inappropriate for the system. However, the PACS were isolated on a separate network subnet and protected by a network switch with an access control list. Additionally, the entity implemented periodic manual reviews that resulted in the discovery of the second issue during an internal investigation because of regularly scheduled reviews. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate these issues, the entity has:</p> <ol style="list-style-type: none"> 1) authorized changes to, and updated, the baseline configurations for the Cyber Assets in scope; 2) updated process documentation to include more detailed instructions for the patching process; and 3) streamlined the baseline configuration procedure to minimize data entry errors and limited the ability to manually enter asset data to only when a change has not yet been completed. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020218	CIP-007-6	R1	[REDACTED]	[REDACTED]	07/01/2016	07/17/2018	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 violation.)			<p>On August 12, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] it was in potential noncompliance with CIP-007-6 R1. Specifically, the entity had a total of [REDACTED] enabled logical network accessible ports on [REDACTED] Physical Access Controls Systems (PACS) and [REDACTED] Electronic Access Control or Monitoring Systems (EACMS) associated with [REDACTED] Medium Impact Bulk Electric System (BES) Cyber System (MIBCS), with External Routable Connectivity, that had not been determined needed and should have been disabled and/or blocked. The entity discovered the enabled logical ports when it installed new technology that specifically scanned for enabled ports that were not authorized. This issue began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on July 17, 2018, when the entity determined [REDACTED] of the affected logical ports were needed and disabled the remaining [REDACTED] logical ports on a PACS, for a duration of 747 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls. Specifically, upon implementation of its whitelisting tool, the entity did not conduct a preliminary test as a preventative control to ensure the tool used to scan for open ports was compatible with all Cyber Assets used by the entity; as such the entity was unaware it had [REDACTED] enabled ports not deemed necessary and that it should have disabled.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to enable only logical network accessible ports that had been determined to be needed as it related to [REDACTED] logical ports on eight Cyber Assets, as required by CIP-007-6 R1 Part 1.1.</p> <p>Failure to enable only logical ports needed by the entity could have resulted in an enabled port providing a pathway to a network-based attack on the MIBCS. However, the entity determined [REDACTED] of the [REDACTED] open logical ports were needed; the remaining [REDACTED] open logical ports were on very low-risk Cyber Assets on an isolated network. Additionally, the entity has a small footprint and only operates [REDACTED] of generation and a [REDACTED] of transmission line. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty because significant time has elapsed between the two previous issues therefore, not indicative of broader compliance issues or failed mitigation efforts.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a scan of all open logical ports, disabled [REDACTED] unnecessary ports, and determined the remaining [REDACTED] open ports necessary; and 2) deregistered as a [REDACTED] as such, the entity will have only Low-Impact Assets and is no longer required to comply with CIP-007-6 R1. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020219	CIP-007-6	R3: P3.3	[REDACTED]	[REDACTED]	07/01/2016	06/18/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On August 12, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] it was in potential noncompliance with CIP-007-6 R3. Specifically, the entity did not test and install signature updates to its Intrusion Detection System (IDS). The entity had a documented process to update signatures and patterns associated with its antivirus solution; however, at the time, the entity had not identified that its IDS was in scope of the Requirement. After further consideration, the entity identified that two of the six types of updates made to the IDS contain signatures or patterns and that its documented process for updating signatures or patterns should include the IDS. This issue began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on June 18, 2018, when the entity tested and installed the signatures to the IDS, for a duration of 718 days.</p> <p>The root cause of the issue was attributed to less than adequate implementation of the Standard and Requirement. Specifically, the entity did not correctly identify that applicability of the Requirement extended to the IDS appliance; as a result, the entity did not apply the protections required.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its process for those methods identified in Part 3.1 that use signatures or patterns; a process that addresses testing and installing the signatures or patterns as required by CIP-007-6 R3 Part 3.3 for its IDS appliance.</p> <p>Such a failure could have resulted in the entity's method of malicious code prevention failing to operate and cause the introduction of malicious code into the environment. However, the entity had restricted the function of the IDS to monitoring only, which significantly reduced its ability to impact the Bulk Electric System. Additionally, this issue was discovered because of the entity's efforts to identify opportunities to strengthen its compliance posture. Additionally, the entity has a small footprint and only operates [REDACTED] of generation and a [REDACTED] transmission line. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) tested and installed signatures on the IDS; 2) updated its documented process to reflect the testing method for the IDS appliance; and 2) deregistered as a [REDACTED]; as such, the entity will have only Low-Impact Assets and is no longer required to comply with CIP-007-6 R3. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020220	CIP-007-6	R5: P5.6	[REDACTED]	[REDACTED]	07/01/2016	07/31/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On August 12, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-007-6 R5. Specifically, the entity did not change the password for a total of eleven accounts associated with [REDACTED] Cyber Assets, every 15 calendar months as required by CIP-007-6 R5 Part 5.6. Five accounts, associated with the same type of Cyber Asset, were created as backup accounts and were never accessed. The remaining six accounts, associated with [REDACTED] different Cyber Asset types, were administrative accounts used for maintenance of the affected Cyber Assets. One of the eleven accounts was regularly used; the remaining ten were never or rarely used. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on July 31, 2018 when the entity had changed all passwords, for a duration of 761 days.</p> <p>The root cause of the issue was attributed to a less than adequate process design. Specifically, the entity utilized a spreadsheet as an internal control to track the date account passwords were changed but did not incorporate tracking of when those passwords expired. The entity relied solely on account users to recall when passwords needed to be changed.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to implement its documented process to either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months for password only authentication for interactive user access, for 11 accounts as required by CIP-007-6 R5 Part 5.6.</p> <p>Failure to enforce password changes increases the risk of a malicious actor having the ability to login to one of these Cyber Assets to make changes or gather configuration information. However, ten of the 11 accounts were rarely or never used. Additionally, the entity had implemented alerts for unsuccessful login attempts and logged security events. Additionally, the entity has a small footprint and only operates [REDACTED] of generation and a [REDACTED] transmission line. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) reviewed the necessity of each account and removed five accounts as unnecessary; 2) changed the password of the remaining six accounts; and 3) deregistered as a [REDACTED]; as such, the entity will have only Low-Impact Assets and is no longer required to comply with CIP-007-6 R5. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020265	CIP-007-6	R2: P2.2; P2.3	[REDACTED]	[REDACTED]	01/01/2018	08/08/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On August 22, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-007-6 R2 related to three issues. Specifically, for the first issue, the entity did not apply or create a dated mitigation plan for one security patch deemed applicable to [REDACTED] BES Cyber Assets (BCA) and [REDACTED] protected Cyber Assets (PCA) associated with [REDACTED] Medium Impact BES Cyber Systems (MIBCS) located at the primary and backup Control Center as required by CIP-007-6 R2 P2.3. The entity evaluated applicability of the security patch within the required 35-day timeframe and determined it most prudent to wait for a subsequent, fully-tested release prior to applying the patch. However, the employee failed to draft a mitigation plan to mitigate identified vulnerabilities associated with waiting to apply the patch in the interim. This issue started on January 1, 2018 when the entity initially failed to apply a patch, create a dated mitigation plan, or revise an existing mitigation plan and ended on July 31, 2018, for a duration of 212 days.</p> <p>For the second issue, the entity did not implement its documented process to evaluate the applicability of one security patch, later deemed applicable to [REDACTED] Electronic Access Control or Monitoring Systems (EACMS) associated with a MIBCS, as required by CIP-007-6 R2 Part 2.2.; nor did the entity apply the patch or create a dated mitigation plan as required by Part 2.3. Specifically, the entity's documented process was incomplete and did not include steps for evaluating and applying patches for EACMS. As such, when the entity transferred responsibility for evaluation and application of security patches, the employee to whom responsibility was transferred did not evaluate patches for the EACMS in scope. This issue started on February 3, 2018 and ended on August 8, 2018, when the entity installed the security patches, for a duration of 187 days.</p> <p>For the third issue, the entity failed to evaluate the applicability of 15 security patches for [REDACTED] EACMS associated with [REDACTED] MIBCS as required by CIP-007-6 R2 Part 2.2; nor did the entity apply the patch or create a dated mitigation plan as required by Part 2.3. Specifically, a vendor had changed how security patch updates were communicated to the entity. The employee responsible for performing these tasks was unfamiliar with the new format and did not identify that the patches at issue had been released. This issue started on March 10, 2018 and ended on July 24, 2018, when the entity installed the security patches, for a duration of 137 days. The aggregate of the three issues began on January 1, 2018 and ended on August 8, 2018, for a duration of 220 days.</p> <p>The root cause of these issues was attributed to the entity's failure to adequately track the completion and status of action items. Specifically, the entity did not implement internal controls sufficient to verify that mitigation plans had been drafted, that personnel were reviewing all security patch vendors, or that employees were aware of how the security patch releases were being communicated.</p>					
Risk Assessment			<p>These issues 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, 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 deemed applicable, as required by CIP-007-6 R2 Part 2.2, for one security patch associated with [REDACTED] EACMS in the second issue, and 15 security patches associated with [REDACTED] EACMS in the third issue. Additionally, the entity failed to, for applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, to take one of the following actions: apply the applicable patches; or create a dated mitigation plan; or revise an existing mitigation plan as required by CIP-007-6 R2 Part 2.3 for one security patch associated with [REDACTED] Cyber Assets in the first issue, one security patch associated with [REDACTED] EACMS in the second issue, and fifteen security patches associated with [REDACTED] EACMS in the third issue.</p> <p>Failure to evaluate, apply, or mitigate security patches could have resulted in vulnerabilities not being identified and addressed on the affected Cyber Assets. Additionally, a malicious actor could have exploited a known vulnerability to disrupt the BES. However, the entity implemented controls to limit electronic and physical access to assets located within the Electronic Security Perimeter and Physical Security Perimeter to only individuals with authorized access. Additionally, the entity implemented redundancy in their environments to mitigate the risk associated with the malfunctioning of a single Cyber Asset and conducted a review of all applications twice a month as a detective control; one of these issues was discovered because of this control. Finally, the entity has a small footprint and only operates [REDACTED] of generation and a [REDACTED] transmission line. No harm is known to have occurred.</p> <p>WECC determined that the entity had two prior issues in its compliance history but should not serve as a basis for applying a penalty. One was issued as a Compliance Exception and the second was issued in 2012; therefore, not indicative of broader compliance issues or failed mitigation efforts.</p>					
Mitigation			<p>To mitigate these issues, the entity has:</p> <ol style="list-style-type: none"> 1) evaluated the security patches for applicability; 2) installed the applicable security patches; 3) corrected and updated the source of the security patch release vendor; 4) trained relevant personnel on the security patch requirements and process; and 					

<p>4) deregistered as a [REDACTED]; as such, the entity will have only Low-Impact Assets and is no longer required to comply with CIP-007-6 R2. WECC has verified the completion of all mitigation activity.</p>
--

