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 FFTs 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	FRCC2018019085			Yes	Yes	Yes								Category 2 – 12: 2 years
2	FRCC2018019083			Yes	Yes	Yes								Category 2 – 12: 2 years
3	FRCC2018019084	Yes		Yes	Yes	Yes								Category 1 - 3 years Category 2 – 12: 2 years
4	FRCC2018020749	Yes		Yes	Yes									Category 1 - 3 years Category 2 – 12: 2 years
5	MRO2017017620	Yes		Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 years
6	SPP2018019313	Yes		Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 years

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2018019085	CIP-006-6	R1. 1.4. 1.5. 1.6. 1.7.	[redacted] ("the Entity")	[redacted]	09/08/2017	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 noncompliance.)	On January 30, 2018, the Entity submitted a Self-Report stating that, as a [redacted] it was in noncompliance of CIP-006-6 R1 (Parts 1.4 through 1.7). This noncompliance started on September 8, 2017, when the Entity failed to implement one or more documented physical security plan(s), and ended on September 12, 2018, when the Entity resolved the deficiencies in its Physical Security Plan. Specifically, on September 8, 2017 from 2300 through September 9, 2017 at 0700 (8 hours), the Entity failed to monitor and/or issue an alarm or alert due to unauthorized physical access for their PSPs and PACS [redacted] as required by CIP-006-6 R1 (Parts 1.4 through 1.7). On September 9, 2017, at 2100 through September 10, 2017 at 2300 (26 hours), the Entity experienced a system-wide PACS communication failure for all their PSPs. The Entity security personnel were monitoring the PSP at Headquarters and contracted security were monitoring PSPs at an offsite backup control center. However, the Entity failed to monitor and/or issue an alarm or alert due to unauthorized physical access for their PSPs and PACS [redacted] as required by CIP-006-6 R1 (Parts 1.4 through 1.7). On September 9, 2017, at 2100 through September 12, 2017 at 0600 (57 hours), the contracted guard [redacted] was sent home by the contract security company for safety purposes due to Hurricane Irma without notification to the Entity. During this time the Entity failed to monitor and/or issue an alarm or alert due to unauthorized physical access for their PSPs and PACS [redacted] as required by CIP-006-6 R1 (Parts 1.4 through 1.7). The causes for this noncompliance were 1) lack of communications both verbally and written and 2) equipment failure as a result of a weather event.					
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, the Entity's failure to monitor and alert/alarm for unauthorized access into a PSP could have allowed individuals to gain access to secure facilities causing reliability issues, vandalism, and or personal injury. The risk was reduced because the majority of the sites were manned 24/7. Upon restoration of communication links, it was confirmed that no physical breaches were attempted. No harm is known to have occurred.							
Mitigation	To mitigate this violation, the Entity: 1) performed a root cause analysis; 2) installed a new PACS enterprise server; 3) met with the contract security vendor to review expectations defined in the agreement to prevent future recurrance; 4) completed an extent of condtion analysis; 5) standardized all applicable NERC related communications to [redacted] 6) updated internal controls by adding security business unit plans and weather related check lists; and 7) completed training on new server and procedures and created an ongoing training plan.							

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2018019083	CIP-007-6	R4. 4.1.	[redacted] ("the Entity")	[redacted]	07/01/2016	2/25/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed noncompliance.)	On January 30, 2018, the Entity submitted a Self-Report stating that, as a [redacted] it was in noncompliance of CIP-007-6 R4 (Part 4.1). This noncompliance started on July 1, 2016, when the Entity failed to log events at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that included detected successful login attempts, and ended on February 25, 2018, when the Entity updated their Cyber Assets to enable the required logging function. Specifically, for seven (7) medium impact BES Cyber Assets [redacted], four (4) with external routable connectivity (ERC) and three (3) without ERC, the Entity failed to log unsuccessful password login attempts as required by CIP-007-6 R4 (Part 4.1) for Cyber Assets that had such capability. The cause for this noncompliance was determined to be a lack of internal controls to confirm that proper logging capabilities were enabled on the applicable relays.					
Risk Assessment	This noncompliance posed a moderate 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 ensure that logs of unsuccessful login attempts were generated and captured, exposed those BES Cyber Assets to a loss of visibility for possible unauthorized access attempts. Any undetected compromise of these Cyber Assets could have allowed potential impact to the reliability of the BPS within the Region. The risk was reduced because the devices capture logs locally for use in after-the-fact investigation in the case there was a cyber-security event. At no time since the devices were placed in-service has an event requiring investigation occurred. The devices reside in a PSP [redacted] in the ESP. Passwords must be requested in order to access the device remotely and locally. No harm is known to have occurred.					