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019020887	CIP-002-5.1a	R2: P2.1, P2.2	[REDACTED]	[REDACTED]	06/01/2018	11/08/2018	Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>During a Compliance Audit conducted [REDACTED] WECC determined that the entity, as a [REDACTED] was in potential noncompliance with CIP-002-5.1a R2 Parts 2.1 and 2.2. Specifically, the entity did not review the identifications made pursuant to CIP-002-5.1a R1 within 15 calendar months of completion of the prior identification as required in CIP-002-5.1a R2.1. As such, the entity's CIP Senior Manager or delegate did not approve the identifications made pursuant to CIP-002-5.1a R1 at least once every 15 calendar months as required by CIP-002-5.1a R2.2. The entity had completed its prior review on March 1, 2017 which resulted in confirmation of [REDACTED] identified Medium Impact BES Cyber System (MIBCS) and [REDACTED] Low Impact BES Cyber Systems (LIBCS). This issue began on June 1, 2018, when the entity should have reviewed the identifications made pursuant to CIP-002-5.1a R1 within 15 calendar months of the prior review and ended on November 8, 2018, when the entity reviewed the identifications made pursuant to CIP-002-5.1a R1 and its CIP Senior Manager approved those identifications, for a duration of 161 days.</p> <p>The root cause of the issue was attributed to a misinterpretation of the requirement and lack of internal controls. Specifically, the entity was unaware a review was required if there were no changes identified, therefore it had not implemented preventative controls to avoid occurrence of this issue.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to review its identifications made pursuant to Requirement 1 and its parts at least every 15 calendar months and have its CIP Senior Manager or delegate approve the identifications as required by CIP-002-5.1 R2 Parts 2.1 and 2.2, for [REDACTED] MIBCS and [REDACTED] LIBCS.</p> <p>Failure to the review and approve the identified BCS could have resulted in the mis-categorization of a BCS and potentially led to ineffective or nonexistent protective measures for the entity's BES Cyber Assets. However, in this instance, the entity did not have any newly identified BCS. Additionally, the entity had conducted an interim review in September 2017, but failed to document the review and approval appropriately. Finally, the entity has a small footprint and only operates [REDACTED] of generation and a [REDACTED] of transmission line. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) reviewed its identifications made pursuant to CIP-002-5.1a R1 and obtained CIP Senior Manager approval of the identifications; 2) created a recurring agenda item to review due dates of required compliance-related activities during weekly scheduled CIP Compliance meetings; 3) documented a process for new and revised Standard implementation; and 3) deregistered as a [REDACTED] as such, the entity will have only Low-Impact Assets. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019297	CIP-007-6	R2: P2.1; P2.2	[REDACTED]	[REDACTED]	07/01/2016	12/13/2017	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On February 28, 2018 the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-007-6 R2. Specifically, on November 28, 2017, the entity discovered it had not adequately documented and implemented its process to track security patch sources as required by CIP-007-6 R2 Part2.1; as a result, the entity did not evaluate one cyber security patch for applicability within 35 days of its release as required by Part 2.2. In this instance, an employee had received a Technical Bulletin used to alert users of cyber security patch releases via email, however, the employee failed to identify the Technical Bulletin as a patch source in its documented process for cyber security patch management. Therefore, when the employee retired, the undocumented patch source was not tracked; consequently, the entity did not evaluate one security patch that was applicable to 22 Bulk Electric System (BES) Cyber Assets (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The Part 2.1 issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on December 13, 2017, when the entity had documented the Technical Bulletin as a source of security patches, for a duration of 531 days. The Part 2.2 issue began on November 6, 2017 when the permitted 30-day timeframe to evaluate security patches expired and ended on November 28, 2017, when the entity evaluated the security patch for applicability, for a duration of 23 days.</p> <p>The root cause of the issue was attributed to a less than adequate tracking of a task or process. Specifically, execution of the security patch management program was not sufficiently tracked to expose the gap in program documentation – a result of the employee’s failure to document all security patch sources.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to implement its documented patch management process for tracking, evaluating, and installing cyber security patches for one security patch associated with applicable Cyber Assets as required by CIP-007-6 R2 Part 2.1; as a result, the entity failed to, at least once every 35 days, evaluate one security patch 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.</p> <p>Failure to evaluate a security patch could result in a malicious actor exploiting a known vulnerability of a Cyber Asset to introduce malicious code into the MIBCS. However, the entity had implemented monitoring in the MIBCS to prevent and detect malicious code, detect unusual account activity, and monitor network communication. Additionally, the entity restricts open ports and services within its Electronic Security Perimeter to only those deemed necessary. Finally, the entity physically secured each asset and system within a Physical Security Perimeter. No harm is known to have occurred.</p> <p>WECC determined that the entity’s compliance history should not serve as a basis for applying a penalty. Due to the facts, circumstances, and timing, the prior violations are not indicative of a systemic and programmatic issue.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) evaluated and applied the applicable cyber security patch; 2) updated the entity’s contact information with the vendor to a group email address to preclude individual points of contact; and 3) included the review of technical bulletins in the Patch Management Program. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019298	CIP-007-6	R3: P3.3	[REDACTED]	[REDACTED]	3/27/2017	2/5/2018	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On February 28, 2018, the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-007-6 R3. Specifically, the entity did not implement its documented process to test the signatures or patterns during the process of updating the entity's malicious code detection and prevention. In this instance, the entity had applied an authorized cyber security patch; the patch unexpectedly enabled the automatic update setting on the entity's method of malicious code detection and prevention. As a result, updates to the method of malicious code prevention were made without testing the signatures or patterns in accordance with the entity's documented process. This instance impacted 29 Bulk Electric System (BES) Cyber Assets (BCA) associated with a Medium Impact BES Cyber System. This issue began on March 27, 2017, when the entity stopped implementing its documented process to update signatures and patterns and ended on February 5, 2018, when the entity disabled the automatic update setting on all BCAs, for a duration of 316 days.</p> <p>The root cause of the issue was attributed to less than adequate change management; specifically, the risks associated with application of the cyber security patch were not adequately assessed or reviewed.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to implement its documented process, for the update of signatures or patterns, that addresses testing and installing the signatures or patterns for one method identified in Part 3.1 as required by CIP-007-6 R3 Part 3.3.</p> <p>Failure to test signatures and patterns could have resulted in a loss of monitoring and therefore, a heightened risk of the introduction of malicious code. However, the BCAs were located within a Physical Security Perimeter and were logically protected by the Electronic Security Perimeter. Additionally, the entity reduced the risk to its assets by limiting the ports and services to only those deemed necessary by the entity. The entity also continuously monitored network traffic through use of an integrated intrusion detection and intrusion prevention system. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty. Due to the facts, circumstances, and timing, the prior violations are not indicative of a systemic and programmatic issue.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) disabled the automatic update feature on the BCAs; and 2) redesigned its documented process to test signatures and patterns in a non-critical environment. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021157	CIP-011-2	R1: P1.2	[REDACTED]	[REDACTED]	11/1/2018	10/28/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On March 1, 2019, the entity submitted a Self-Report stating that, as a [REDACTED], it was in potential noncompliance with CIP-011-2 R1. Specifically, two employees emailed a total of three communications internally that contained information identified by the entity as Bulk Electric System (BES) Cyber System Information (BCSI) without encrypting the data or including a disclaimer that access to the information was restricted to the intended recipient only per its documented procedures. On November 1, 2018, an employee emailed a procedure the entity had identified as BCSI to the second employee; approximately an hour later, the first employee emailed a prior version of the same procedure to the second employee. On November 2, 2018, the second employee, emailed the same procedure to a third employee. This issue began on November 1, 2018, when the first email containing BCSI was sent and ended on October 28, 2019, when all three emails were deleted, for a total of 362 days.</p> <p>The root cause of the issue was attributed to less than adequate process documentation and a lack of training. Specifically, the two employees that sent all three emails were new employees. The employees had not been trained on how to encrypt a document and lacked sufficient awareness to identify BCSI and to protect the BCSI in accordance with the entity's documented program. Further, the entity's documented procedure did not contain instructions on encryption.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to implement its documented procedure for securely handling BCSI, including storage, transit, and use as required by CIP-011-2 Part 1.2. Failure to encrypt and label communications containing BCSI during transit internally could have resulted in an employee unknowingly forwarding BCSI externally to a third-party.. However, in the event that BCSI was accessed by a third party, the entity had deployed an integrated approach to malicious code prevention through the use of intrusion detection and intrusion prevention and limited the ports and services on its BES Cyber Assets to only those deemed necessary. Additionally, no emails containing BCSI were emailed to external parties and the senders and receivers of the communications were authorized for access to the BCSI. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty. Due to the facts, circumstances, and timing, the prior violations are not indicative of a systemic and programmatic issue.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) deleted the emails from all impacted employee laptops; 2) provided training to the employees involved on how to encrypt a document and use the disclaimer statement; 3) provided information protection training to all employees, which included instructions on encryption and use of the disclaimer statement; and 4) uploaded the entity's Information Protection Procedure to an internal SharePoint site. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC20190022288	CIP-002-5.1a	R2: P2.2	[REDACTED]	[REDACTED]	7/1/2016	9/9/2016	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>During a Compliance Audit conducted [REDACTED] determined that the entity, as a [REDACTED] was in potential noncompliance with CIP-002-5.1a R2 Part 2.2. Specifically, the entity was not able to provide evidence that its CIP Senior Manager had approved the BES Cyber System identifications required by Requirement R1 by the initial performance date of July 1, 2016. During the audit, the entity provided two separate evidence documents to support the CIP Senior Manager approval of its BES Cyber System identifications, one dated April 1, 2016 and the other dated September 9, 2016. During the onsite audit, the entity stated the April 1, 2016 approval process had not been completed, thus the list was never formally approved until September 9, 2016, for a total of 71 days.</p> <p>The root cause of the issue was attributed to a less than adequate oversight and coordination of work to ensue there was enough lead time to complete compliance obligations timely. The execution of R2.1 took longer than expected as it was a new task for many stakeholders.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 as required by CIP-002-5.1a R2 Part 2.2 by the initial performance date of July 1, 2016.</p> <p>Such failure could have resulted in the entity not identifying or mis-categorizing BES Cyber Systems and led to ineffective or nonexistent protective measures for the Cyber Assets in and associated with the BES Cyber System. The entity had no internal controls in place to ensure the task was completed in a timely manner. However, this issue was administrative in nature. The entity had a process documented and a job aid that explained that CIP-002 had to be reviewed and approved. The entity simply missed the mandatory and enforceable date of performing the approval. Nevertheless, no harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty. The entity had one relevant compliance history which was a minimal risk issue identified in 2014; therefore, not indicative of broader compliance issues.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) obtained CIP Senior Manager approval of the BES Cyber System identifications; 2) updated its procedures to clarify procedural steps relating to the annual review and approval of the indemnifications as required by Part 2.2, to include the use of an automated work management system for evidence task assignment, tracking, and collection; and 3) trained the impacted stakeholders on any procedure changes performed. The process owners also delivered a training session to walk through the procedure changes with required personnel. <p>WECC has not verified the completion of mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022289	CIP-003-6	R1	[REDACTED]	[REDACTED]	7/1/2016	6/28/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>During a Compliance Audit conducted [REDACTED] determined that the entity, as a [REDACTED] was in potential noncompliance with CIP-003-6 R1. Specifically, for one instance the entity had a delegate approve its documented cyber security policies on October 14, 2017; however, the Requirement does not allow the CIP Senior Manager to delegate the actions required by CIP-003-6 R1. Additionally, for the second issue, the entity did not perform the approvals at least once every 15 calendar months from the last approval. These issues began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on June 28, 2018, when the CIP Senior Manager approved the CIP-003-6 R1 policies, for a total of 727 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and oversight of compliance tasks to ensure those tasks were clearly managed.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to have its CIP Senior Manager approve its policies as required by CIP-003-6 R1 by the initial performance date of July 1, 2016.</p> <p>Such failure could have resulted in distribution of inaccurate guidance or outdated policies. However, as compensation, the policies had been approved by a delegate at the request of the CIP Senior Manager and disseminated to all those that needed to be aware. This issue was administrative in nature and simply an oversight regarding who was formally required to approve the policies. No harm is known to have occurred.</p> <p>WECC determined the entity had no previous compliance history with this Standard and Requirement.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) obtained CIP Senior Manager approval of the CIP-003-6 R1 policies; 2) communicated to the Standard owner, delegate, and subject matter experts that only the CIP Senior Manager could sign the CIP-003-6 policies; 3) updated and published its CIP-003 procedure to include clarifying language that the approval of the policies cannot be delegated; and 4) added internal controls into its work management system to manage recurring compliance tasks. <p>WECC has not verified the completion of mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022350	CIP-010-2	R1: P1.1.1; P1.1.2 and P1.1.3	[REDACTED]	[REDACTED]	07/01/2016	07/15/2019	Compliance Audit	Completed
<p>Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)</p>			<p>During a Compliance Audit conducted [REDACTED], [REDACTED] determined that the entity, as a [REDACTED] was in potential noncompliance with CIP-010-2 R1 Part 1 subpart 1.1.1, 1.1.2, and 1.1.3.</p> <p>Specifically, for [REDACTED] BES Cyber Assets without External Routable Connectivity (ERC) associated with [REDACTED] different Medium Impact BES Cyber Systems (MIBCS) the entity failed to develop a baseline configuration that included the Operating System (including version), any commercially available or open-source application software (including version) intentionally installed, and any custom software. For [REDACTED] BES Cyber Asset (BCA), the baseline configuration was missing the Operating System version number, two installed commercial software applications, and the column for "custom software installed" was left blank. For the [REDACTED] BCA, the baseline configuration was missing version numbers for all installed software, and the area for custom installed software was left blank. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on July 15, 2019, when the entity dated the baseline configurations for the two BCAs in scope, for a total of 1,110 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls to check the accuracy of data that was manually input into a master list of baseline configurations.</p>					
<p>Risk Assessment</p>			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to develop baseline configurations that included the Operating system (including version), any commercially available or open-source application software (including version) intentionally installed, and any custom software as required by CIP-010-2 R1 Part 1 subparts 1.1.1, 1.1.2, and 1.1.3, for [REDACTED] BCAs associated with [REDACTED] different MIBCS.</p> <p>Failure to document complete baseline configurations could have resulted in the entity's change review board approving changes without full knowledge of what was installed on the BES Cyber Assets, which could have led to those BES Cyber Assets not functioning appropriately. Additionally, inaccurate baseline configurations could have delayed restoring the two BES Cyber Assets should the need arise. However, as compensation, the two BCAs had all other baseline configuration protective measures applied, were protected with electronic and physical access controls and monitor, and were updated with the most recent firmware to ensure operational integrity and security. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty because the one prior noncompliance was related to not identifying a Cyber Asset; therefore, it is distinct and separate from this issue.</p>					
<p>Mitigation</p>			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) updated baseline configurations for the [REDACTED] BCAs; 2) deployed a new baseline configuration functionality work management system into the production environment and performed a validation of functionality to verify that errors and deficiencies are properly reported to users and appropriate groups; 3) revised procedures, associated job-aids, and checklists to include the use of the new work management system functionality for baseline configurations; 4) ensured accurate migration of baseline configuration spreadsheets into the new work management system; and 5) trained CIP Cyber System Owners on the new work management system functionality. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019547	CIP-007-3a	R7: R7.2	[REDACTED]	[REDACTED]	12/21/2015	8/9/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On April 17, 2018, the entity submitted a Self-Report stating, as a [REDACTED] it was in potential noncompliance with CIP-011-2 R2. Specifically, on February 28, 2018, the entity discovered that [REDACTED] Protected Cyber Assets (PCAs) containing Bulk Electric System (BES) Cyber System Information (BCSI) associated with its High Impact BES Cyber System (HIBCS), were redeployed to a non-CIP environment on December 12, 2015. During the change management process for the redeployment of the PCAs, a label was removed from the description of the Cyber Assets in the change management system that indicated they contained BCSI. However, the entity did not actually remove the BCSI from the Cyber Assets. Additionally, because the Cyber Assets were not identified as containing BCSI, on June 27, 2017 when the entity sent the them for disposal to its third-party disposal company, the entity did not wipe the Cyber Assets of BCSI prior sending them.</p> <p>The root cause of the issue was attributed to less than adequate internal controls. Specifically, while the entity had a process in place for the redeploying and disposing of Cyber Assets containing BCSI, they did not have controls in place to ensure the process was followed correctly. These issues began on December 21, 2015, when the PCAs were redeployed without removing BCSI and ended on August 9, 2017, when the PCAs were destroyed for a total of 598 days.</p>					
Risk Assessment			<p>WECC determined these issues posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to take action to prevent the unauthorized retrieval of BCSI from [REDACTED] PCAs data storage media prior to their redeployment as required by CIP-007-3a R7.2 and failed to take action to prevent the unauthorized retrieval of BCSI from those same PCAs or destroy the data storage media prior to disposal as required CIP-0 11-2 R2 Part 2.2.</p> <p>Failure to prevent unauthorized retrieval of BCSI when reusing or disposing of a PCA could have resulted in the BCSI being used by a nefarious person to gain access to the entity's HIBCS in order to affect operations including generation, transmission, and balancing. However, as compensation, the entity implemented striping on the storage array to prevent unauthorized data retrieval thereby making the data very difficult to recover. This reduced the potential risk that an unauthorized individual would be able to gain logical access to BCSI on the PCAs. Additionally, the BCSI on the PCAs was outdated and of limited value. No harm is known to have occurred.</p> <p>WECC determined that the entity's compliance history should not serve as a basis for applying a penalty. The underlying cause of the instant noncompliance is unrelated to the prior instances of noncompliance, and the associated mitigation plans could not have prevented the instant noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ul style="list-style-type: none"> a) destroyed the [REDACTED] PCAs containing BCSI; b) added a control to its CIP-011 processes to ensure devices are taken to a designated disposal storage area for the secure storage of applicable Cyber Assets until scheduled destruction occurs. The process also includes a provision for securing the Cyber Assets at remote locations that cannot be immediately transported to the designated disposal storage area; c) transitioned the responsibility for the CIP-011-2 Requirements to a separate team, which was already responsible for overseeing all additions and removals from the data centers; and d) created a segmentation of CIP and non-CIP assets to ensure the tag in the asset change system will not be removed as a control to address future prevention. <p>WECC has verified completion of all mitigation activities.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019411	CIP-010-2	R1: P1.1 sub-part 1.1.1.	[REDACTED]	[REDACTED]	09/14/2016	12/7/2016	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On March 19, 2018, under an existing multi-region registered entity agreement, the entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. Specifically, the entity did not document the firmware baseline configuration for one Bulk Electric System (BES) Cyber Asset (BCA), prior to commissioning the BCA associated with a Medium Impact BES Cyber System without External Routable Connectivity. In this instance, the entity had scheduled the commissioning of the BCA for a later date; however, when an unrelated emergency change was made, the entity determined it appropriate to place the BCA into service immediately. The employee tasked with documenting the baseline did not do so. This issue began on September 14, 2016, when the entity failed to document the firmware baseline configuration and ended on December 7, 2016, when the entity documented the baseline configuration, for a duration of 85 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls. Specifically, the entity did not implement preventative controls sufficient to avoid occurrence of the issue, such as a checklist for employees to utilize during the commissioning process for new Cyber Assets. In this instance, the employee was aware of their responsibility to document the baseline configuration but did not recall all steps required to commission the BCA.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to implement its documented process to develop a baseline configuration, individually or by group, which includes the operating system or firmware of the asset for one BCA as required by CIP-010-2 R1 Part 1.1 sub-part 1.1.1.</p> <p>Failure to document the firmware baseline configuration could have resulted in a prolonged system restoration if the BCA needed to be restored to its original firmware. However, because the change was planned for a later date, the entity had already enforced additional security controls on the asset. Additionally, no security patches were released between the time the asset was commissioned and the date the baseline was documented. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) documented the baseline configuration of the BCA ; 2) created a checklist as a preventative control to be used to document or update a baseline configuration; and 3) informed all relevant personnel that use of the checklist is required. <p>WECC has verified the completion of all mitigation activity.</p>					

COVER PAGE

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

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	MRO2019022046			Yes	Yes									Category 2 – 12: 2 years
2	MRO2019022136			Yes	Yes									Category 2 – 12: 2 years
3	MRO2019021944			Yes	Yes									Category 2 – 12: 2 years
4	MRO2019022386			Yes	Yes									Category 2 – 12: 2 years
5	MRO2019022388		Yes	Yes	Yes									Category 2 – 12: 2 years
6	MRO2019021364			Yes	Yes									Category 2 – 12: 2 years
7	MRO2019021366	Yes		Yes	Yes					Yes				Category 2 – 12: 2 years
8	MRO2019021367			Yes	Yes									Category 2 – 12: 2 years
9	MRO2019021368			Yes	Yes									Category 2 – 12: 2 years
10	MRO2019021369			Yes	Yes					Yes				Category 2 – 12: 2 years
11	MRO2019021370			Yes	Yes									Category 2 – 12: 2 years
12	MRO2019021867			Yes	Yes									Category 2 – 12: 2 years
13	SPP2017016732			Yes	Yes						Yes	Yes	Yes	Category 2 – 12: 2 years
14	SPP2017016745			Yes	Yes						Yes	Yes		Category 2 – 12: 2 years
15	SPP2017017544			Yes	Yes						Yes	Yes	Yes	Category 2 – 12: 2 years
16	SPP2017017545			Yes	Yes						Yes	Yes	Yes	Category 2 – 12: 2 years
17	SPP2017017549			Yes	Yes						Yes	Yes	Yes	Category 2 – 12: 2 years
18	SPP2017017550	Yes		Yes	Yes						Yes	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)
19	SPP2017017551			Yes	Yes						Yes	Yes	Yes	Category 2 – 12: 2 years
20	MRO2018019352	Yes		Yes	Yes					Yes				Category 2 – 12: 2 years
21	MRO2019022101			Yes	Yes									Category 2 – 12: 2 years
22	MRO2019022346			Yes	Yes									Category 2 – 12: 2 years
23	MRO2019022382			Yes	Yes									Category 2 – 12: 2 years
24	MRO2019022387			Yes	Yes									Category 2 – 12: 2 years
25	MRO2019021261			Yes	Yes									Category 2 – 12: 2 years
26	MRO2018020734			Yes	Yes									Category 2 – 12: 2 years
27	NPCC2018019941	Yes		Yes	Yes						Yes			Category 1: 3 years Categories 3 – 4: 2 years Category 10: 3 years
28	NPCC2018019942	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years Categories 3 – 4: 2 years Category 9 – 10: 3 years
29	NPCC2019022070	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years Categories 3 – 4: 2 years Category 8 – 9: 3 years
30	RFC2019021026	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
31	RFC2019021477	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
32	RFC2019021621	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
33	RFC2019021233	Yes	Yes	Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2-12: 2 years.
34	RFC2019021230	Yes	Yes	Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2-12: 2 years.
35	RFC2019021231	Yes	Yes	Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2-12: 2 years.
36	RFC2019021306	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2-12: 2 years.
37	RFC2019021686	Yes	Yes	Yes	YEs									Category 1: 3 years; Category 2-12: 2 years.
38	WECC2018020443	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
39	WECC2019022177		Yes	Yes	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)
40	WECC2019021119		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
41	WECC2019022179		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
42	WECC2019022168		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
43	WECC2019022180		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
44	WECC2019022167		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
45	WECC2019022178		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
46	WECC2019022169		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
47	WECC2019022170		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
48	WECC2019022171		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
49	WECC2019021116		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
50	WECC2019022176		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
51	WECC2019022172		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
52	WECC2019022183		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
53	WECC2019022174		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
54	WECC2019022182		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
55	WECC2019022173		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
56	WECC2019022175		Yes	Yes	Yes							Yes		Category 2 – 12: 2 years
57	WECC2019021674			Yes	Yes									Category 2 – 12: 2 years
58	WECC2019021676			Yes	Yes									Category 2 – 12: 2 years
59	WECC2019021677			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)
60	WECC2019021682			Yes	Yes									Category 2 – 12: 2 years

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022046	CIP-004-6	R5	[REDACTED] (the Entity)	[REDACTED]	06/08/2019	06/14/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R5.</p> <p>The Entity reported that it had started an individual's termination process, however, the Entity failed to remove the individual's unescorted physical access and Interactive Remote Access (IRA) within 24 hours of the "termination action."</p> <p>The cause of noncompliance was the Entity's process for unescorted physical access and IRA revocation was deficient in addressing cases where an individual had approved PTO and later absence from work without notifying the Entity (interpretation of termination action).</p> <p>The noncompliance began on June 8, 2019, when the individual's access was not removed within 24 hours of the termination action, and ended on June 14, 2019, when access was removed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per the entity, it revoked the physical access and IRA within 24 hours of identifying the individual's absence from work without notification. Per the entity, the individual of issue did not use the unauthorized unescorted physical access or IRA during the issue duration. The duration of the noncompliance was limited to seven days, which reduced the risk. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) removed the individual's access; 2) defined and updated "termination action" as the time when revocation of physical, electronic, and/or remote access will take place (the date of the termination action may not be the last day worked). 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022136	CIP-006-6	R1	[REDACTED] (the Entity)	[REDACTED]	07/02/2019	07/03/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On July 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R1. On July 2, 2019, the Entity modified its Physical Security Perimeter (PSP) of its Backup Control Center (BCC) to add a new office door to remove the office from the PSP. On July 3, 2019, during the Entity's Supervisory Control and Data Acquisition (SCADA) department's daily review of nightly baseline scans for the BCC's SCADA workstation, the Entity discovered that the SCADA workstation in the new office has been disconnected from network. The SCADA department logically disconnected the port and performed a self-evaluation of the BCC. During the self-evaluation, the Entity discovered that the BCC workstation had been properly stored in a secure location but the SCADA Energy Management System (EMS) network port in the room wall (which was no longer inside the PSP) was still cabled into the SCADA EMS Electronic Security Perimeter (ESP) not in accordance with CIP-006-6 R1.10.</p> <p>The cause of the noncompliance was that the Entity failed to follow its documented plan to address CIP-006-6 R1.10 due to a failure of coordinating construction work in the Entity's PSPs and ESPs with the CIP subject matter experts (SMEs).</p> <p>This noncompliance began on July 2, 2019, the day the new office door was added to the PSP, and ended on July 3, 2019, when the port was logically disabled.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per the Entity, no device was connected to the port between the removal of the office from the PSP and the time that the ports were logically disabled. Additionally, the new office space is within the interior of the facility with badged access requirements and security personnel manning the front desk, thereby limiting the attack vectors to PSP and ESP. Lastly, per the Entity, the Entity's robust compliance program enabled the Entity to find and mitigate the risk, limiting the duration to less than one day.</p> <p>No harm was known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) logically disabled the relevant ports; 2) physically disconnected the cable from the switch and added port locks; and 3) contacted the facilities manager and reinforced the importance of coordinating all construction work near PSPs and ESPs with the CIP Senior Manager and 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
MRO2019021944	CIP-004-6	R4	<div style="background-color: black; width: 100%; height: 1em; margin-bottom: 2px;"></div> (the Entity)	<div style="background-color: black; width: 100%; height: 1em;"></div>	09/13/2018	04/25/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)	<p>On July 19, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4. This Self-Log contained two instances of noncompliance.</p> <p>In the first instance of noncompliance, the Entity identified that physical access to one Physical Security Perimeter (PSPs) at a generation station containing medium impact BES Cyber Systems (BCS) was granted to one individual without authorization. This was identified during the required quarterly access review.</p> <p>The noncompliance began on September 13, 2018, when the access was granted, and ended on December 12, 2018, when the access was revoked.</p> <p>In the second instance of noncompliance, the Entity identified access to one physical BES Cyber System Information (BCSI) storage location (security office) was granted to one individual without authorization.</p> <p>The noncompliance began on December 3, 2018, when access was provisioned, and ended on April 25, 2019, when access was revoked.</p> <p>The cause of the noncompliance for both instances was that the Entity failed to follow its process for provisioning physical access to PSPs and BCSI storage locations by granting access to more than that which was authorized during provisioning.</p> <p>The aggregate of the two instances of noncompliance began on September 13, 2018 and ended on April 25, 2019.</p>							
Risk Assessment	<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>For the first instance, the access was limited to one individual for the PSPs at a generation station containing medium impact BCS. The individual who was granted access also had authorized access to the PSPs containing high impact BCS. The individual had completed the required training and a personnel risk assessment (PRA). Additionally, prior to accessing the PSP at the substation, the individual would have had to access the exterior gate, for which access was not provisioned.</p> <p>For the second instance, the individual who was granted access had other approved access to PSPs. This individual had completed cyber security training and a PRA, which are not required for BCSI access. The issue was discovered through quarterly BCSI access reviews, which go beyond the frequency required by the standard and the individual did not utilize the provisioned access during the duration of the issue.</p> <p>No harm was known to have occurred.</p>							
Mitigation	<p>To mitigate the both instances of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) revoked access for the individuals involved; and 2) performed one-on-one coaching between the individuals who provisioned the unauthorized access and their managers. 							

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022386	CIP-004-6	R4	[REDACTED] (the Entity)	[REDACTED]	04/01/2019	04/12/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4.</p> <p>The Entity reported that during an annual review of electronic access and BES Cyber System Information (BCSI) access (as required by CIP-004-6 R4.3 and R4.4), it found that a quarterly review of the individuals with unescorted physical access was not completed during the first quarter of 2019.</p> <p>The cause of the noncompliance was that, while the entity had an internal control to remind the responsible employee ahead of time to perform the quarterly review for physical access, the employee failed to follow the Entity's CIP-004-6 R4.2 process to perform and complete the access review on time.</p> <p>The noncompliance began on April 1, 2019, when the Entity failed to verify for the first calendar quarter that individuals with unescorted physical access have proper authorizations on file, and ended on April 12, 2019, when the access verification was completed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per the Entity, the issue was minimal because it was limited to the delayed quarterly review of individuals with unescorted physical access, and there were no physical access discrepancies identified after the review was completed. Additionally, the duration of the noncompliance was limited to 12 days. Lastly, MRO concluded that the issue was related to a detective control measure and was not related to an active measure for preventing or deterring unauthorized electronic or physical access. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed its physical access review; and 2) adopted a compliance oversight plan that includes monitoring of all compliance reminders within its system to ensure that all specified due dates are met. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022388	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	05/30/2019	06/05/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 10, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1.</p> <p>The Entity reported that while staff were preparing for a monthly patch cycle, it discovered an unauthorized change to the baseline configuration. [REDACTED] Software related to a patch was uninstalled from a high impact Supervisory Control And Data Acquisition (SCADA) support workstation because the software was determined to no longer be required from an operational perspective. During this time, the Entity did not believe that removing this software would cause a change in the baseline configuration. Upon further investigation, it was found that the removal of this software did, in fact, cause an unauthorized change to the baseline configuration.</p> <p>The cause of the noncompliance was that the Entity did not realize that removal of software drivers would alter the impacted Protected Cyber Asset's (PCA) baseline which led to a failure to follow its change management process, resulting in baseline changes being made without authorization.</p> <p>The noncompliance began on May 30, 2019, when the Entity failed to authorize and document a change to existing baselines when it removed software that was determined to no longer be needed from a single high impact PCA, and ended on June 5, 2019, when the Entity retroactively authorized this change.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per the Entity, the issue was minimal as it was limited to one Physical Access Control System (PACS) associated with a high impact BES Cyber System. Also, subsequent testing of security controls found no adverse impacts. Additionally, the issue was resolved by updating authorization and documentation, rather than by making any changes to any Cyber Assets, therefore documentation in nature. Lastly, the change was due to the removal of software from a PACS and not the addition or change of software, inherently reducing the risk of adverse impacts to the system. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) retroactively authorized the baseline change; and 2) altered its procurement phase processes associated with its SCADA upgrade to ensure that all high and medium impact BES Cyber Assets are configured with the same hardware and software. This ensures that all similar BES Cyber Assets during a SCADA upgrade have matching baselines and there is not additional equipment or software installed that would need to be removed after the baselines were created. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021364	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	09/08/2016	02/11/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 9, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-010-2 R1. Specifically, per the Entity, prior to a change that deviated from the existing baseline configuration, the Entity did not determine the required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change as required by Part 1.4.1. As a result, the Entity could not verify that the required cyber security controls determined in 1.4.1 were not adversely affected as required by 1.4.2 nor could the Entity document the results of the verification as required by 1.4.3.</p> <p>The cause of the noncompliance was that the individual failed to follow the Entity's CIP-010-2 R1 program to verify cyber security controls in CIP-005 and CIP-007.</p> <p>This noncompliance began on September 8, 2016, when an individual began to not follow the Entity's program to verify cyber security controls in CIP-005 and CIP-007 in accordance with CIP-010-2 R1.4 for a deviation from the existing baselines and ended on February 11, 2019, when the last of 12 changes that impacted eight medium impact BES Cyber Assets (MIBCA) at a Control Center, failed to have its cyber security controls verified by this individual.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per the Entity, the impacted Control Centers only contain MIBCA, and only low impact BES Cyber Systems are impacted by this Control Center. Also, the 12 impacted changes represent about 3.3% of all changes during the duration of this issue. The Entity's ongoing internal controls monitoring CIP-005 and CIP-007 security controls exceed the requirements. For example, the Entity performs; a daily ports and services change report, weekly baseline changes report, weekly enabled logging and alerting verification, daily new account alerts, and, real-time whitelist alerts (the eight BCAs are whitelisted). Additionally, MRO understands that after subsequent testing of security controls the Entity reported no adverse impacts. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) verified all CIP-005 and CIP-007 controls during the baseline change that followed this issue; and 2) reviewed with all applicable personnel its process to document and review all CIP-005 and CIP-007 controls in accordance with its CIP-010-2 program. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021366	CIP-007-6	R5	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	02/25/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 9, 2019, the Entity submitted a Self-Log stating that, as a as a [REDACTED], it was in noncompliance with CIP-007-6 R5. This submission contained four instances of noncompliance.</p> <p>In the first instance of noncompliance, the Entity reported that it failed to identify, inventory, and change the default passwords for all known enabled default [REDACTED] medium impact BES Cyber Assets (BCAs) at two substations. The cause of the noncompliance was that the Entity's process for identifying default accounts was insufficient, resulting in unidentified accounts.</p> <p>This noncompliance began on July 1, 2016, when the Entity failed to identify, inventory, and change the default passwords for eleven medium impact BCAs at two substations, and ended on January 14, 2019, when the default passwords on nine BCAs where changed and two BCAs were removed from service.</p> <p>In the second instance of noncompliance, the Entity reported that it failed to change the [REDACTED] account passwords on two medium impact BCAs from the previously required six-character complexity to eight. The cause of the noncompliance was that the Entity failed to follow its process to enforce password complexity of eight characters.</p> <p>This noncompliance began on July 1, 2016, when the Entity failed to change the passwords to eight characters, and ended on February 25, 2019, when both passwords were upgraded to eight characters.</p> <p>In the third instance of noncompliance, the Entity reported that it failed to submit four CIP-007-6 R5 Technical Feasibility Exceptions (TFE) Material Change Reports within sixty days (as per NERC Rules of Procedure) for adding four additional [REDACTED] medium impact BCAs that already contain the same modules and had an active TFE for those modules. The cause of the noncompliance was that the Entity failed to identify a change in quantity to existing communications equipment for BCAs which would require a TFE Material Change Report to be submitted.</p> <p>This noncompliance began on January 20, 2018, when the Entity failed to submit TFEs, and ended on December 28, 2018, when the Entity submitted the TFE Material Change Reports.</p> <p>In the fourth instance of noncompliance, the Entity reported that it failed to change shared account passwords for two Electronic Access Control and Monitoring Systems (EACMS) associated with high impact BCSs within 15 calendar months. The cause of the noncompliance was due to a lack of clarity on role responsibilities, the Entity failed to follow its process for changing passwords at least once every 15 calendar months.</p> <p>This noncompliance began on October 2, 2018, when the Entity failed to change the shared account passwords, and ended on October 5, 2018 when the passwords were changed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance was minimal because this issue impacted [REDACTED] similar BCAs which represents about [REDACTED] of similar devices. A user must authenticate to two lower level accounts prior to accessing the [REDACTED] account, and all individuals authorized for the lower levels would be authorized for this access. Lastly, the devices that had an issue were not accessible via External Routable Connectivity, thereby limiting the attack vectors to the device.</p> <p>The second instance was minimal because a user must authenticate to one lower level account prior to accessing the [REDACTED] account. The devices of issue were not accessible via External Routable Connectivity, thereby limiting the attack vectors to the device. Lastly, both passwords met the three character-type complexity requirement and met the previous requirement for six-character complexity, limiting the potential risk for unauthorized access.</p> <p>The third instance was minimal because the issue was documentation-in-nature and was resolved through the update of documentation, rather than implementation of a change to the system. The compensating and mitigation measures in place from the existing TFEs applied to the additional new equipment. Lastly, this issue was identified proactively in an unrequired evaluation of previous internal TFE analysis, thereby limiting the duration of this issue</p> <p>The fourth instance was minimal because the impacted generic account did not provide interactive user access, it is limited to install and set-up of the EACMS server. The issue was limited to two EACMS associated with a high impact BCS. Multifactor authentication is required for remote login to these devices which is above what is required, and the issue duration was limited to four days.</p> <p>No harm is known to have occurred.</p>					

Mitigation	<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none">1) identified, inventoried, and changed the default passwords on nine of the BCAs and the other two BCAs were removed from service;2) updated its vendor documentation search criteria to ensure calibration accounts were identified; <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none">1) changed the impacted passwords to eight character complexity; and2) reviewed the spreadsheets from the updated job aid with applicable individuals. <p>To mitigate the third instance of noncompliance, the Entity:</p> <ol style="list-style-type: none">1) submitted the TFE Material Change Reports. <p>To mitigate the fourth instance of noncompliance, the Entity:</p> <ol style="list-style-type: none">1) changed both impacted passwords; and2) added a note to the account inventory to assign responsibility to the IT team.
-------------------	---