Mitigation	To mitigate this violation, the Entity: 1) enabled logging on identified relays; 2) performed a detailed root cause analysis; 3) performed an extent of condition review on all Cyber Assets that are capable of performing a logging function back to the July 1, 2016 the enforcement date; 4) enhanced Internal Controls by creating a commissioning check sheet to ensure when devices are deployed they are compliant with NERC Standards; 5) performed initial training for all applicable employees on new processes/procedures and Internal Controls and created a plan for ongoing and annual training; and 6) provided the Region with all current and updated procedures for Cyber Asset logging.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2018019084	CIP-007-6	R4. 4.2.	[redacted] ("the Entity")	[redacted]	07/01/2016	2/18/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed noncompliance.)			On January 30, 2018, the Entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance of CIP-007-6 R4 (Part 4.2). This noncompliance started on July 1, 2016, when the Entity failed to generate alerts for detected malicious code within BES Cyber Assets in medium impact BES Cyber Systems with External Routable Connectivity and ended on February 18, 2018, when the Entity updated the BCAs to perform the required alerting function. Specifically, on four (4) BCAs, two (2) located at [redacted] and two (2) located at [redacted], the Entity failed to generate alerts for detected malicious code intrusion as required by CIP-007-6 R4 (Part 4.2). Two (2) devices are used for serial-to-Ethernet connectivity for protective relays located in the two (2) medium impact substations and two (2) are utilized as Ethernet Security Gateway devices for remote password and settings management, [redacted]. The cause for this noncompliance was determined to be a lack of controls during the commissioning process of new device types to the Entity's system.					
Risk Assessment			This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, the Entity's failure to ensure that alerts for detected malicious code, exposed those BCAs to possible malware intrusion allowing nefarious individuals to gain control and compromise these BCAs which, would have allowed potential impact to the reliability of the BPS within the Region. The risk was reduced because the devices reside in a PSP and passwords are changed monthly. A review of the logs for the devices did not indicate erroneous or unusual activity. No harm is known to have occurred.					
Mitigation			To mitigate this violation, the Entity: 1) configured the syslog server to alert for malicious code within the covered BCAs; 2) performed a detailed root cause analysis; 3) performed an extent of condition review on all Cyber Assets that are capable of performing a logging function back to the July 1, 2016 enforcement date; 4) enhanced Internal Controls by creating a commissioning check sheet to ensure when devices are deployed they are compliant with NERC Standards 5) performed initial training for all applicable employees on new processes/procedures and Internal Controls and provided a schedule or plan for ongoing and annual training; and 6) provided the Region with all current and updated procedures for Cyber Asset alerting.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2018020749	CIP-010-2	R3. 3.1. 3.3.	[redacted] ("the Entity")	[redacted]	6/20/2017	10/16/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed noncompliance.)	On December 3, 2018, the Entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-010-2 R3 Part 3.1 and Part 3.3. This noncompliance started on June 20, 2017, when two (2) Cyber Assets were added to the production environment without first performing an active cyber vulnerability assessment (CVA) and ended on October 16, 2018, when an active CVA was conducted on the two (2) missed Cyber Assets. This noncompliance involves two (2) CVA issues: 1) Part 3.3 required CVAs were not completed on two (2) Integrated Lights Out (iLO) appliances, and 2) Part 3.1 required CVAs were performed late (i.e., not within the required 15-month interval) on Cyber Assets that are associated with four (4) medium impact Transmission Substations. Both issues were discovered during the Entity's preparation to respond to the 2018 Self-Certification request by the Region. Issue 1: Two (2) iLO appliances were inadvertently omitted from a CVA scan that was conducted prior to adding them to the energy management system (EMS) on June 19, 2017. The two (2) devices were omitted due to an error in the scan parameters. The issue was discovered on October 15, 2018 and was corrected on October 16, 2018, 472 days after the devices were placed in service. The Entity performed an extent of condition review for 253 other Cyber Assets, including four (4) other iLO appliances. No additional iLO appliances were identified for which no CVA scan existed making it a total of two (2) discovered Cyber Assets that were noncompliant representing an error rate of less than 1%. Issue 2: The Entity completed the Part 3.1 CVAs for its medium impact Transmission Substations and generated the 2017 Part 3.4 report on April 1, 2017, well ahead of the July 1, 2017 version 5 implementation deadline. Actual assessment activity for the Substations, however, were run from mid-July 2016 until mid-December 2016. The Entity completed the second round of CVAs in the first quarter of 2018 and generated the 2018 Part 3.4 report on March 23, 2018, which was 11 months after the 2017 report. However, under an extent of condition review, it showed the times between the field work conducted as required under Part 3.1 for 4 of 8 Substations (50%) varied between 16 and 19 months, which exceeded the maximum 15-month internal required by the Standard. The cause for the issue #1 noncompliance was a thorough reconciliation was not performed for the initial CVA scans compared to the master list of assets being onboarded as part of the EMS upgrade project; the cause for issue #2 was the Entity misinterpretation of the language of the Standard and scheduled the second CVA based on the Part 3.4 report date rather than on the completion date of the first substation CVA performed for Part 3.1.