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021367	CIP-007-6	R4	[REDACTED] (the Entity)	[REDACTED]	09/27/2018	11/29/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 9, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R4. During an annual vulnerability assessment, the Entity discovered that it failed to configure two relays at one new substation for logging successful and failed login attempts when they became medium impact Bulk Electric System (BES) Cyber Assets (MIBCA).</p> <p>The cause of the noncompliance was that the Entity's process lacked sufficient detail to ensure that logging for successful and failed login attempts was configured for new Cyber Assets.</p> <p>This noncompliance began on September 27, 2018, when the Entity failed to configure two relays, at one new substation, to log successful and failed login attempts why they became MIBCA's, and ended on November 29, 2018, when the Entity configured both MIBCA's to log successful and failed login attempts.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity determined that the devices of issue did not have External Routable Connectivity, thereby limiting the attack vectors to the device. Also, a security badge is required to enter the locked substation control house which exceeds the physical security controls required by the CIP standards. Additionally, this issue was limited to two MIBCA's at a single substation where no incidents occurred during the days of the misconfiguration. Lastly, the issue was related to a passive detective control measure and was not related to an active measure for preventing/detering security events or control of the BES. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) configured both impacted MIBCA's to log successful and failed login attempts; and 2) altered the timing of its process to verify the settings of devices prior to becoming BCAs which will bring the process into alignment with the timing of energization such that verification will be completed prior to devices becoming BCAs . 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021368	CIP-011-2	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	03/06/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 9, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-011-2 R1. This submission contained three instances of noncompliance.</p> <p>In the first instance of noncompliance, the Entity received an email from a contractor that contained a file (substation drawing) that was not encrypted and was determined to contain BES Cyber System Information (BCSI). This non-encrypted BCSI was emailed again by the Entity to the same contractor the next day. The Entity's CIP-011-2 procedure for protecting in-transit BCSI required the information to be encrypted. The noncompliance began on December 26, 2018, when the contractor improperly transmitted BCSI, and ended on December 27, 2018, when both the Entity and the contractor stopped improperly transmitting the BCSI.</p> <p>In the second instance of noncompliance, an employee started keeping a medium impact substation drawing that contained BCSI in an unsecured location (office floor) and the document eventually was recycled instead of destroyed. The noncompliance began on April 11, 2018, when the substation drawing was kept in an unsecured location, and ended on January 4, 2019, when the recycling company shredded all items collected which included the drawing.</p> <p>In the third instance of noncompliance, the Entity failed to identify electronic backup data from two systems as BCSI. The noncompliance began on July 1, 2016, when the standard became enforceable, and ended on March 6, 2019, when the backup data was correctly identified.</p> <p>The cause of noncompliance in all three instances was that the Entity failed to follow its process for identifying and protecting BCSI.</p> <p>The aggregate of the three instances began on July 1, 2016 and ended on March 6, 2019.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>In the first instance, the BCSI contained information for only a single substation and did not include shared passwords, Internet Protocol addresses, or phone numbers, which limits the ability to impact the BPS only by a misuse of the information. Additionally, the Entity reports that the substation does not have External Routable Connectivity, meaning that an adversary would have to infiltrate the substation's physical security controls to gain access to the BES Cyber Assets at all substations. Lastly, the risk was significantly reduced because it was limited to two emails and not a general release of BCSI.</p> <p>In the second instance, the BCSI was limited to a single substation drawing, significantly reducing the risk because it was not a general release of BCSI. The BCSI did not include shared passwords, IP addresses, or phone numbers, which limited the ability to misuse the information. Additionally, the single substation whose information is of issue does not have External Routable Connectivity, which limits the use of the BCSI to individuals with physical access to the substation. Lastly, the Entity has physical security controls that require a badge to gain access to any BES Cyber Assets at its substations, further preventing misuse.</p> <p>In the third instance, the BCSI access was limited to individuals that work in information technology rather than a general release of information. All individuals have had background checks and training, which is above the requirements for designated storage locations. Although the information was not identified as BCSI, it had been protected and securely handled as such, per the Entity's Information Protection Program. MRO concluded that this issue was documentation in nature as the BCSI was not identified correctly. Lastly, the BCSI protections expected by CIP-011-2 were in place because the Entity's culture of compliance goes over and above what the standards require.</p> <p>No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) stopped improperly transmitting the BCSI; and 2) sent an email reminder to the impacted employee and contractor on its procedure to encrypt attachments with BES CSI when sent in external emails. <p>To mitigate the second instance of noncompliance, the Entity:</p>					

<p>1) instructed its recycling company to shred all contents it had collected, effectively destroying any BCSI; and 2) reviewed procedures for protecting and securely handling BCSI with the impacted individual and also verified that all other applicable employees continue to understand the procedures.</p> <p>To mitigate the third instance of noncompliance, the Entity:</p> <p>1) identified the backup data as BCSI; 2) the backup system was designated as a BCSI storage location; and 3) communication with reminders on identification of BES CSI was sent to individuals with access to backup data.</p>

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021370	CIP-004-6	R4:	[REDACTED] (the Entity)	[REDACTED]	10/05/2018	10/05/2018	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 9, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4, Part 4.1 and 4.1.3.</p> <p>The Entity reported that they discovered an authorized custodian had used their access badge to let an unauthorized custodian (contractor employee) into a designated storage area containing BES Cyber System Information (BCSI).</p> <p>The cause of the noncompliance was that the Entity failed to follow its process to authorize access to designated storage locations containing BCSI.</p> <p>The noncompliance began and ended on October 5, 2018, when the unauthorized custodian used the authorized custodian's badge to gain access to a designated BCSI storage area and then exited this area.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per the Entity, the impacted contractor did not have access to any Physical Security Perimeters (PSP) or BES Cyber Assets. The designated storage location has limited paper documents deemed BCSI, but does not include any CIP-applicable systems or information that could provide access to CIP-applicable systems. Additionally, this was a single instance as the designated storage area is staffed 24/7 and was discovered immediately by authorized staff. Lastly, the Entity had a signed Confidentiality Agreement with the contractor. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance for reoccurrence, the Entity:</p> <ol style="list-style-type: none"> 1) removed unescorted access for all individuals associated with the custodian contract company; 2) allowed escorted access only during the day for individuals associated with custodian contract company; and 3) ultimately terminated its contract with the custodian contract company of 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
MRO2019021867	CIP-004-6	R4	[REDACTED] (the Entity)	[REDACTED]	11/01/2018	11/09/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On March 1, 2019, the Entity submitted a Self-Report stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4.</p> <p>The Entity reported that during an internal evaluation of CIP standards, it discovered that it had not verified user account groups and role access once every 15 calendar months as per CIP-004-6 requirement R4.3. The Entity completed its previous evaluation on July 1, 2017 and evaluated its quarterly access review (requirement R4.2) on September 27, 2017; however, it did not also verify all of the requirements as per R4.3. The review process was completed by a single reviewer.</p> <p>The cause of the noncompliance was that the Entity's process was defective as it did not ensure that all user account groups and role access reviews were performed as part of the once every 15 calendar months evaluation.</p> <p>The noncompliance began on November 1, 2018, the day after the last day of 15 month evaluation date, and ended on November 9, 2018, when a thorough review of all user account groups and role access were completed.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity reported that the noncompliance was discovered during an internal evaluation, limiting the duration of the noncompliance to nine days. Additionally, no improper privileges of individuals, user account groups, or user role categories resulted from this issue. Lastly, no other CIP requirements were at risk of noncompliance as a result of this issue. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) completed the full 15 calendar month evaluation; 2) created a Change Advisory Team (CAT) which consists of compliance executive leadership and technical subject matter experts who can collectively evaluate the once every 15 calendar months review; and 3) updated the access review procedure for CIP-004-6 to reflect the CAT and improvements to the 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
SPP2017016732	CIP-007-6	R3	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	12/16/2016	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED], the Entity submitted Self-Reports [REDACTED] containing two instances of noncompliance, stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R3. The Self-Reports were submitted in preparation for a Compliance Audit that was conducted from [REDACTED].</p> <p>In the first instance of noncompliance, the backup Control Center (BCC) Physical Access Control System (PACS) server did not deploy a method to deter, detect, or prevent malicious code. The cause of the noncompliance was that during the building of its new BCC, the Entity lacked the understanding of the standard, and therefore, did not realized that a BCC PACS system would be an in-scope Cyber Asset and need a baseline configuration developed. This resulted in the Entity not identifying the need to deploy a method to deter, detect, or prevent malicious code. The Entity relied on the baseline for identification of other applicable standards. The noncompliance began on August 15, 2016 when the BCC was placed in-service and ended on December 16, 2016 when the PACS system was moved to the primary Control Center (PCC), where a method to deter, detect, or prevent malicious code was present.</p> <p>In the second instance of noncompliance, an Electronic Access Control or Monitoring System (EACMS) did not have a process to test malicious code signatures as per CIP-007-6 P3.3. The EACMS (log aggregator) was initially considered to be only a data repository, but the Entity later determined it should have been considered an EACMS. The cause of the noncompliance was the Entity's lack of understanding of the Standard, which led to a failure to identify a log aggregator server as an EACMS, which resulted in a failure to implement the required method for testing signatures or patterns used in detecting malicious code. The noncompliance began on July 1, 2016 when the Standard became enforceable and ended on November 30, 2016 when a process for testing malicious code was implemented.</p> <p>The aggregate of the issues began on July 1, 2016 when the Standard became enforceable, and ended on December 16, 2016, when the PACS server in the first instance was moved to the PCC.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Per the Entity, the first instance was minimal because the PACS server was on a dedicated isolated PACS server network with no outside communications. The PACS server did not have remote login capability and to access the PACS server locally, the user must have been inside the Physical Security Perimeter (PSP) and use the physical console to login using the administrative username and password. The second instance was minimal, because the Entity determined that the anti-virus signature files were being updated automatically; they just were not tested first. Additionally, the data repository only aggregates logs from BES Cyber Systems and cannot exert control over those BES Cyber Systems. Additionally, if a failure of the logging on the repository occurred as a result of a failure to test the signatures, each of the BES Cyber Assets continue to log and store logs locally, such that logs would still be available for after-the-fact review. The data repository is located within a PSP and outside of Electronic Security Perimeter (ESP); additionally, the data communication between the data repository and ESP are monitored by a firewall. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate the instances of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) removed the BCC PACS server from service and all tasks performed were moved to PCC PACS server; 2) implemented work flow for NERC CIP update; and 3) sanitized the BCC PACS server. <p>The completion of all mitigation activity has been verified.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017016745	CIP-009-6	R1	[REDACTED] (the Entity)	[REDACTED]	07/1/2016	01/16/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED], the Entity submitted a Self-Report, in preparation for a Compliance Audit, stating that as a [REDACTED], it was in noncompliance with CIP-009-6 R1. The Compliance Audit was conducted from [REDACTED].</p> <p>The Entity determined that it failed to identify multiple devices (ACS Virtual Private Network (VPN) routers and Tripwire Log Center server) as Electronic Access Control and Monitoring Systems (EACMS), which resulted in a failure to establish documented recovery plans for those devices.</p> <p>Specifically, the Primary Control Center (PCC) and backup Control Center (BCC) ACS VPN routers were not identified as EACMS devices. This resulted in a failure to comply with the subsequent CIP requirements, including documenting the recovery plans as per CIP-009-6 R1. The noncompliance for this began on July 1, 2016, when CIP v5 standard became enforceable, and ended on December 20, 2016, when the routers were identified as EACMS and necessary recovery plans were created.</p> <p>The Entity also determined that the Tripwire Log Center server log aggregator was also not correctly identified as EACMS. As a result, recovery plan was not created as per CIP-009-6 R1. The noncompliance for this began on July 1, 2016, when CIP v5 standard became enforceable, and ended on January 16, 2017, when the routers were identified as EACMS and necessary recovery plans were created.</p> <p>The cause of the noncompliance for both issues was the Entity's lack of understanding of the standard led to a failure to identify the routers and Tripwire Log Center server as EACMS, which resulted in failure to document the recovery plans.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issues were minimal because access to the VPN routers of issue did not directly provide any access to Cyber Assets other than the Intermediate System. The operation of the BCC and PCC Bulk Electric System (BES) Cyber Systems is not affected by the lack of recovery plan and had no impact on the reliability of the BES. Also, the log aggregator server aggregates logs from BES Cyber Systems, and no controls of BES could be performed from this system. The operation of BES Cyber Systems is not affected by the lack of recovery plan and had no impact on the reliability of the BES. Lastly, there have been no security events associated with any of the affected devices. No harm is known to have occurred.</p> <p>The Entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate both instances of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) created a recovery plan for VPN routers ; 2) created a recovery plan for the Tripwire log center server; and 3) conducted a mock audit and CIP V5 boot camp for its CIP team to ensure better understanding of the CIP standards and managing the CIP environment. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017017544	CIP-007-6	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	05/03/2017	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED], the Entity submitted a Self-Report, in preparation for a Compliance Audit, stating that as a [REDACTED], it was in noncompliance with CIP-007-6 R1. The Compliance Audit was conducted from [REDACTED]. In addition to this Self-Report, an additional instance of noncompliance was found during the Compliance Audit that was conducted from [REDACTED]. All instances were consolidated and are being processed under the findings from the Compliance Audit.</p> <p>In the first instance of noncompliance, the Entity reported [REDACTED] that its backup Control Center (BCC) Physical Access Control System (PACS) server had unnecessary logical ports and services enabled. The noncompliance began on August 15, 2016, when the new BCC went into service, and ended on December 16, 2016, when the BCC PACS server was removed from service.</p> <p>Additionally, during the Compliance Audit, it was discovered that the Primary Control Center (PCC) Intermediate System (jump host) had unnecessary logical ports and services enabled. The noncompliance began on July 1, 2016, when the CIP v5 standards became enforceable, and ended on May 3, 2017, when the unnecessary ports on the PCC Electronic Access Control or Monitoring System (EACMS) were disabled.</p> <p>The cause of the noncompliance for both instances was that personnel responsible to perform compliance tasks related to CIP-007-6 R1 had not been provided sufficient training on the standard and the Entity's related documented processes to be able to correctly perform those tasks.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance of noncompliance was minimal because the PACS server was on a dedicated isolated PACS server network with no outside communications, and the server did not have remote login capability. Additionally, the user must be inside the Physical Security Perimeter (PSP) and use the physical console to login using the administrative username and password. Lastly, the Entity's Control Centers have medium impact BES Cyber Systems according to the CIP-002-5.1 Impact Rating Criteria and this Control Center can only control low impact BES Cyber Systems.</p> <p>The instance discovered during the Compliance Audit was minimal since the jump host is accessible only from a VPN router after multi-factor authentication or physical console access inside the PSP. Also, the issue was limited to one Cyber Asset (Intermediate System/EACMS).</p> <p>No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate the instances of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) transferred tasks performed by the BCC PACS system to the PACS server located in the PCC; 2) removed the BCC PACS server from service; 2) disabled the network ports and services on the PCC jump host (EACMS); and 3) sanitized BCC PACS server. <p>The completion of all mitigation activity has been verified.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017017545	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	01/19/2017	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED], the Entity submitted two Self-Reports, in preparation for a Compliance Audit, stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R2. In addition to these Self-Reports, an additional instance of noncompliance were found during the Compliance Audit that was conducted from [REDACTED]. All instances were consolidated and are being processed under the findings from the Compliance Audit.</p> <p>In the first instance of noncompliance, the Entity reported [REDACTED] that a patch source was not identified for its Backup Control Center (BCC) Physical Access Control System (PACS) server as required by CIP-007-6 Part 2.1. The cause of the noncompliance was that the Entity failed to follow its process to identify a patch source as required by CIP-007-6 Part 2.1. The noncompliance began on August 15, 2016, when the server entered service, and ended on December 16, 2016, when the Entity transferred the functions of the PACS to the Primary Control Center (PCC) PACS and removed the BCC PACS server from service.</p> <p>In the second instance of noncompliance, the Entity reported [REDACTED] that it failed to identify multiple devices as Electronic Access Control and Monitoring Systems (EACMS), which in turn resulted in a failure to identify a patch source and otherwise follow the Entity's patch management process for those devices. This Self-Report contained two device types that were affected: ACS Virtual Private Network (VPN) routers and a Tripwire Log Center server log aggregator. For the ACS VPN routers, the PCC and BCC routers were not identified and therefore, not classified as EACMS devices. This resulted in a failure to identify a patch source as required by CIP-007-6 Part 2.1. The noncompliance began on July 1, 2016, when CIP v5 standard became enforceable, and ended on January 19, 2017, when the Entity identified the patch source. For the Tripwire Log Center server log aggregator, the Entity determined that this device was also not identified and not correctly classified. As a result, a patch source was not identified as required by CIP-007-6 Part 2.1. The noncompliance began on July 1, 2016, when CIP v5 standard became enforceable, and ended on November 30, 2016, when the tripwire log center was identified as an EACMS. The cause of noncompliance for both instances was that the Entity failed to follow its process to identify a patch source for multiple devices as required by CIP-007-6 Part 2.1.</p> <p>During the Compliance Audit, it was discovered that for the backup Control Center (BCC) intermediate system, two applicable patches were not assessed for applicability within 35 days of being published by the designated patch source as required by CIP-007-6 Part 2.2. The cause of the noncompliance was that the Entity did not follow its process to perform assessments of patches within the required 35 calendar days as required by CIP-007-6 Part 2.2. The noncompliance began on July 1, 2016, when CIP v5 standard became enforceable, and ended on July 3, 2016, when the Entity identified the patch source.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance of noncompliance was minimal risk because the Entity reported that the PACS server did not have remote login capability. The user must be inside the Physical Security Perimeter (PSP) and use the physical console to login.</p> <p>The second instance of noncompliance was minimal risk because the Entity reported that no control of the Bulk Electric System (BES) can be performed from the VPN router, and compromise of the VPN router would only disable remote access and would not directly affect any BES Cyber System. Also, the Tripwire log center server aggregates logs from the BES Cyber System, and no control of BES is performed from this system. If a failure of logging on the repository occurred as a result of not updating the patches, each of the BES Cyber Assets would continue to log and store logs locally, such that logs would still be available for after-the-fact review. Lastly, there have been no security events associated with any of the devices.</p> <p>Lastly, the Compliance Audit discovery was minimal risk as the Intermediate System is only accessible either from a VPN router with multi-factor authentication or through physical console access inside the PSP. Therefore, ability to access the Intermediate System was reduced because only persons with authorized access can enter the PSP, which limited risk.</p> <p>No harm is known to have occurred.</p> <p>The Entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate the instances of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) updated Tripwire log center windows operating system Microsoft security patches; 2) added the VPN routers to monitor security patches; 					

<p>3) re-classified the VPN routers and Tripwire Log centers as EACMS; 4) removed the BCC PACS server from service and the task performed by BCC PACS server was transferred to PACS server located at PCC; 5) installed the patches on the BCC Intermediate System; and 6) sanitized the BCC PACS server.</p> <p>The completion of all mitigation activity has been verified.</p>
--