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed by this noncompliance was that an undetected and unknown vulnerability could have been introduced into the Electronic Security Perimeters allowing further compromise of other BES Cyber Assets potentially impacting the BPS. For issue #1, the risk was reduced because the two (2) iLOs in question are similar to four (4) other iLOs that were scanned for vulnerabilities during onboarded efforts and the iLOs reside within a jump-host environment which cannot be accessed directly from the corporate environment. The Entity deploys multiple layers of defense to protect its NERC environment. Therefore, the ability to exploit this vulnerability is further minimized due to multiple defense in depth layers. Such defense layers include [redacted] Furthermore, these assets were afforded CIP-005 (intermediate system, multi-factor authentication, etc.) and CIP-007 (ports and services, logging, malicious code prevention, account management, etc.) security controls during onboarding efforts due to being declared as associated high-impact EACMS. For issue #2, the risk was reduced because the delays in completing the second round of CVAs were four months or less. The Entity performed the substation CVAs in the last half of 2016, nine months before the required date. The second round of CVAs started in February 16, 2018 and completed March 16, 2018. Four (4) of the eight (8) substations were completed within the 15-month period 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
FRCC2018020749	CIP-010-2	R3. 3.1. 3.3.	[redacted] ("the Entity")	[redacted]	6/20/2017	10/16/2018	Self-Report	Completed
			by CIP-010 R3. The remaining four (4) substations were completed late at intervals between 16 and 19 months. Furthermore, the Cyber Assets in the substations are proprietary devices that are hardened by the vendor without External Routable Connectivity (ERC). No harm is known to have occurred as no vulnerabilities were found on the two (2) devices in which the CVA was missed, nor were any discovered for the CVAs performed late in the Substations. The Region determined that the Entity's compliance history should not serve as a basis for applying a penalty.					
Mitigation			To mitigate this noncompliance, the Entity: 1) performed CVAs for the missed iLOS with no vulnerabilities found; 2) performed extent of condition review only identifying the two iLO appliances inadvertently omitted from the CVA scan; 3) determined root cause was that a thorough reconciliation was not performed for the initial CVA scans compared to the master list of assets being onboarded as part of the EMS upgrade project; 4) created preventative control with a new procedure for new and existing asset CVAs to perform a thorough reconciliation including one-time training to affected team on new procedure; 5) perform CVAs for Substations; 6) determined extent of condition identifying only the four out of eight substation CVAs exceeded the required 15-month period; 7) determined root cause was that the Entity misinterpreted the language of the Standard and scheduled the second CVA based on the Part 3.4 report rather than on the completion date of the first substation CVA done under Part 3.1.; 8) designed a preventative control tracking mechanism to remind the affected team to conduct CVAs within the 15 calendar months from the date CVAs were conducted at each facility; and 9) trained the affected team on preventative control tracking mechanism and communicated correct interpretation of the language of the Standard 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
MRO2017017620	CIP-005-5	R1	[redacted]	[redacted]	07/01/2016	01/11/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			On April 5, 2017, [redacted] submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-005-5 R1. Specifically, [redacted] substation firewalls allowed access to an overly broad range of IP addresses. [redacted] stated that during its annual vulnerability assessment, it discovered that a [redacted] was permitted direct connectivity to medium impact BES Cyber Assets at [redacted] substations. [redacted] conducted an extent of condition assessment and determined that the [redacted] was able to gain access because of a firewall IP address object that was incorrectly implemented on the firewalls for substations that contain medium impact BES Cyber Systems. The address object permitted inbound access from [redacted] when only one IP address [redacted] was required. Within the extended address range, the firewall access rule also permitted inbound access for a broad range of services from the range of [redacted] IP addresses including [redacted]. The cause of the noncompliance was that [redacted] relevant process lacked sufficient detail, resulting in an insufficient assessment of the firewall access rule for need. The noncompliance began on July 1, 2016, when the Standard and Requirement became enforceable and ended on January 11, 2017 when [redacted] updated the firewall access rule.				
Risk Assessment			The noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk of the noncompliance was not minimal as the firewall rule allowed [redacted] IP addresses from [redacted] Additionally, the firewall rule allowed a broad range of services. Further, the noncompliance had the ability to impact [redacted] medium impact substations, including a substation [redacted]. However, the risk of the noncompliance was not serious or substantial as the firewall rule [redacted]. Further, [redacted] further limited electronic access [redacted]. Additionally, [redacted] limited physical access to [redacted]. Moreover, an extent of condition analysis upon the substation firewalls (verified by MRO) confirmed that the noncompliance was limited to one improperly broad firewall IP address object. Finally, the noncompliance was limited to potentially improper access to substation ESPs and did not permit access to the Control Center ESP. No harm is known to have occurred. MRO reviewed [redacted] relevant CIP-005-5 R1 compliance history. [redacted] compliance history includes a minimal risk FFT for noncompliance with CIP-005-1 R2.2 [redacted]) that was mitigated on August 4, 2013. The prior noncompliance involved an enabled port that was necessary but undocumented on the EAP. MRO determined that [redacted] compliance history should not serve as a basis for applying a penalty. The prior noncompliance and the current noncompliance are distinct in character and in cause, additionally; the current noncompliance was not caused by a failure to mitigate the prior noncompliance.				