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017017549	CIP-007-6	R4	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	01/27/2017	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED], the Entity submitted a Self-Report, in preparation for a Compliance Audit, stating that as a [REDACTED], it was in noncompliance with CIP-007-6 R4. In addition to this Self-Report, an additional instance of noncompliance was found during the Compliance Audit that was conducted from [REDACTED]. All instances were consolidated and are being processed under the findings from the Compliance Audit.</p> <p>In the first instance of noncompliance, the Entity reported [REDACTED] that evidence was not available for logging events, generating alerts, and retain applicable event logs for 90 days as required by CIP-007-6 R4 for one Backup Control Center (BCC) Physical Access Control System (PACS) server. The cause of the noncompliance was that the Entity's lack of understanding of the standard led to a failure to identify the BCC PACS system as an Electronic Access Control or Monitoring Systems (EACMS). The noncompliance began on August 15, 2016, when it entered service, and ended on December 16, 2016, when the Entity transferred the functions of the PACS to the Primary Control Center (PCC) PACS and removed the BCC PACS server from service.</p> <p>During the Compliance Audit, it was discovered that the ACS Virtual Private Network (VPN) routers were not classified as EACMS devices. This resulted in a failure to comply with the subsequent CIP requirements, including logging events, generating alerts, and retaining applicable event logs as required by CIP-007-6 R4. The cause of the noncompliance was that the Entity's lack of understanding of the standard led to a failure to identify the routers as EACMS, which resulted in failure to log events, generate alerts, or retaining applicable event logs for 90 days. The noncompliance began on July 1, 2016, when CIP v5 standard became enforceable, and ended on January 27, 2017, when the routers were classified as EACMS and applicable requirements were implemented.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance of noncompliance was minimal because the Entity reported that the PACS server was on a dedicated, isolated PACS server network with no outside communications. Also, the PACS server did not have remote login capability, and the user would have needed to be inside the Physical Security Perimeter (PSP) and use the physical console to login.</p> <p>The instance discovered during the Compliance Audit was minimal as access to the VPN routers does not directly provide any access to Cyber Assets other than the Intermediate System. Intermediate System access is logged and alerted. Additionally, access to the VPN routers requires multi-factor authentication which limits the potential access. Lastly, the issue was limited to one Intermediate System Cyber Asset (EACMS).</p> <p>No harm is known to have occurred.</p> <p>The Entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate both instances of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) reconfigured the routers to support logging to Tripwire center; and 2) removed the BCC PACS server from service and all tasks performed were moved to PCC PACS server. <p>The completion of all mitigation activity has been verified.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017017550	CIP-007-6	R5	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	09/15/2017	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED], the Entity submitted four Self-Reports, in preparation for a Compliance Audit, stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R5. Additionally, during the Compliance Audit conducted from [REDACTED], it was discovered that the Entity had an additional instance of noncompliance. All instances were consolidated and are being processed under the findings from the Compliance Audit.</p> <p>In the first instance of noncompliance, the Entity reported [REDACTED] that the Primary Control Center (PCC) satellite clock, Backup Control Center (BCC) satellite clock, and network printer connected to the Supervisory Control and Data Acquisition (SCADA) network at the PCC were not capable of limiting the number of unsuccessful authentication attempts or alerting after a threshold of failed logon attempts as per requirement CIP-007-6, Part 5.7. The Entity was unaware of the Technical Feasibility Exception (TFE) process and did not document the equipment incapability with a TFE.</p> <p>This noncompliance began on July 1, 2016, when the CIPv5 standards became enforceable, and ended on March 2, 2017, when a TFE was submitted by the Entity.</p> <p>In the second instance of noncompliance, the Entity reported [REDACTED] that the PCC SCADA system's [REDACTED] multi-interface serial hubs and [REDACTED] multi-interface serial hub are not capable of limiting the number of unsuccessful authentication attempts or alerting after a threshold of failed logon attempts as per requirement CIP-007-6, Part 5.7. These devices are obsolete and no longer supported by the manufacturer. The Entity was unaware of the TFE process and did not document the equipment incapability with a TFE.</p> <p>This noncompliance began on July 1, 2016, when the CIPv5 standards became enforceable, and ended on March 2, 2017, when a TFE was submitted by the Entity.</p> <p>In the third instance of noncompliance, the Entity reported [REDACTED] that [REDACTED] switches and [REDACTED] switch are not capable of limiting the number of unsuccessful authentication attempts or alerting after a threshold of failed logon attempts as per requirement CIP-007-6, Part 5.7. These devices are unmanaged switches used as hubs which need only a password to login and cannot track individual users. The Entity was unaware of the TFE process and did not document the equipment incapability with a TFE.</p> <p>This noncompliance began on July 1, 2016, when the CIPv5 standards became enforceable, and ended on March 2, 2017, when a TFE was submitted by the Entity.</p> <p>In the fourth instance of noncompliance, the Entity reported [REDACTED] that [REDACTED] Programmable Communications Interfaces (PCI) and a BCC SCADA PCI which were used for Remote Terminal Unit (RTU) communications are not capable of limiting the number of unsuccessful authentication attempts or alerting after a threshold of failed logon attempts as per requirement CIP-007-6, Part 5.7. The SCADA vendor had assigned unique username/password and the credentials were not provided to the Entity. These devices are obsolete and no longer supported by the manufacturer. The Entity was unaware of the TFE process and did not document the equipment incapability with a TFE.</p> <p>This noncompliance began on July 1, 2016, when the CIPv5 standards became enforceable, and ended on September 15, 2017, when a TFE was submitted by the Entity.</p> <p>In the fifth instance of noncompliance it discovered during a Compliance Audit that the Entity failed to identify and inventory application and database default user accounts as per CIP-007-6, Part 5.2.</p> <p>This noncompliance began on July 1, 2016, when the CIPv5 standards became enforceable, and ended on April 3, 2017, when the Entity identified and inventoried application and database default user accounts.</p> <p>The cause of noncompliance for instances one through four was that the Entity failed to realize that these devices were unable to comply with CIP-007-6 Part 5.7 and they were also unfamiliar with the TFE submittal process.</p> <p>The cause of noncompliance for the fifth instance was that the Entity did not have a documented process to manage application and database default user accounts.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>The first instance of noncompliance was minimal because when a SCADA systems clock is compromised, it loses communication with the clock and will revert to its on-board clock for timekeeping. This process does not have any impact on the situational awareness of BES systems and no controls of BES is possible from this clock. Also, the network printer is used for printing screen displays and reports. This has no impact on the situational awareness of BES systems and no control of the BES is possible from this printer. Lastly, the Entity found no known exploitation or impact to the BPS as result of these issues.</p>					

	<p>The second instance of noncompliance was minimal since loss of communication with these RTU's did not impact the BES transmission network since these were not in BES transmission substations (they were used for communications to distribution substations). Additionally, the loss of communication with these RTU's did not affect situational awareness with its BES transmission system; the affect was limited to its situational awareness of distribution substations. Lastly, the Entity found no known exploitation or impact to the BPS as a result of this issue.</p> <p>The third instance of noncompliance was minimal as the capability of the switches was limited to logging of certain errors and the logs were not accessible by the Entity's logging alert center. The switches had a baseline record and firmware was updated according to the Entity's change management process. The Entity found no known exploitation or impact to the BPS as a result of this issue. The primary issue was failure to file a TFE.</p> <p>The fourth instance of noncompliance was minimal as the PCI devices did not provide any logs accessible by Entity's logging alert center. These devices were obsolete and no longer supported by the vendor and have been updated with latest released firmware. The Entity found no known exploitation or impact to the BPS as a result of this issue. The primary issue was failure to file a TFE.</p> <p>The fifth instance of noncompliance was minimal as the Entity did not understand that it needed to identify and inventory application and database default user accounts in the same manner as operating system user accounts. The database accounts were housed on a Cyber Asset with operating system user accounts protected per CIP-007-6 R5. The Entity found no known exploitation or impact to the BPS as a result of this issue.</p> <p>No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>
<p>Mitigation</p>	<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) submitted a TFE; 2) removed the clocks at the PCC and BCC from the ESP and added to the isolated PCC and BCC Demilitarized Zone (DMZ) configured on a firewall which isolated the devices from the ESP and SCADA network; and 3) removed the network printer from the ESP and added to a DMZ configured on a firewall which isolated device from ESP and SCADA network. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) submitted a TFE; and 2) replaced the RTU's, and the hubs are no longer being used. <p>To mitigate the third instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) submitted a TFE; 2) replaced the switch at the BCC with switches capable of logging and alerting failed login attempts and limiting unsuccessful logging attempts; and 3) replaced the switches at the PCC with switches capable of logging and alerting failed login attempts and limiting unsuccessful logging attempts. <p>To mitigate the fourth instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) submitted a TFE; 2) created a manual log to track user access; and 3) replaced the PCI with newer version supporting syslog functionality. <p>To mitigate the fifth instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) identified and inventoried the application and database default user accounts; and 2) modified the default account list to add a new tab titled "Application & Database" to document the user accounts.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2017017551	CIP-010-2	R1	[REDACTED] (the Entity)	[REDACTED]	07/01/2016	04/10/2017	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On [REDACTED], the Entity submitted two Self-Reports, in preparation for a Compliance Audit, stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R1. In addition to these Self-Reports, two additional instances of noncompliance were found during the Compliance Audit that was conducted from [REDACTED]. All instances were consolidated and are being processed under the findings from the Compliance Audit.</p> <p>In the first instance of noncompliance [REDACTED], the Entity reported that its Backup Control Center (BCC) Physical Access Control System (PACS) server did not have a baseline configuration as per CIP-010-2 R1 Part 1.1. The cause of the noncompliance was that the Entity failed to follow its process to create the baseline configuration. The noncompliance began on August 15, 2016, when the BCC PACS entered into service and ended on December 16, 2016, when the Entity transferred the functions of the PACS to the Primary Control Center (PCC) PACS.</p> <p>In the second instance of noncompliance [REDACTED], the Entity reported that it failed to identify multiple devices as Electronic Access Control and Monitoring Systems (EACMS), which resulted in a failure to establish baselines for the devices. The devices included Access Control Server (ACS) Virtual Private Network (VPN) routers where the PCC and BCC routers did not have a developed baseline and a Tripwire Log Center server (log aggregator) baseline configuration was not developed. The cause of the noncompliance was that the Entity's lack of understanding of the standard led to a failure to identify the routers and log aggregator server as EACMS, which resulted in failure to develop baseline configurations. The ACS VPN router noncompliance began on July 1, 2016, when CIP v5 went into effect, and ended on January 28, 2017, when the Entity developed baselines for the Cyber Assets (CAs). The Tripwire Log Center noncompliance began on July 1, 2016, and ended on November 30, 2016, when the log aggregator server was reclassified as an EACMS and the baseline configuration was developed.</p> <p>During the Compliance Audit, it was discovered that two switches in the PCC and one switch at the BCC did not have a baseline configuration as per CIP-010-2 R1 Part 1.1.4. The cause of the noncompliance was that the Entity's process did not have sufficient procedural controls to ensure baselines were developed. This instance of noncompliance began on January 18, 2017, when the switches entered service, and ended on April 10, 2017, when the baseline was created.</p> <p>Additionally, during the Compliance Audit, it was discovered that the PCC Intermediate System was updated automatically and the Entity did not authorize and document the changes as per CIP-010-2 R1 Part 1.2. The cause of the noncompliance was that the Entity's process did not have sufficient procedural controls to ensure automatic updates were disabled. This instance of noncompliance began on July 1, 2016, when CIP v5 went into effect, and ended on July 18, 2016 when the Entity authorized the change and updated the baseline document.</p> <p>The aggregate of the issues began on July 1, 2016 and ended on April 10, 2017.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system.</p> <p>In the first Self-Report, the Entity reported that the PACS server was on a dedicated, isolated PACS server network with no outside communications allowed and the PACS server did not have remote login capability. Therefore, the user would have needed to be inside the PSP and used the physical console to login.</p> <p>In the second Self-Report, the Entity reported that no control of the BES could be performed from the VPN router and failure of the VPN routers would have only disabled remote access and would not have directly affected any BES Cyber System. Additionally, the log aggregator server aggregates logs from the BES Cyber System and no controls of BES could be performed from this system. If a failure of logging on the repository occurred as a result of not updating the patches, each of the BES Cyber Assets would have continued to log and store logs locally, such that logs would have still been available for after-the-fact review. The Entity identified that there were no security events associated with any of the devices.</p> <p>Lastly, for the Compliance Audit discoveries, the switches' baselines existed and the issue was limited to the lack of documented logical network accessible ports within those baselines and the Intermediate System was only accessible from a VPN router with multi-factor authentication or through physical console access inside the PSP. Therefore, ability to access the Intermediate System was reduced, which limited risk.</p> <p>No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					

Mitigation	<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none">1) transferred the tasks performed by the BCC PACS to the PCC PACS server, which eliminated the CIP-010-2 R1 applicability because the CA was no longer a PACS;2) BCC PACS server was removed from service; and3) developed a "new Asset installation checklist" for installing new devices; <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none">1) reclassified the log aggregator server as an EACMS and the baseline configuration was developed;2) reclassified the VPN routers as EACMS and the baseline configurations were developed; and3) conducted a mock audit and CIP V5 boot camp for its CIP team to ensure better understanding of the CIP standards and managing the CIP environment. <p>To mitigate the third instance of noncompliance, the Entity:</p> <ol style="list-style-type: none">1) updated the baselines for the switches to include logical network accessible ports. <p>To mitigate the forth instance of noncompliance, the Entity:</p> <ol style="list-style-type: none">1) authorized the changes and updated the baselines with current configuration;2) disabled automatic update, and the configuration change management process was followed for further updates;3) modified its CIP-010-2 R1 configuration management procedure to add controls for developing baselines and disabling automatic updates for Cyber Assets; and4) developed a new Asset installation checklist for installing new devices.
-------------------	--