Mitigation			To mitigate this noncompliance, [redacted]: 1) updated the overly broad address range for the firewall rule at issue; 2) conducted a full extent of condition to discover the additional instances; and 3) updated its ""add/update/remove Cyber Asset"" workflow in its compliance software tool to include additional considerations. MRO verified the completion of the mitigating activities.				

Midwest Reliability Organization (MRO) FFT 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
SPP2018019313	CIP-007-6	R2	[redacted]	[redacted]	12/28/2016	08/23/2017	Self-Certification	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On February 28, 2018, [redacted], submitted a Self-Certification to SPP RE stating that, as a [redacted], it was in noncompliance with CIP-007-6 R2. [redacted] The noncompliance impacted Cyber Assets that are located [redacted] identified two instances of noncompliance with P2.3. In the first instance of noncompliance, [redacted] stated that thirteen patches were not successfully applied on [redacted] BES Cyber Assets ([redacted] Servers) as required by P2.3. [redacted] discovered this noncompliance on a documentation review of all [redacted] Servers. [redacted] was unaware that to apply a patch to the [redacted] it needed to update a [redacted]. The cause of the noncompliance was inadequate detail in its processes for patch installation that caused [redacted] to miss the final step needed to apply the patch. Additionally, the [redacted] were not updated as part of the vendor's install script and therefore the install script did not update [redacted]. The noncompliance began on December 28, 2016, the date that the first patch was to be installed and ended on August 23, 2017 when all thirteen patches were successfully applied. In the second instance of noncompliance, [redacted] stated that seven patches were not applied to [redacted] BES Cyber Assets ([redacted] servers) within 35 calendar days of assessment as required by P2.3. An administrator applied the patches to all [redacted] Servers through a single patch label, but because the BES Cyber Assets were a different version than the other servers, the label did not include the patches that had been evaluated under P2.2. The cause of the noncompliance is that [redacted] had inadequate processes for patch installation; specifically [redacted] did not have a process to review the combining of patches into a label. The noncompliance began on April 4, 2017, when the patches were not applied within 35 days of the evaluation, and ended on May 23, 2017, when the patches were applied. The noncompliance began on December 28, 2016, the date that the first patch was to be installed in the first instance of noncompliance and ended on August 23, 2017 when all thirteen patches were successfully applied in the first instance of noncompliance.
Risk Assessment	The noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk of the first instance of noncompliance was not minimal because the duration of the noncompliance was 238 days, which represents a risk to the BPS given the importance of mitigating the risk from well-known software vulnerabilities. However, the risk was not serious or substantial as [redacted] Further, a review of [redacted] network diagram demonstrates that the noncompliance only impacted approximately [redacted] percent of [redacted] Cyber Assets. No harm is known to have occurred. The risk of the second instance of noncompliance was minimal because [redacted] conducted an extent of condition analysis and determined that patch labels had not caused any similar instances of noncompliance. Additionally, the duration of the noncompliance was limited to 49 days and [redacted] No harm is known to have occurred. MRO reviewed [redacted] relevant CIP-007-6 R2 compliance history. [redacted] compliance history includes a minimal risk violation for noncompliance with CIP-007-3a R3 ([redacted] that was mitigated on April 11, 2012. The prior noncompliance involved [redacted] failure to adequately document approximately six percent of patches. MRO determined that [redacted] compliance history should not serve as a basis for applying a penalty. The prior noncompliance and the current noncompliance are distinct in character and in cause, separated by a significant duration, and the current noncompliance was not caused by a failure to mitigate the prior noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] To mitigate the first instance of noncompliance, [redacted] 1) applied the patches by updating the configuration file; and 2) augmented its process document to include a step to ensure the updated Operating System has been booted and provided training on that process document. To mitigate the second instance of noncompliance, [redacted]

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SPP2018019313	CIP-007-6	R2	[redacted]	[redacted]	12/28/2016	08/23/2017	Self-Certification	Completed
			1) applied the patches that had been missed; 2) conducted an extent of conditions analysis to seek out additional instances of noncompliance related to patch labels; and 3) augmented its process to include a step where the administrator runs a report to verify all patches were deployed. MRO verified the completion of all mitigating activities.					

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 FFTs 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	FRCC2018020577			Yes	Yes									Category 2 – 12: 2 years
2	MRO2018019937			Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 years
3	NPCC2017018605			Yes	Yes									Category 2 – 12: 2 year
4	NPCC2017018609			Yes	Yes									Category 2 – 12: 2 year
5	NPCC2017018606			Yes	Yes									Category 2 – 12: 2 year
6	RFC2017018414	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 year
7	RFC2017018410	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 year
8	RFC2018019281	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 year
9	RFC2017018409	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 year
10	RFC2018019255	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 year
11	RFC2018019256	Yes	Yes	Yes	Yes	Yes								Category 1: 3 years; Category 2 – 12: 2 year
12	RFC2017018415	Yes	Yes	Yes	Yes		Yes							Category 1: 3 years; Category 2 – 12: 2 year
13	SERC2016016171	Yes		Yes	Yes					Yes				Category 1 – 3 years; Category 2 – 12: 2 years
14	SERC2016016418			Yes	Yes					Yes				Category 2 – 12: 2 years
15	SERC2017018724			Yes	Yes					Yes				Category 2 – 12: 2 years
16	SERC2017016970	Yes		Yes	Yes					Yes				Category 1 – 3 years; Category 2 – 12: 2 years
17	SERC2017018599	Yes		Yes	Yes					Yes				Category 1 – 3 years; Category 2 – 12: 2 years

Florida Reliability Coordinating Council, Inc. (FRCC) FFT CIP

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2018020577	CIP-007-6	R5.	[redacted] ("the Entity")	[redacted]	3/21/2018	5/9/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On October 25, 2018, the Entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R5 (Part 5.7). This noncompliance started on March 21, 2018, when the Entity failed to limit unsuccessful authentication attempts or alert for unsuccessful authentication attempts and ended on May 9, 2018, when the Entity corrected their network policy authentication issues. Specifically, the Entity discovered that one (1) BES Cyber System network domain did not have the network policies set to limit or alert on the number of unsuccessful authentication attempts. Subsequent investigation revealed that the policy was reset as a result of a system upgrade on March 21, 2018. The error was corrected on May 9, 2018, when the group policy was restored to the appropriate settings. A total of 31 out of 99 (31.3%) cyber assets were affected by this group policy. An extent of condition investigation was performed to determine if other networks were impacted by the upgrade. There are only two (2) applicable networks, and the second network was confirmed to have the correct settings. The cause for this noncompliance was insufficient internal controls to identify and ensure that security controls are properly verified following system modifications.						
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, the Entity's failure to limit or alert on unsuccessful authentication attempts could give a malicious actor a greater window of opportunity to gain access to protected devices through password cracking techniques. This risk was reduced because physical access and remote electronic access are both restricted to only authorized personnel by two-factor authentication. A review of user authentication logs was conducted for the timeframe where the policy was not set for unsuccessful authentication attempts and revealed no suspicious events.						
Mitigation	To mitigate the noncompliance, the Entity: 1) corrected network policy setting for the affected domain; 2) performed an extent of condition investigation and corrected any additional affected domains; 3) performed a cause analysis for instances discovered; 4) reviewed user authentication logs of affected domains for affected time period to determine any suspicious events; 5) revised change ticketing workflow to add additional internal controls; and 6) communicated with affected personnel on new internal controls.						

Midwest Reliability Organization (MRO) FFT 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
MRO2018019937	CIP-007-6	R2	[redacted]	[redacted]	[redacted]	5/3/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On May 31, 2018, [redacted] submitted a Self-Report stating that as a [redacted], it was in noncompliance with CIP-007-6 R2. [redacted]. The noncompliance impacted Cyber Assets located at [redacted] Control Center and Back-Up Control Center which are both located [redacted] [redacted] stated that in [redacted] it underwent a large scale upgrade of its [redacted] stated that after the upgrade it failed to update its list of software application sources to track the release of cyber security patches as required by P1.1. This resulted in the patch sources for [redacted] Cyber Assets to be undocumented or incomplete. [redacted] stated that it discovered the noncompliance in March 2018 during its annual internal compliance review of CIP-007-6 R2. The cause of the noncompliance was inadequate processes regarding changes, which resulted in the patch source list to not be updated after the EMS was upgraded. The noncompliance began on [redacted] the source list became inaccurate, and ended on May 3, 2018 when [redacted] updated its source list and completed one patch cycle (which included applying any missed patches).
Risk Assessment	The noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was not minimal as the noncompliance covered [redacted] of [redacted] Cyber Assets and the software impacted by the noncompliance is important to the performance and protection of BES Cyber Systems. [redacted] which represents a significant delay in accessing patches and could result in known vulnerabilities being unpatched and vulnerable to adversaries. However, the risk of the noncompliance was not serious or substantial as [redacted] had retained a patch management vendor who did not rely upon [redacted] P1.1 documentation. The retention of a patch management vendor resulted in the vast majority of applicable patches to be assessed and applied; only nine applicable patches (spread over multiple sources) were not applied as a result of [redacted] incomplete documentation. Additionally, [redacted] Control Centers are the only assets that contain [redacted] BES Cyber Systems and only control [redacted] BES Cyber Systems. Finally, the noncompliance did not impact malware and antivirus definitions that were maintained at all times during the noncompliance. No harm is known to have occurred. [redacted] relevant CIP-007-6 R1 compliance history includes a moderate risk violation of CIP-005-2 R1 [redacted] and a minimal risk violation of CIP-006-3a R2 [redacted]. The CIP-005-2 R1 [redacted] violation involved [redacted] not applying patches to a specific EACMS device for 34 months and the noncompliance was mitigated on [redacted]. The CIP-006-3a R2 [redacted] violation involved [redacted] not applying patches to a specific PACS device for 17 months and the noncompliance was mitigated on [redacted] MRO determined that [redacted] compliance history should not serve as a basis for applying a penalty. The prior violations have different causes than the current noncompliance, the current noncompliance was not caused by a failure to mitigate the prior violations, and there is a significant time duration between the time that the prior violations were mitigated and the start of the current noncompliance.