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019352	CIP-010-2	R4	[REDACTED] (the Entity)	[REDACTED]	04/01/2017	10/31/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a “noncompliance,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On December 1, 2017, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-010-2 R4. The Entity determined that it had three instances of noncompliance involving [REDACTED] Transient Cyber Assets (TCA); [REDACTED] of which were associated with high impact BES Cyber Systems (BCS) and [REDACTED] of which were associated with medium impact BCS.</p> <p>For the first instance of noncompliance, the Entity discovered that all entity personnel were able to use the TCAs irrespective of authorization status. The noncompliance began on April 1, 2017, when the standard became enforceable, and ended on October 31, 2018, when the Entity implemented Active Directory Organizational Units, enabling them to limit use on a group basis.</p> <p>For the second instance of noncompliance, the Entity had one or more software applications installed on its TCAs that were not properly patched according to its process. The noncompliance began on April 1, 2017, when the standard became enforceable, and ended on May 25, 2017.</p> <p>For the third instance of noncompliance, the Entity had one or more software applications installed on the TCAs which were not necessary to perform business functions. The noncompliance began on April 1, 2017, when the standard became enforceable, and ended on December 14, 2017, when the software was removed.</p> <p>The cause of all three instances of noncompliance was that the Entity’s process for managing TCAs lacked sufficient rigor and internal controls.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity determined that all the TCAs were stored within a Physical Security Perimeter (PSP) when not under the control of someone with authorized access. Electronic access to the TCAs was limited to Entity employees. The TCAs had various cyber security controls installed on them (Carbon Black, Anti-Virus, and Log Monitor). Lastly, the patching-related issue, in the second instance of noncompliance, was limited to 55 days, a duration which is within the span of a single patch cycle under the analogous patching requirement for BES Cyber Systems (CIP-007-6 R2). No harm is known to have occurred.</p> <p>MRO considered the Entity’s compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate the first instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) implemented Active Directory Organizational Units (OUs), creating an OU exclusively for individuals authorized to use TCAs; and 2) implemented improved technical and procedural controls over its TCAs. <p>To mitigate the second instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) applied applicable security patches to the TCAs; and 2) implemented improved technical and procedural controls over its TCAs. <p>To mitigate the third instance of noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) removed applications that were not needed; 2) implemented improved technical and procedural controls over its TCAs. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022101	CIP-007-6	R2	[REDACTED] (the Entity)	[REDACTED]	02/13/2019	03/12/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On April 9, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-007-6 R2.</p> <p>The noncompliance occurred when an individual had to leave due to a family emergency and was in the middle of a patch management process. After another individual resumed the work, they missed relevant information that resulted in the Entity's patch management process not being correctly followed. Ultimately, a Microsoft patch for 14 Cyber Assets (six medium impact BES Cyber Assets (MIBCA)s and eight Protected Cyber Assets (PCAs)) was not evaluated within the required 35 days.</p> <p>The cause of the noncompliance was the Entity failed to follow its CIP-007-6 patch management process by not evaluating a patch within the required 35 days.</p> <p>This noncompliance began on February 13, 2019, when the patch should have been evaluated in the required timeframe, and ended on March 12, 2019, when the patch was added to a security patch mitigation plan.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity identified the 14 Cyber Assets of issue as serially connected and were not accessible via External Routable Connectivity (ERC), thereby limiting the attack vectors to the Cyber Assets. All serial communication in relation to this issue are owned and controlled by the Entity. The impacted Cyber Assets are located within a Physical Security Perimeter (PSP) with dual factor authentication, which is above the requirements for MIBCA)s. Additionally, for the Cyber Assets without ERC, the Entity only applies patches twice a year, and this impacted patch was added to a current security patch mitigation plan which scheduled it for the June patch maintenance period. Therefore, the delay in the evaluation did not impact the June patch maintenance period. Lastly, the duration of the issue was limited to 28 days, reducing the exposure of the vulnerability on the Cyber Assets. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) added this patch to a security patch mitigation plan; 2) provided human performance training to impacted individuals; and 3) updated its procedure to provide better guidance for the Entity's Batch Patch 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
MRO2019022346	CIP-004-6	R4	[REDACTED] (the Entity)	[REDACTED]	06/01/2019	07/30/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 7, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R4.</p> <p>The Entity reported that during an internal compliance control spot check, it identified a high impact BES Cyber System Information (BCSI) repository which was not validated for the 15 calendar month access account review as per Part R4.4. The repository is a backup file server containing high impact BCSI. The Backup BCSI repository was added to the guideline document on February 9, 2018, however, it was not added to the access management program document that is used for complying with NERC CIP-004-6 Requirement 4.</p> <p>The cause of the noncompliance was that the Entity failed to follow its access management process for the 15 calendar month access account review. Additionally, the Entity's process was deficient since it did not ensure the synchronization of BCSI repositories between the guideline document and the access management program document.</p> <p>The noncompliance began on June 1, 2019, when the 15 month verification should have been completed, and ended on July 30, 2019, when the access to the designated BCSI storage location was officially reviewed and signed verifying that only the appropriate personnel have authorized access.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue was discovered during the internal compliance spot-check, which limited the duration and risk of the noncompliance. The backup file server resides within a Physical Security Perimeter (PSP) and protected as per CIP-006-6. Additionally, physical access to the PSP was reviewed before the 15 month calendar review in accordance with CIP-004-6 part 4.4. BCSI information is stored in an encrypted format, and only the server administrators have access. The server administrator approved BCSI access was reviewed before the 15 month calendar review and no issues were found. Lastly, BCSI access is monitored and alerted for changes using Active Directory.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) verified authorized electronic user access to BCSI repository; 2) reviewed and reconciled BCSI repository lists for the missing BCSI repository; 3) modified guidelines to have a single approver for the guideline document and the access management program document which will enable synchronization of the two documents; and 4) modified the Access Management procedure to reference the guideline document for the list of designated BCSI repositories which will eliminate maintaining two lists for high impact BCSI repository 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
MRO2019022382	CIP-004-6	R1	[REDACTED] (the Entity)	[REDACTED]	04/01/2019	04/04/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 8, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-004-6 R1.</p> <p>On April 1, 2019, the employee working in high impact control center reported that security awareness posters were not issued for the calendar quarter of Q1 2019 in compliance with CIP-004-6 R1, Part 1.1.</p> <p>The cause of the noncompliance was that the Entity's process did not provide sufficient reminders to the Subject Matter Expert (SME) responsible for issuing the calendar quarter security awareness posters.</p> <p>The noncompliance began on April 1, 2019, which was one day after the quarterly access review, and ended on April 4, 2019, when the Q1 security awareness posters were posted.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The instance was minimal because the noncompliance was observed and reported by the SME, which limited the duration of the noncompliance to four days. Additionally, the security awareness program is intended to be an informational program and did not impact the reliability or performance of the BES. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) posted security awareness posters; 2) updated the responsible SME's calendar with security awareness posters due date reminders; 3) created work order tickets for each quarterly task to provide an additional layer of controls to ensure completion of the quarterly task; and 4) added security awareness tracking spreadsheet to the Compliance CIP-004 SharePoint site. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019022387	CIP-006-6	R2	[REDACTED] (the Entity)	[REDACTED]	07/29/2019	07/29/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On October 8, 2019, the Entity submitted a Self-Log stating that, as a [REDACTED], it was in noncompliance with CIP-006-6 R2.</p> <p>The Entity reported that an employee with escorted physical access was allowed into a high impact Physical Security Perimeter (PSP) by another authorized individual and was not escorted for a duration of 10 minutes resulting in noncompliance with CIP-006-6 R2, Part 2.1.</p> <p>The cause of the noncompliance was that the individual, who was an employee with authorized NERC unescorted access failed to follow the Entity's process for allowing an employee without NERC unescorted physical access into a high impact PSP and escorting them the entire duration of the visit.</p> <p>The noncompliance began on July 29, 2019, when the individual without unescorted access was not escorted, and ended within 10 minutes on July 29, 2019, when the individual was escorted out of the PSP.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was minimal because the noncompliance was observed and reported by a second employee (The Director), which limited the duration of the noncompliance to only 10 minutes. The visitor was an employee with a current background check on file. Additionally, the BES Cyber Assets housed by the PSP of issue were the Energy Management System/Supervisory Control and Data Acquisition system for which the individual did not have electronic access. Lastly, the employee documented their presence on the visitor log, creating a record of his or her presence in the PSP. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) Director escorted the individual of issue to the PSP exit; 2) had management review the importance of its visitor control program for security and escorting with the employee who did not properly follow the escorting requirements; 3) employee acting as escort during this noncompliance completed the annual NERC CIP training to maintain access to NERC CIP High Impact BES Cyber System areas following the incident; and 4) discussed the importance of security and compliance with NERC requirements in subsequent division meetings. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2019021261	CIP-003-6	R1	[REDACTED] (the Entity)	[REDACTED]	10/01/2017	09/06/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On February 22, 2019, the Entity submitted a Self-Report stating that as a [REDACTED], it was in noncompliance with CIP-003-6 R1.</p> <p>The Entity reported that it failed to obtain CIP Senior Manager approval within 15 months of the previous approval. This occurred when the Entity's Primary Compliance Contact (PCC) reviewed and approved 14 cyber security policies instead of its CIP Senior Manager performing the review. The Entity's document management tool assigned the review and approval task to the PCC instead of the CIP Senior Manager.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for the review and approvals from the CIP Senior Manager of its cyber security policies once every 15 calendar months.</p> <p>The noncompliance began on October 1, 2017, when the CIP Senior Manager failed to approve the cyber security policies 15 months from last approval, and ended on September 6, 2018, when the CIP Senior Manager approved the cyber security policies</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity determined that 12 out of the 14 cyber security policies were not altered from the last review and approval. The cyber security policies were reviewed and approved by the PCC instead of the CIP Senior Manager twice since the last approval; each meeting the 15 month review cycle. The PCC is part of the CIP Subject Matter Expert (SME) team and is the NERC Compliance Manager, limiting the issue to the approval of the cyber security policies by the CIP Senior Manager. Additionally, this issue was resolved by the CIP Senior Manager reviewing and approving the cyber security policies and did not require any changes to those policies as a result, limiting this issue to only documentation of approval. Lastly, the Entity's Control Centers only contain medium impact BES Cyber Systems and the Control Centers are only responsible for low impact BES Cyber Systems. No harm is known to have occurred.</p> <p>The Entity has no relevant compliance history.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) had its CIP Senior Manager review and approve the 14 cyber security policies of issue; 2) updated its document workflow tool to have the review and approval tasks assigned directly to the CIP Senior Manager; and 3) confirmed the updates to the document workflow tool for the review and approval tasks successfully were assigned to the CIP Senior Manager. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020734	CIP-006-6	R1	[REDACTED] (the Entity)	[REDACTED]	10/11/2018	10/11/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>On November 5, 2018, the Entity submitted a Self-Report stating that as [REDACTED], it was in noncompliance with CIP-006-6 R1. [REDACTED]</p> <p>The Entity discovered that it failed to log an individual's access into one Physical Security Perimeter (PSP) as required by Part 1.8. This occurred on October 11, 2018, when an operator attempted to access the PSP and found that his badge was not working properly. The operator was then granted access by another operator, however they did not log in as required by the Entity's process.</p> <p>The cause of the noncompliance was that the Entity failed to follow its process for logging access to PSPs for individuals with authorized unescorted access.</p> <p>The noncompliance began on October 11, 2018, when the access was not logged, and ended on the same date as it was instantaneous in nature.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The duration of the issue was limited to one day, one individual, and one instance. Additionally, the individual who accessed the PSP without logging into the PSP was authorized for access to the PSP. No harm is known to have occurred.</p> <p>The Entity has no relevant history of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the Entity:</p> <ol style="list-style-type: none"> 1) performed an extent-of-condition review and found no other instances of access being granted when a badge was not working; 2) sent an email reminding employees of the proper procedure for handling inoperative badges; and 3) held refresher training on the procedure for handling inoperative badges. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019941	CIP-002-5.1	R1.	[REDACTED]	[REDACTED]	07/01/2016	10/10/2018	Off-site Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			<p>During a Compliance Audit conducted from [REDACTED], NPCC determined that [REDACTED] (the entity), as a [REDACTED], was in noncompliance with CIP-002-5.1 R1 (1.1, 1.2, 1.3). The entity failed to implement a process that identified BES Cyber Systems.</p> <p>This noncompliance started on July 1, 2016 when the entity failed to implement a process to assess applicable assets for BES Cyber Systems. The noncompliance ended on October 10, 2018 when the entity implemented a process to identify applicable BES Cyber Systems. The identification process resulted in one new medium impact BES Cyber System without external routable connectivity.</p> <p>Specifically, the entity acquired one facility from another entity on [REDACTED] and contracted with the other entity for all O&M Services including the CIP compliance responsibilities for the facility. However, the contracted entity's CIP responsible personnel did not have the knowledge and training to effectively evaluate the equipment within the facility because the installation was completely constructed and commissioned by the equipment vendor.</p> <p>The failure of the entity to implement a process to assess applicable assets for BES Cyber Systems led to other CIP controls being missed. The entity conducted patch management on an annual basis. The Cyber Assets were put in service in 2016, but patch management was not completed until 2018, missing the 2017 cycle.</p> <p>The root cause of this noncompliance was lack of understanding of the CIP identification of the site, and a lack of understanding of the requirement used in BES Reliability Operating Services.</p>					
Risk Assessment			<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify BES Cyber Systems that are applicable to the CIP Standards, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets (CA) to unauthorized use. The CA in scope were part of a turnkey solution provided by the vendor and are used to increase the capacity of the transmission lines at this site. If the Facility or associated CA became unavailable, the transmission line would remain in service, but at a reduced capacity. The entity could bypass the CA in real-time to maintain the operations of the line if any issues or alarms were identified by operators.</p> <p>Although the entity failed to afford the required CIP protections to the CA in scope, it reduced the risk of compromise by applying physical access controls and limiting physical access to only personnel with a business need. Specifically, the CA in scope were located within a [REDACTED] and additionally, [REDACTED]. [REDACTED] access was restricted to only a limited set of individuals. Physical access was granted and tracked in accordance with the contracted entity's CIP program. The entity required completed Personnel Risk Assessments (PRAs) and Cyber Security training before access could be granted and has a policy to revoke access upon termination of personnel within 24 hours, reducing the likelihood of inappropriate access to the CA. Completion is required every fifteen months. As a result of identification of the BES Cyber System, there was no change or update required to the physical access process in place and/or privileges provided to any individual.</p> <p>The CA in scope do not have external routable connectivity or dial-up access. After review of the CIP controls, the entity found that there were patches required to be installed and several other CIP controls to implement that were not originally configured. A typical patch management schedule for these Cyber Assets is annual during a scheduled outage. The devices were placed in service in the summer of 2016, which would have initiated the process for tracking patches. Patches would have been tracked from that point and applied in 2017 during an outage. As the BCA is generally by-passed (i.e. not utilized) in the winter, patches would have been applied in 2017Q4 (Winter Season) to reduce the impact on operations. Once included in the program the system was brought up to date in Q42018. Based on this schedule the entity missed one cycle of patch management (2017).</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no relevant underlying causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) Performed equipment training 2) Conducted an onsite walkthrough of the facility 3) Approved BES CA List 4) Shared lessons learned 5) Developed/Revised Procedures 6) Developed Webinar performing an active CVA 7) Provided Webinar/Training to Personnel 8) Integrated the addition of the active CVA into all projects 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2018019942	CIP-002-5.1	R2.	[REDACTED]	[REDACTED]	07/01/2016	10/10/2018	Off-site Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>On [REDACTED], NPCC auditors submitted an Off-site Audit finding, stating that [REDACTED] (the entity), as a [REDACTED], was in noncompliance with CIP-002-5.1 R2. (2.1., 2.2.) after auditors discovered the entity failed to identify medium impact BES Cyber Systems.</p> <p>This noncompliance started on July 1, 2016 when the entity failed to review the identifications in requirement R1 and have its [REDACTED] or delegate approve the identifications. The noncompliance ended on October 10, 2018 when the entity implemented a process to identify its BES Cyber Systems and had its [REDACTED] approve the identifications. The identification process resulted in one new medium impact BES Cyber System without external routable connectivity.</p> <p>Specifically, the entity acquired the facility from another entity on [REDACTED] and contracted the other entity for all O&M Services including the CIP compliance responsibilities for the facility. However, the contracted entity's CIP responsible personnel did not have the knowledge/training to effectively evaluate the equipment within the facility because the installation was completely constructed and commissioned by the equipment vendor.</p> <p>The root cause of this noncompliance was lack of understanding of the CIP identification of the site, and a lack of understanding of BROS functionality and of the equipment at the site.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify BES Cyber Systems that are 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 BCA and associated Cyber Assets in scope were part of a turnkey solution provided by the vendor. The Cyber Assets are used to increase the capacity of the transmission lines at this site. If the Facility or associated Cyber Assets became unavailable or are by-passed for economic reasons, the transmission line would remain in service, but at a reduced capacity. If operators identify any issues or alarms with the BCA, the entity could bypass the BCA in real-time to maintain the operations of the line.</p> <p>Although the entity failed to afford the required CIP protections to the Cyber Assets in scope, it reduced the risk of Cyber Assets becoming compromised by applying physical access controls and limiting physical access to only personnel with a business need. Specifically, the Cyber Assets were located within a [REDACTED] and additionally, [REDACTED]. [REDACTED] access was restricted to only a limited set of individuals. Physical access was granted in accordance with the [REDACTED] CIP program and tracked by [REDACTED] through [REDACTED] standard process. As a result of identification of the BES Cyber System, there was no change or update required to the physical access process in place and/or privileges provided to any individual.</p> <p>The Cyber Assets do not have external routable connectivity or dial-up access. After review of the CIP controls, the entity found that there were patches required to be installed and several other CIP controls to implement that were not originally configured. A typical patch management schedule for these Cyber Assets is annual during a scheduled outage. The devices were placed in service in the summer of 2016, which would have initiated the process for tracking patches. Patches would have been tracked from that point and applied in 2017 during an outage. As the BCA is generally by-passed (i.e. not utilized) in the winter, patches would have been applied in 2017Q4 (Winter Season) to reduce the impact on operations. Once included in the program the system was brought up to date in Q42018. Based on this schedule the entity missed one cycle of patch management (2017).</p> <p>No harm is known to have occurred as a result of this noncompliance.</p> <p>NPCC considered the entity's compliance history and determined there were no relevant underlying causes.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) Performed equipment training 2) Conducted an onsite walkthrough of the facility 3) Approved BESCA List 4) Shared lessons learned 5) Developed/Revised Procedures 6) Developed Webinar performing an active CVA 7) Provided Webinar/Training to Personnel 8) Integrated the addition of the active CVA into all projects 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2019022070	CIP-007-6	R4.	[REDACTED]	[REDACTED]	06/22/2018	04/26/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)		<p>On August 15, 2019, [REDACTED] (the entity) submitted a Self-Log stating that as a [REDACTED] and [REDACTED], it was in noncompliance with CIP-007-6 R4 (4.3, 4.4). Specifically, the entity failed to retain all applicable event logs for the required 90 days and failed to review a summarization or sampling of logged events.</p> <p>The entity discovered the issue while trying to accomplish an enhancement to the monitoring process that detects event logging failures. The SCADA workstation was logging at the local level, but it was unable to retain logs for the full 90 days. When operating correctly, the logs are fed from the workstation to a configuration management application that retains the logs for the required 90 days. However, the management application failed to capture logs beginning on June 22, 2018.</p> <p>The entity was unable to determine why the configuration monitoring agent failed to communicate with the management server and stopped sending logs. The entity verified the scope by checking if other assets were not reporting and found the issue was confined to just the lone workstation. Initially installed on November 4, 2016, the SCADA workstation operated correctly, sending logs to the configuration management application until June 22, 2018, when it stopped logging for reasons that remain unclear.</p> <p>The entity failed to review a summarization or sampling of the logged events in less than 15 days.</p> <p>This noncompliance started on June 22, 2018, when the SCADA workstation stopped logging. The noncompliance ended on April 26, 2019, when the workstation resumed logging.</p> <p>The root cause for this noncompliance was a weak process for detecting the issue when logging failed. The entity was also unable to establish a technical reason why the workstation stopped logging.</p>						
Risk Assessment		<p>The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to retain event logs for 90 days and failing to review a sample of the events could potentially cause Cyber Security incidents to go undetected or impede the entity's ability to investigate incidents.</p> <p>However, the workstation had security monitoring software installed as well as all technical security controls [REDACTED] in place during the period of noncompliance which would have logged any suspicious network activity and alerted [REDACTED] directly, independently of the configuration management application. The workstation was also located [REDACTED] that was afforded all the required CIP security protocols. Finally, the workstation is a Protected Cyber Asset (PCA) that does not perform any reliability tasks and represents less than one percent (0.18%) of the entity's assets.</p> <p>No harm is known to have occurred as a result of this noncompliance.</p>						