Mitigation	To mitigate this noncompliance, [redacted] 1) updated its patch source list and completed one patch cycle; 2) updated its processes and procedures; and 3) provided reinforcement training to all applicable staff. MRO verified the completion of the mitigating activities.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018605	CIP-004-6	R4.	[redacted]	[redacted]	1/11/2017	8/28/2017	Self-Report	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On November 13, 2017, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered on August 17, 2017 it was in noncompliance with CIP-004-6 R4. (4.1.) after it found an issue within the workflow of its approval system. This noncompliance started on January 11, 2017 when the entity failed to follow its process to authorize electronic access for two (2) individuals to a Medium Impact BES Cyber System. The noncompliance ended on August 28, 2017 when the entity revoked the unauthorized access for one individual and approved access for the second individual. Specifically, the entity's approval system stopped populating the "approver" field, as a result, the system auto approved access for two individuals instead of sending the approval request to the proper approver. The two individuals in scope were granted access to a Medium Impact BES Cyber System, without approval. The system issue was corrected on August 22, 2017. • One individual was granted unauthorized access to a Medium Impact BES Cyber System on June 27, 2017; the entity revoked the unauthorized access on August 28, 2017 (62 days). • The second individual was granted unauthorized access to a Medium Impact BES Cyber System on May 17, 2017; the entity authorized the access on August 28, 2017 (103 days). The root cause of this noncompliance was due to lack of functionality testing after a change was made that inadvertently dropped the approvers from the approval system workflow.
Risk Assessment	The noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not following its approval process the entity granted access electronic access to two (2) contractors that should not have been approved for access. The contractors were granted full access to relays and other devices within the entity's substations and could have used that access to change relay settings and take the relays out of service, which could have had a severe impact to the BES. The entity reduced the risk of impact to the BES by not providing the contractors in scope with login credentials. The entity has also enabled alarms on equipment that is capable, that would have sent alarms to the entity's ECC SCADA operations team in real time had the contractors logged and caused the devices to become unstable. The entity reviewed access logs and found no records of any login. No harm is known to have occurred as a result of this noncompliance. The entity has seven previous violations of CIP-004. NPCC determined that the entity's compliance history should not serve as a basis for applying a penalty. There was a different underlying cause for each of the prior violations.
Mitigation	To mitigate this noncompliance, the entity: 1) revoked access for one individual; 2) approved access for one individual; 3) repopulated all of the approver fields with the appropriate designated approvers; 4) implemented control to stop the workflow if the approver field is blank; 5) conducted an off-cycle review in August 2017 and will compare against their upcoming third quarter access review; 6) created and updated their quarterly review procedure; and 7) conducted additional off cycle reviews in November and December of 2017.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018609	CIP-004-6	R4.	[redacted]	[redacted]	1/11/2017	9/6/2017	Self-Report	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On November 13, 2017, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered on August 17, 2017 it was in noncompliance with CIP-004-6 R4. (4.1.) during a SOX audit of its global provisioning system. This noncompliance started on January 11, 2017 when the entity failed to follow its process to authorize electronic access for two (2) individuals to a Medium Impact BES Cyber System. The noncompliance ended on September 6, 2017, when the entity revoked the access that was unauthorized. Specifically, the entity's approval system stopped populating the "approver" field; as a result, the system auto approved access for two individuals instead of sending the approval request to the proper approver. The system issue was corrected on August 22, 2017. • One individual was granted unauthorized electronic access to a Medium Impact BES Cyber System on June 7, 2017. The entity revoked the unauthorized access on September 6, 2017 (91 days). • Another individual was granted unauthorized electronic access to a designated storage location for BES Cyber System Information on February 10, 2017. The entity revoked access on August 28, 2017 (199 days). (no need and no CIP training) The root cause of this noncompliance was due to lack of functionality testing after a change was made that inadvertently dropped the approvers from the approval system workflow.
Risk Assessment	The noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not following its approval process, the entity granted electronic access to two (2) employees that should not have been approved for access. One employee was granted access to relays and other devices within the entity's substations and another employee was granted access to review confidential and restricted information. With this access, one individual could have managed relays and breakers and the second individual could have reviewed confidential network diagrams. If the individual that was granted access to the Medium Impact BES Cyber System had connected to any relays, there would be no alert or notification, but the access would have been logged. After review, the entity found that during the noncompliance period, neither user accessed the system they were incorrectly given access to. No harm is known to have occurred as a result of this noncompliance. The entity has two previous violations of CIP-004. NPCC determined that the entity's compliance history should not serve as a basis for applying a penalty. There was a different underlying cause for each of the prior violations.