Mitigation		<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) ensured the asset configuration showed the workstation was set up for logging and monitoring; 2) created a new configuration management application dashboard and associated health widgets to better identify non-communicating assets (including failures in event logging); 3) updated task list sheet to require IT personnel to check the new dashboard with daily and weekly requirements; 4) trained [REDACTED] on dashboard non-communicating assets; and 5) conducted an extent of condition by reviewing internal monitoring software to ensure all in-scope CIP assets are being logged. 						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021026	CIP-004-6	R5	[REDACTED]	[REDACTED]	10/13/2018	10/15/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On January 23, 2019, the entity submitted a Self-Report stating that, [REDACTED], it was in noncompliance with CIP-004-6 R5.</p> <p>In this noncompliance, a contractor's final day for the entity was on October 12, 2018. The terminating manager initiated the termination action with human resources but did not complete all necessary actions in the entity's termination checklist for employees and contractors until the following business day. Specifically, the terminating manager did not notify [REDACTED] IT [REDACTED] or the Security Operations Center, nor did the terminating manager submit a termination request until the following business day. Therefore, physical access and Interactive Remote Access were not removed until October 15, 2018.</p> <p>The root cause of this noncompliance was inadequate training of managers on the documented process to revoke access upon termination because the instance arose from a manager's failure to adhere to the process.</p> <p>This noncompliance involves the management practices of verification and workforce management. Verification is involved because the entity failed to confirm that a terminated individuals' physical access or Interactive Remote Access were removed within 24 hours of termination. Workforce management is involved because the entity failed to effectively manage employee permissions to access assets.</p> <p>This noncompliance began on October 13, 2018, when 24 hours passed after termination without corresponding access revocation, and ended on October 15, 2018, when access was revoked.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this instance of noncompliance is allowing the opportunity for a former employee or contractor to access, and potentially compromise, Bulk Electric System Cyber Systems. The risk is minimized here because the duration of the instance was just two days. Further, the contractor's laptop and security badge were collected on the contractor's last day. Additionally, the individual impacted was in good standing with the company, had a valid Personal Risk Assessment, and was up to date on NERC CIP training. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances involved different facts and circumstances that are not related to the instant noncompliances. Additionally, the entity has demonstrated an ability to promptly identify and correct these types of noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) addressed the instance and removed the relevant access permissions; 2) performed an extent of condition; and 3) enhanced existing documentation for manager's termination steps. The entity modified the [REDACTED] highlight that two steps are needed to fully complete a termination action. In addition to the revised document, the storage location for the Manager's checklist will be made more accessible on the entity's internal webpage. The entity also trained managers on this new checklist which helps prevent recurrence. 4) established a biannual detective control in the company compliance management system. Every 6 months a statistically significant sample set of terminations requiring access revocations will be reviewed to verify access was revoked in accordance with the entity's programs and any applicable NERC Requirements. The tasks associated with executing and tracking this detective control will be entered into the entity's [REDACTED] as a Control Procedure; and 5) established biennial assurance control in the entity's compliance management system. Stakeholders involved with employee terminations will convene to review the termination process to 1) affirm that the process is working appropriately, and 2) identify any improvements to the termination process to align with any applicable NERC Requirements. The tasks associated with executing and tracking this control will be entered into [REDACTED] as a Control Procedure. The first occurrence of this control will be completed by the end of Q1 2020, then by the end of Q1 2022, Q1 2024, etc. at the longest interval. In the event of another reportable incident, the Control Procedure will be implemented and associated tasks completed. The subsequent review will be completed no more than 24 months from this completion date. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021477	CIP-004-6	R5	[REDACTED]	[REDACTED]	1/30/2019	2/8/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On May 2, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5.</p> <p>In this noncompliance, an employee's physical access was not removed within 24 hours of termination. The employee's last day of employment with the entity was on January 29, 2019, and physical access was not removed until February 8, 2019. The terminating manager submitted a back-dated termination request on February 7, 2019. On February 7, 2019, an entity detective control triggered an access review as a result of the manager entering the termination request, which identified that the employee's badge was still active in the entity's physical access management system and had not been disabled.</p> <p>The root cause of this noncompliance was inadequate training of managers on the documented process to revoke access upon termination because this instance arose from a manager's failure to adhere to the process. The terminating manager did not notify [REDACTED] IT [REDACTED] or the Security Operations Center, nor did the terminating manager submit a termination request on time.</p> <p>This noncompliance involves the management practices of verification and workforce management. Verification is involved because the entity failed to confirm that a terminated individuals' physical access or Interactive Remote Access were removed within 24 hours of termination. Workforce management is involved because the entity failed to effectively manage employee permissions to access assets.</p> <p>The noncompliance began January 30, 2019 when 24 hours passed after termination without access revocation, and ended on February 8, 2019, when access was revoked.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this instance of noncompliance is allowing the opportunity for a former employee or contractor to access, and potentially compromise, Bulk Electric System Cyber Systems. The risk is minimized here because the noncompliance was discovered by an internal detective control indicating strong internal controls. Further minimizing the risk, the employee's badge was returned on their last day of employment. Additionally, the individual was in good standing with the company and had a valid Personal Risk Assessment. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances involved different facts and circumstances that are not related to the instant noncompliances. Additionally, the entity has demonstrated an ability to promptly identify and correct these types of noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) addressed the instance and removed the relevant access permissions; 2) performed an extent of condition; and 3) enhanced existing documentation for manager's termination steps. The entity modified the [REDACTED] highlight that two steps are needed to fully complete a termination action. In addition to the revised document, the storage location for the Manager's checklist will be made more accessible on the entity's internal webpage. The entity also trained managers on this new checklist which helps prevent recurrence. 4) established a biannual detective control in the company compliance management system. Every 6 months a statistically significant sample set of terminations requiring access revocations will be reviewed to verify access was revoked in accordance with the entity's programs and any applicable NERC Requirements. The tasks associated with executing and tracking this detective control will be entered into the entity's [REDACTED] as a Control Procedure; and 5) established biennial assurance control in the entity's compliance management system. Stakeholders involved with employee terminations will convene to review the termination process to 1) affirm that the process is working appropriately, and 2) identify any improvements to the termination process to align with any applicable NERC Requirements. The tasks associated with executing and tracking this control will be entered into [REDACTED] as a Control Procedure. The first occurrence of this control will be completed by the end of Q1 2020, then by the end of Q1 2022, Q1 2024, etc. at the longest interval. In the event of another reportable incident, the Control Procedure will be implemented and associated tasks completed. The subsequent review will be completed no more than 24 months from this completion date. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021621	CIP-004-6	R5	[REDACTED]	[REDACTED]	2/16/2019	2/22/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On May 28, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-004-6 R5.</p> <p>In this noncompliance, the entity discovered a retired employee's unescorted physical access had not been removed as required. The retiree's employment was terminated on February 15, 2019, and his physical access was not removed until February 22, 2019, when the termination manager submitted a back dated termination notice. On February 22, 2019, an entity detective control triggered an access review as a result of the manager entering the termination request, which identified that the retiree still had unescorted physical access privileges.</p> <p>The root cause of this noncompliance was inadequate training of terminating managers on the documented process to revoke access upon termination because this instance arose from a terminating manager's failure to adhere to the process.</p> <p>This noncompliance involves the management practices of verification and workforce management. Verification is involved because the entity failed to confirm that a terminated individuals' physical access or Interactive Remote Access were removed within 24 hours of termination. Workforce management is involved because the entity failed to effectively manage employee permissions to access assets.</p> <p>This noncompliance started on February 16, 2019, when 24 hours passed after termination without access revocation and ended on February 22, 2019, when the entity revoked the retiree's access.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by this instance of noncompliance is allowing the opportunity for a former employee or contractor to access, and potentially compromise, Bulk Electric System Cyber Systems. The risk is minimized here because the entity discovered the noncompliance through an internal detective control which indicates strong internal controls. Additionally, the retiree was in good standing with the company and had a valid Personal Risk Assessment. Lastly, the entity confirmed that the retiree made no access attempts during the noncompliance. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances involved different facts and circumstances that are not related to the instant noncompliances. Additionally, the entity has demonstrated an ability to promptly identify and correct these types of noncompliances.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) addressed the instance and removed the relevant access permissions; 2) performed an extent of condition; and 3) enhanced existing documentation for manager's termination steps. The entity modified the [REDACTED] highlight that two steps are needed to fully complete a termination action. In addition to the revised document, the storage location for the Manager's checklist will be made more accessible on the entity's internal webpage. The entity also trained managers on this new checklist which helps prevent recurrence. 4) established a biannual detective control in the company compliance management system. Every 6 months a statistically significant sample set of terminations requiring access revocations will be reviewed to verify access was revoked in accordance with the entity's programs and any applicable NERC Requirements. The tasks associated with executing and tracking this detective control will be entered into the entity's [REDACTED] as a Control Procedure; and 5) established biennial assurance control in the entity's compliance management system. Stakeholders involved with employee terminations will convene to review the termination process to 1) affirm that the process is working appropriately, and 2) identify any improvements to the termination process to align with any applicable NERC Requirements. The tasks associated with executing and tracking this control will be entered into [REDACTED] as a Control Procedure. The first occurrence of this control will be completed by the end of Q1 2020, then by the end of Q1 2022, Q1 2024, etc. at the longest interval. In the event of another reportable incident, the Control Procedure will be implemented and associated tasks completed. The subsequent review will be completed no more than 24 months from this completion date. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021233	CIP-007-6	R4	[REDACTED]	[REDACTED]	7/1/2016	12/7/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On March 8, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-007-6 R4.</p> <p>On August 7, 2018, a new entity employee assigned to Technical Feasibility Exceptions (TFEs) discovered a mismatch of internal device lists vs. externally reported device lists in [REDACTED] for device counts related to existing TFEs.</p> <p>Upon further analysis, the entity determined this incident had been occurring since the start of CIP v5 compliance on July 1, 2016. After consulting with internal stakeholders and subject matter experts, the entity discovered that there were gaps in the existing process and a lack of transparency with the internal TFE reporting process. There were several opportunities for error and the entity had insufficient controls to ensure that accurate information regarding TFEs was updated in [REDACTED]. The initial analysis concluded that [REDACTED] assets in [REDACTED] had either been removed from service or had been placed into service but were not accurately updated in [REDACTED]. Further analysis concluded that the following number of assets were related to CIP-007-6, R4.3: [REDACTED]</p> <p>This noncompliance involves the management practices of work management and information management. The root cause of this noncompliance was an ineffective communication process to ensure that accurate information regarding TFEs was updated in [REDACTED]. The entity also lacked an effective verification control to ensure the accuracy of information in [REDACTED].</p> <p>This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-007-6 R4 and ended on December 7, 2018, when the entity updated its TFE device lists in [REDACTED] using the simplified process and new spreadsheet.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to identify and manage TFE assets is the entity may fail to implement mitigating measures to the vulnerabilities that are present in assets that have technical limitations. The risk is minimized because all of the assets at issue were properly cataloged within the entity's own database, which resulted in all of the assets being afforded the required protections within the entity's CIP program for the duration of the noncompliance. Therefore, this is primarily a documentation issue. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, [REDACTED] determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances involved different facts and circumstances and arose from different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the asset management device list to match [REDACTED] 2) performed an extent of condition review on all TFE device population; 3) simplified the entity TFE internal reporting process; and 4) implemented controls and communicated the documented process to all stakeholders. <p>[REDACTED] has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021230	CIP-007-6	R5	[REDACTED]	[REDACTED]	7/1/2016	12/7/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On March 8, 2019, the entity submitted Self-Reports stating that, [REDACTED] it was in noncompliance with CIP-007-6 R5.</p> <p>On August 7, 2018, a new entity employee assigned to Technical Feasibility Exceptions (TFEs) discovered a mismatch of internal device lists vs externally reported device lists in [REDACTED] for device counts related to existing TFEs. Upon further analysis, the entity determined that this incident had been occurring since the start of CIP v5 on July 1, 2016. After consulting with internal stakeholders and subject matter experts (SMEs), the entity discovered that there were gaps in the existing process and a lack of transparency with the internal TFE reporting process. There were several opportunities for error and the entity had insufficient controls to ensure that accurate information regarding TFEs was updated in [REDACTED]</p> <p>The entity's initial analysis concluded that [REDACTED] had either been removed from service or had been placed into service, but were not accurately updated in [REDACTED]. Further analysis concluded that the following number of assets were specifically impacted: [REDACTED]</p> <p>This noncompliance involves the management practices of work management and information management. The root cause of this noncompliance was an ineffective communication process to ensure that accurate information regarding TFEs was updated in [REDACTED]. The entity also lacked an effective verification control to ensure the accuracy of information in [REDACTED]</p> <p>This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-007-6 R4 and ended on December 7, 2018, when the entity updated its TFE device lists in [REDACTED] using the simplified process and new spreadsheet.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to identify and manage TFE assets is the entity may fail to implement mitigating measures to the vulnerabilities that are present in assets that have technical limitations. The risk is minimized because all of the assets at issue were properly cataloged within the entity's own database, which resulted in all of the assets being afforded the required protections within the entity's CIP program for the duration of the noncompliance. This is primarily a documentation issue. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, [REDACTED] determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances involved different facts and circumstances and arose from different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the asset management device list to match [REDACTED] 2) performed an extent of condition review on all TFE device population; 3) simplified the entity TFE internal reporting process; and 4) implemented controls and communicated the documented process to all stakeholders. <p>[REDACTED] has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021231	CIP-007-6	R5	[REDACTED]	[REDACTED]	7/1/2016	12/7/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On March 8, 2019, the entity submitted Self-Reports stating that, [REDACTED] it was in noncompliance with CIP-007-6 R5.</p> <p>On August 7, 2018, a new entity employee assigned to Technical Feasibility Exceptions (TFEs) discovered a mismatch of internal device lists vs externally reported device lists in [REDACTED] for device counts related to existing TFEs. Upon further analysis, the entity determined that this incident had been occurring since the start of CIP v5 on July 1, 2016. After consulting with internal stakeholders and subject matter experts (SMEs), the entity discovered that there were gaps in the existing process and a lack of transparency with the internal TFE reporting process. There were several opportunities for error and the entity had insufficient controls to ensure that accurate information regarding TFEs was updated in [REDACTED]</p> <p>The entity's initial analysis concluded that [REDACTED] had either been removed from service or had been placed into service, but were not accurately updated in webCDMS. Further analysis concluded that the following number of assets were specifically impacted: [REDACTED]</p> <p>This noncompliance involves the management practices of work management and information management. The root cause of this noncompliance was an ineffective communication process to ensure that accurate information regarding TFEs was updated in [REDACTED]. The entity also lacked an effective verification control to ensure the accuracy of information in [REDACTED]</p> <p>This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-007-6 R4 and ended on December 7, 2018, when the entity updated its TFE device lists in [REDACTED] using the simplified process and new spreadsheet.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to identify and manage TFE assets is the entity may fail to implement mitigating measures to the vulnerabilities that are present in assets that have technical limitations. The risk is minimized because all of the assets at issue were properly cataloged within the entity's own database, which resulted in all of the assets being afforded the required protections within the entity's CIP program for the duration of the noncompliance. This is primarily a documentation issue. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, [REDACTED] determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances involved different facts and circumstances and arose from different root causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) updated the asset management device list to match [REDACTED] 2) performed an extent of condition review on all TFE device population; 3) simplified the entity TFE internal reporting process; and 4) implemented controls and communicated the documented process to all stakeholders. <p>[REDACTED] has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021306	CIP-007-6	R5	[REDACTED]	[REDACTED]	12/11/2018	2/5/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On March 29, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-007-6 R5. The entity was implementing a new [REDACTED]. While in development/pre-production, a subject matter expert (SME) created a shared account with the username "ahead" on a network switch. The switch is a Protected Cyber Asset (PCA). Personnel created the shared account for the sole purpose of having an onsite vendor configure the switch. The entity utilizes [REDACTED]. In this case, [REDACTED] the switch, went into production on December 11, 2018, but personnel did not document the "ahead" account [REDACTED] or delete it. As a result, between December 11, 2018, and February 5, 2019, the entity did not have evidence of compliance with CIP-007-6 R 5.3, which requires that entities identify individuals who have authorized access to shared accounts. On February 5, 2019, a SME discovered the account and determined that the entity failed to list it [REDACTED]. That same day, the SME removed the account.</p> <p>The root causes of this noncompliance were: (a) a failure to comply with project plans and procedures; and (b) a lack of verification controls. The entity had created an action item list before [REDACTED] assets were placed into production, and one of those items was to remove the shared account at issue. However, responsible personnel failed to complete this task, and the entity did not have adequate controls to monitor performance and completion of the task.</p> <p>This involves the management practices of implementation, workforce management, and verification. When implementing new assets, an entity should strive to ensure that said implementation does not introduce risks to the reliability and resilience of the bulk power system (BPS). This can be achieved, in part, through effective workforce management, which includes the development and implementation of clear, thorough, and executable processes, procedures, and work instructions. And, where feasible, those processes, procedures, and work instructions should include verification controls to monitor the performance and completion of various tasks.</p> <p>This noncompliance started on December 11, 2018, when the switch went into production with an undocumented shared account and ended on February 5, 2019, when the entity removed the account.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS based on the following factors. Failing to account for shared accounts or identify individuals with access to shared accounts increases the risk of unauthorized access through said accounts. Here, the following facts reduced the risk. During the period of this noncompliance, a user could not remotely access the switch and "ahead" account because of existing configurations and conditions. [REDACTED] Therefore, in order to utilize the shared account, an individual would have needed physical access to the switch to connect a console cable. Lastly, only two individuals knew the credentials for the local account, and both had completed NERC-CIP training and were subjected to extensive background checks. The entity reviewed access records and verified that the account was not accessed during the time of this noncompliance. No harm is known to have occurred.</p> <p>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior violations involved different facts, circumstances, and/or causes.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) removed and deleted the shared account; 2) updated a standard work instruction to add a note about the use of temporary shared accounts, [REDACTED], and verification of the existence/removal of accounts. The entity communicated the updated work instruction to appropriate personnel; and 3) performed a required read of its existing process relating to entitlements for new or modified assets and ensured that it is a part of the entity's annual 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
RFC2019021686	CIP-003-6	R1	[REDACTED]	[REDACTED]	7/1/2016	12/11/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			<p>On June 11, 2019, the entity submitted a Self-Report stating that, [REDACTED] it was in noncompliance with CIP-003-6 R1.</p> <p>The entity had cyber security policies that addressed Cyber Security Awareness and Cyber Security Incident Response as required for assets containing [REDACTED] impact Bulk Electric System (BES) Cyber Systems that were approved by the plant manager who was a designated CIP delegate by the entity's CIP Senior Manager as of July 1, 2016. The CIP Senior Manager, however, did not approve the Cyber Security Awareness and Cyber Security Incident Response policies as required by CIP-003-6 R1.</p> <p>The root cause of this noncompliance was an inadequate understanding of CIP-003-6 R1. Specifically, the entity incorrectly believed that a designated CIP delegate was sufficient to approve the Cyber Security Awareness and Cyber Security Incident Response policies. The CIP Senior manager must approve these policies.</p> <p>This noncompliance involves the management practices of reliability quality management and workforce management. Reliability quality management is involved because the entity did not properly define staff roles and responsibilities for NERC CIP compliance. Workforce management is involved because the entity's CIP Senior Manager did not understand that it was his responsibility to approve these policies.</p> <p>This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-003-6 R1 and ended on December 11, 2018, when the CIP Senior Manager approved the Cyber Security Awareness and Cyber Security Incident Response policies.</p>					
Risk Assessment			<p>This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The failure to have one or more approved policies that address physical security and electronic access for assets containing low impact BES Cyber Systems could result in personnel not having proper direction and guidance when creating the procedures and processes for and implementing various cyber security matters, thereby increasing the likelihood of a deficient security posture. The risk here is minimized because this is a documentation issue; the entity had Cyber Security Awareness and Cyber Security Incident Response policies in place as well as approval from a designated CIP delegate for the duration of the noncompliance. The entity simply failed to have the CIP Senior Manager approve these policies. No harm is known to have occurred.</p> <p>ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) obtained CIP senior manager approval of the cyber security policies that address Cyber Security Awareness and Cyber Security Incident response immediately upon becoming aware that the approval of those policies could not be delegated; and 2) now uses [REDACTED] software as a compliance calendar. The entity will obtain approval once every 15 calendar months from the CIP Senior Manager and [REDACTED] will ensure this is completed through automated reminders. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020443	CIP-003-6	R2, Attachment 1, Sect. 4, 4.5	[REDACTED]	[REDACTED]	04/01/2017	04/11/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On September 24, 2018, the entity submitted a Self-Report stating, as a [REDACTED], it was in potential noncompliance with CIP-003-6 R2. Specifically, the entity did not perform the initial test of its Cyber Security Incident response plan by April 1, 2017 when the Standard and Requirement became mandatory and enforceable. In this instance, the employee responsible for the completion and tracking of tests of the Cyber Security Incident response plan was not aware that the initial performance of the Requirement was required to be completed by April 1, 2017, and therefore, did not complete the test until the previously scheduled date of April 11, 2017, for a duration of 11 days.</p> <p>The root cause of the issue was attributed to lack of management oversight. The employee mistakenly believed the that initial performance of the requirement was due 36 months after the Standard and Requirement became enforceable.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement CIP-003-6 R2, Attachment 1, Section 4, subsection 4.5 when it failed to perform the initial test of one Cyber Security Incident response plan.</p> <p>Failure to perform an initial test of the Cyber Security Incident response plan could have resulted in personnel being unprepared to handle a Cyber Security Incident if one occurred. However, the entity had conducted an annual test of its Cyber Security Incident response plan under CIP-008-3. Additionally, the only changes to the entity's plan was to list [REDACTED] Low Impact Bulk Electric System (BES) Cyber System (LIBCS) that had not been in scope prior to the effective date of the current Requirement and Standard. Additionally, all Cyber Security Incidents are investigated using the same process documented in the entity's program, regardless of whether the incidents involve BES Cyber Systems. As such, any incident involving the [REDACTED] LIBCS not previously listed in the procedure, would have been handled per the entity's documented process. No harm is known to have occurred.</p> <p>WECC determined the entity had no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) tested its Cyber Security Incident response plan via tabletop exercise; and 2) instituted weekly meetings with staff and management to discuss compliance-related activities and deadlines associated with those activities. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022177	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021119	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022179	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022168	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	[REDACTED]	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED] it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity did not complete the initial test of its Cyber Security Incident response plan prior to [REDACTED], the date the entity registered as a [REDACTED]. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of [REDACTED] days.</p> <p>The root cause of the issue was attributed to an ineffective preventive control and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to test its documented Cyber Security Incident response plan prior to its registration date as a [REDACTED] as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022180	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022167	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022178	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022169	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022170	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022171	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED] it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021116	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED] the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) complete a tabletop exercise of the Cyber Security Incident Response Plan; 2) train relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implement an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022176	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022172	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022183	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022174	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED] the entity submitted a Self-Certification stating that, as a [REDACTED], it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022182	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	06/06/2018	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED] it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity completed the initial performance of testing its Cyber Security Incident response plan on March 6, 2017, however, it did not test it again within 15 calendar months of completion of the initial performance as required by Part 2.1. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue began on June 6, 2018, when the 15-month timeframe to conduct the test after the initial performance expired and ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of 259 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented Cyber Security Incident response plan associated with a Medium Impact Bulk Electric System (BES) Cyber System at least once every 15 calendar months as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022173	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	[REDACTED]	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED] it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity did not complete the initial test of its Cyber Security Incident response plan prior to [REDACTED], the date the entity registered as a [REDACTED]. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of [REDACTED] days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to test its documented Cyber Security Incident response plan prior to its registration date as a [REDACTED] as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019022175	CIP-008-5	R2: P2.1	[REDACTED]	[REDACTED]	[REDACTED]	02/19/2019	Self-Certification	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	<p>On [REDACTED], the entity submitted a Self-Certification stating that, as a [REDACTED] it was in potential noncompliance with CIP-008-5 R2. Specifically, the entity did not complete the initial test of its Cyber Security Incident response plan prior to [REDACTED] the date the entity registered as a [REDACTED]. In this instance, the entity had scheduled a [REDACTED] task reminder as an internal control intended to alert one employee that the due date for the test approached. When the employee left the organization, the task was not assigned to the new employee, thus rendering the control moot. This issue ended on February 19, 2019, when the entity completed a test of its Cyber Security Incident response plan, for a duration of [REDACTED] days.</p> <p>The root cause of the issue was attributed to a lack of internal controls and training. Specifically, the entity had implemented an internal control with functionality predicated on the continued employment of a single employee; when that employee was terminated, the control no longer functioned. Additionally, the entity did not adequately train its new personnel on the requirement to test the Cyber Security Incident response plan.</p>							
Risk Assessment	<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to test its documented Cyber Security Incident response plan prior to its registration date as a [REDACTED] as required by CIP-008-5 R2 Part 2.1.</p> <p>Failure to test the documented plan could have resulted in employees referencing outdated instructions in the event a need to implement the plan arose. However, the entity did not identify any necessary changes when it exercised its plan, therefore the documented instructions were still valid. No harm is known to have occurred.</p> <p>WECC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.</p>							
Mitigation	<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed a tabletop exercise of the Cyber Security Incident Response Plan; 2) trained relevant employees on its Cyber Security Incident Response Plan and the associated requirements; and 3) implemented an internal control to automate tracking and alerting of compliance related obligations. 							

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021674	CIP-004-6	R4: P4.3	████████████████████ ██████	██████	03/16/2018	05/03/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On May 29, 2019, the entity submitted a Self-Log stating, as a ██████████, it was in potential noncompliance with CIP-004-6 R4 Part 4.3. Specifically, the entity had implemented a manual process to track shared accounts but had neglected to track a total of two administrative accounts on the spreadsheet. Because of this oversight, the entity did not verify that electronic access to the two administrative accounts was correct and deemed necessary. The accounts resided on Electronic Access Control or Monitoring Systems (EACMS) associated with the entity's High Impact Bulk Electric System (BES) Cyber Systems (HIBCS). This issue began on March 15, 2019, when the entity used an incomplete list to verify that electronic access was correct and necessary and ended on April 9, 2019, when the entity utilized a corrected list to verify that electronic access was appropriate and necessary, for a duration of 26 days.</p> <p>The root cause of the issue was attributed to a lack of internal controls. Specifically, the entity did not have procedural or automated controls to identify or alert that its administrative accounts were not being tracked and appropriately managed.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, for two administrative user accounts, the entity failed to adequately implement its documented access management program to verify at least once every 15 calendar months, that electronic access associated with said user accounts and their specific, associated privileges were correct and were those that the Responsible Entity deemed necessary as required by CIP-004-6 R4 Part 4.3.</p> <p>Such failure could have resulted in allowing individuals possessing greater access than was necessary to perform their work duties thereby increasing the risk of malicious compromise to the HIBCS. However, the password for both accounts had expired in January 2018, and it was confirmed that no one had logged in using the administrative account beyond that date. Additionally, all individuals with access to both accounts were authorized for access to similarly classified EACMS. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) completed the 15-calendar month verification of the accuracy and necessity of all user accounts, user account groups, user role categories and their specific, associated privileges; and 2) replaced the manual tracking process and implemented automated tracking of electronic access authorization to shared accounts. 					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021676	CIP-004-6	R4: P4.2	[REDACTED]	[REDACTED]	03/16/2018	04/23/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On May 29, 2019, the entity submitted a Self-Log stating, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R4 Part 4.2. Specifically, for one individual, the entity did not verify that one employee with authorized unescorted physical access had authorization records in accordance with its documented access management program. On December 15, 2017, the entity implemented a new compliance tool used to document and track access authorizations and revocations associated with its Bulk Electric System (BES) Cyber Systems. The transition to the new tool required the entity to import badge information from the old system to the new; the entity applied filters designed to restrict the importation of badge information by type, to only those required to be tracked. The employee in question had a singularly unique badge type and his access authorization and privileges were not filtered into the new tool for tracking purposes. This issue began on March 16, 2018, three months after the entity last verified the employee's authorization for unescorted physical access and ended on April 23, 2019, when the entity verified the employee's unescorted physical access was authorized, for a total of 404 days.</p> <p>The root cause of the issue was attributed to a less than adequate implementation of a new process. Specifically, when the entity transitioned to the new tool, a sufficiently comprehensive review of the physical access authorizations transferred to the new system was not performed to ensure that all access was documented and would be tracked in the new system.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to adequately implement its documented access management program to verify at least once each calendar quarter, such that one individual with unescorted physical access had an authorization record as required by CIP-004-6 R4 Part 4.2.</p> <p>Failure to verify authorization records of unescorted physical access could have resulted in an employee retaining access that was no longer necessary, appropriate, or authorized. However, the scope of this issue was limited to one long-term Physical Security Operations employee who was authorized for unescorted physical access. This issue was administrative in nature and not technical or operational. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) entered the employee's physical access authorizations into the compliance tool for tracking; and 2) validated the unescorted physical access data in the new tool was complete and accurate. <p>WECC has verified the completion of all mitigation activity.</p>					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019021677	CIP-004-6	R5: P5.5	[REDACTED]	[REDACTED]	02/15/2019	04/22/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On May 29, 2019, the entity submitted a Self-Log stating, as a [REDACTED], it was in potential noncompliance with CIP-004-6 R5 Part 5.5. Specifically, the entity did not change a password to one shared administrator account within 30 calendar days after the entity determined that seven employees no longer required access to the account due to an internal reassignment. The account in this issue was administrative and associated with a High Impact BES Cyber System (HIBCS). The entity revoked the employee's access to the account and manually updated its tracking spreadsheet accordingly. However, the employee that performed the revocation was unfamiliar with the process and did not know that the password to the shared account needed to be changed within 30-calendar days. This issue began on February 15, 2019, when the 30-calendar day timeframe to change the password expired and ended on April 22, 2019, when the entity changed the password to the shared account, for a total of 67 days.</p> <p>The root cause of the issue was attributed to less than adequate training and a lack of internal controls. Specifically, the employee had not been adequately trained on the documented process. Additionally, the entity did not have internal controls implemented in its documented access revocation program sufficient to prevent or detect the issue from occurring, such as a notification that a revocation instigated the need to change a password.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to change the password for one shared account within 30 calendar days following the date the entity determined the employees no longer required access as required by CIP-004-6 R5 Part 5.5.</p> <p>Failure to change the password to a shared account could have resulted in an employee with malicious intent accessing the account and using it to damage a BES Cyber Asset associated with a HIBCS. However, the employees were transferred to other positions within the company. Further, each employee retained authorized electronic and unescorted physical access to Cyber Assets similarly classified. Finally, the entity reviewed the logs and confirmed that the account had not been accessed within the relevant timeframe. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this issue, the entity has:</p> <ol style="list-style-type: none"> 1) changed the password for the shared account; 2) provided additional training to the employee on the documented process; and 2) implemented tracking authorizations for shared accounts in the entity's compliance tool which alerts relevant personnel via email that a password to a shared account needs to be 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
WECC2019021682	CIP-007-6	R5: P5.2; P5.3	██████████)	██████████	12/15/2017	4/22/2019	Self-Log	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)			<p>On May 29, 2019, the entity submitted a Self-Log stating, as a ██████████ it was in potential noncompliance with CIP-007-6 R5 Parts 5.2 and 5.3. Specifically, in April 2019 while performing baseline configuration activities on servers classified as Electronic Access Control or Monitoring Systems (EACMS) associated with a High Impact Bulk Electric System (BES) Cyber System (HIBCS), the entity's ██████████ staff discovered that local administrator accounts for three EACMS were not listed on its shared account spreadsheet. As such, the entity had not identified individuals who had authorized access to the shared accounts on the EACMS. This issue started on December 15, 2017, when shared accounts on three EACMS should have been inventoried and ended on April 22, 2019, when the entity listed the shared accounts on its spreadsheet and identified those with authorized access, for a total of 524 days.</p> <p>The root cause of these issues was attributed a lack of internal controls. Specifically, the spreadsheet omission could have been detected and corrected had the entity implemented an internal control to check work completion for correctness and would have prevented the additional issue related to Part 5.3.</p>					
Risk Assessment			<p>This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to identify and inventory all known default or other generic account types as required by CIP-007-6 R5 Part 5.2. As such, the entity failed to identify individuals who have authorized access to shared account as required by CIP-007-6 R5 Part 5.3.</p> <p>A failure to appropriately implement system access control on shared accounts could lead to intentional or inadvertent compromise of BES Cyber Assets. However, all individuals with access to the accounts had authorized electronic access to other Cyber Assets similarly classified. Additionally, the entity reviewed the login records for the accounts and confirmed there were no logins attempts after the password expired. No harm is known to have occurred.</p>					
Mitigation			<p>To mitigate this noncompliance, the entity:</p> <ol style="list-style-type: none"> 1) identified and inventoried all known enabled default or other generic account types on the EACMS in scope; 2) identified and inventoried individuals who had authorized access to the shared accounts on the EACMS in scope; 3) utilized an existing tracking tool to track access authorization to shared accounts which replaced the manual shared account spreadsheet; and 4) implemented as a control for CIP-007-6 R5.2 workflows within the tool to notify subject matter experts of accounts approaching password expiration dates. 					