Mitigation	To mitigate this noncompliance, the entity: 1) removed the unapproved access for each user; 2) corrected the workflow for the approval system; 3) conducted an off-cycle review in August 2017 and will compare against their upcoming third quarter access review; 4) created and updated their quarterly review procedure; 5) conducted additional off cycle reviews in November and December of 2017; and 6) implemented a control to stop the approval workflow if the approver field is blank.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
NPCC2017018606	CIP-004-6	R4.	[redacted]	[redacted]	1/11/2017	9/6/2017	Self-Report	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On November 13, 2017, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered on August 17, 2017 it was in noncompliance with CIP-004-6 R4. (4.1.) during a SOX audit of its global provisioning system. This noncompliance started on January 11, 2017 when the entity failed to follow its process to authorize electronic access for two (2) individuals to a Medium Impact BES Cyber System. The noncompliance ended on September 6, 2017, when the entity revoked the access that was unauthorized. Specifically, the entity's approval system stopped populating the "approver" field; as a result, the system auto approved access for two individuals instead of sending the approval request to the proper approver. The system issue was corrected on August 22, 2017. • One individual was granted unauthorized electronic access to a Medium Impact BES Cyber System on June 7, 2017. The entity revoked the unauthorized access on September 6, 2017 (91 days). • Another individual was granted unauthorized electronic access to a designated storage location for BES Cyber System Information on February 10, 2017. The entity revoked access on August 28, 2017 (199 days). (no need and no CIP training) The root cause of this noncompliance was due to lack of functionality testing after a change was made that inadvertently dropped the approvers from the approval system workflow.
Risk Assessment	The noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by not following its approval process, the entity granted electronic access to two (2) employees that should not have been approved for access. One employee was granted access to relays and other devices within the entity's substations and another employee was granted access to review confidential and restricted information. With this access one individual could have managed relays and breakers and the second individual could have reviewed confidential network diagrams. If the individual that was granted access to the Medium Impact BES Cyber System had connected to any relays there would be no alert or notification, but the access would have been logged. After review the entity found that during the noncompliance period, neither user accessed the system they were incorrectly given access to. No harm is known to have occurred as a result of this noncompliance. The entity has three previous violations of CIP-004. NPCC determined that the entity's compliance history should not serve as a basis for applying a penalty. There was a different underlying cause for each of the prior violations.
Mitigation	To mitigate this noncompliance, the entity: 1) removed the unapproved access for each user; 2) corrected the workflow for the approval system; 3) conducted an off-cycle review in August 2017 and will compare against their upcoming third quarter access review; 4) created and updated their quarterly review procedure; 5) conducted additional off cycle reviews in November and December of 2017; and 6) implemented a control to stop the approval workflow if the approver field is blank.

ReliabilityFirst (RF) FFT CIP

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018414	CIP-004-6	R4	[redacted]	[redacted]	7/1/2016	1/11/2018	Self-Report	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On September 22, 2017, [redacted] as a [redacted], submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-004-6 R4. Leading up to July 1, 2017, entity [redacted] performed verifications of electronic access to meet the requirements of CIP-004-6 R4.3. In the course of this work, the entity also opted to verify authorization records of access to CIP Information Repositories containing Bulk Electric System (BES) Cyber System Information (BCSI). In the review, the entity identified a number of instances (388) in which trusted employees and contractors were provisioned with access to CIP Information Repositories containing BCSI related to High Impact and Medium Impact BES Cyber Systems with External Routable Connectivity (ERC) without documented access authorization in the entity's [redacted]. In these cases, all users accessing the BCSI had a valid business need for access, but did not have the proper documentation of approval required by the entity's procedures. The entity completed an extent of condition review and identified no additional instances of noncompliance. The root causes of this noncompliance are as follows: (a) for 345 of the affected users, the CIP Information Repository settings permitted access via [redacted] permissions in [redacted] groups and the CIP Information Repositories were created [redacted] launch and before the entity created a procedure to guide the commissioning of a CIP Information Repositories; [redacted] (b) for the remaining 43 affected users, administrators erred by granting access manually, which is prohibited by the entity's policy; and, (c) when the entity created the CIP Information Repositories commissioning/decommissioning procedure, the entity did not perform checks of existing CIRs to ensure the permissions were set in a similar fashion as a new CIP Information Repositories to restrict use of [redacted] permissions. This noncompliance started on July 1, 2016, the date the entity was required to comply with CIP-004-6 R4, and ended on January 11, 2018, when the entity either requested authorization of access or removed access (because they no longer needed access at the time of discovery) for all affected users.
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk associated with failing to properly document authorization to access BCSI information is that it increases the likelihood that an unauthorized person could access, exfiltrate, or otherwise corrupt BCSI. This risk was mitigated in this case by the following factors. First, this is mostly a documentation issue because all affected users would have been granted access to the CIP Information Repositories had the entity completed the proper steps prior to the launch of [redacted] In other words, the users would have been granted access had they gone through the proper access request and approval process. Second, at the time access was granted, although not required by the standard for information access, the majority of the users had current personnel risk assessments and were up-to-date with the entity's NERC Annual Training as a result of prior or existing NERC CIP access. These factors reduce the likelihood that these users would have used the BCSI for any improper purpose. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances either arose from different root causes or constitute high frequency conduct that ReliabilityFirst determined did not warrant an alternative disposition method.
Mitigation	To mitigate this noncompliance, the entity: 1) performed an extent of condition to identify users who have NERC CIP information access without documented authorization; 2) created a role for [redacted] system administrators in the entity's [redacted] to allow administrators to have authorized access to [redacted] systems with the entity NERC CIP Protected information; 3) created tickets and authorized the [redacted] administrators and shared accounts to be added to the role; 4) requested authorization of access through the entity's [redacted] tool or remove access for the users identified in milestone one; 5) reinforced expectations for documenting and authorizing access controls in the entity's [redacted] documents to system administrators; 6) developed an internal control for identifying NERC CIP access permissions not authorized/tracked in [redacted] 7) confirmed that the entity's [redacted] document contains the [redacted] appropriate settings for a facilitate [redacted] comparison of actual to authorized access to all individuals with access to CIP Information Repositories; 8) assessed all existing CIP Information Repositories to make sure settings and permissions conform with the entity's Access Control procedures to facilitate [redacted] comparison of actual to authorized access to all individuals with access to CIP Information Repositories; and 9) provided training to affected system administrators to reinforce procedural exceptions and to discuss changes made to policies and supporting infrastructure.

ReliabilityFirst (RF) FFT CIP

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018410	CIP-004-6	R4	[redacted]	[redacted]	7/1/2016	1/11/2018	Self-Report	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On September 21, 2017, [redacted] as a [redacted], submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-004-6 R4. Leading up to July 1, 2017, entity [redacted] performed verifications of electronic access to meet the requirements of CIP-004-6 R4.3. In the course of this work, the entity also opted to verify authorization records of access to CIP Information Repositories containing Bulk Electric System (BES) Cyber System Information (BCSI). In the review, the entity identified a number of instances (388) in which trusted employees and contractors were provisioned with access to CIP Information Repositories containing BCSI related to High Impact and Medium Impact BES Cyber Systems with External Routable Connectivity (ERC) without documented access authorization in the entity's [redacted]. In these cases, all users accessing the BCSI had a valid business need for access, but did not have the proper documentation of approval required by the entity's procedures. The entity completed an extent of condition review and identified no additional instances of noncompliance. The root causes of this noncompliance are as follows: (a) for 345 of the affected users, the CIP Information Repository settings permitted access via [redacted] permissions in [redacted] groups and the CIP Information Repositories were created [redacted] launch and before the entity created a procedure to guide the commissioning of a CIP Information Repositories; [redacted] (b) for the remaining 43 affected users, administrators erred by granting access manually, which is prohibited by the entity's policy; and, (c) when the entity created the CIP Information Repositories commissioning/decommissioning procedure, the entity did not perform checks of existing CIP Information Repositories to ensure the permissions were set in a similar fashion as a new CIP Information Repositories to restrict use of [redacted] permissions. This noncompliance started on July 1, 2016, the date the entity was required to comply with CIP-004-6 R4, and ended on January 11, 2018, when the entity either requested authorization of access or removed access (because they no longer needed access at the time of discovery) for all affected users.
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk associated with failing to properly document authorization to access BCSI information is that it increases the likelihood that an unauthorized person could access, exfiltrate, or otherwise corrupt BCSI. This risk was mitigated in this case by the following factors. First, this is mostly a documentation issue because all affected users would have been granted access to the CIP Information Repositories had the entity completed the proper steps prior to the launch of [redacted] In other words, the users would have been granted access had they gone through the proper access request and approval process. Second, at the time access was granted, although not required by the standard for information access, the majority of the users had current personnel risk assessments and were up-to-date with the entity's NERC Annual Training as a result of prior or existing NERC CIP access. These factors reduce the likelihood that these users would have used the BCSI for any improper purpose. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances either arose from different root causes or constitute high frequency conduct that ReliabilityFirst determined did not warrant an alternative disposition method.
Mitigation	To mitigate this noncompliance, the entity: 1) performed an extent of condition to identify users who have NERC CIP information access without documented authorization; 2) created a role for [redacted] system administrators in the entity's [redacted] to allow administrators to have authorized access to [redacted] systems with the entity NERC CIP Protected information; 3) created tickets and authorized the [redacted] administrators and shared accounts to be added to the role; 4) requested authorization of access through the entity's [redacted] tool or remove access for the users identified in milestone one; 5) reinforced expectations for documenting and authorizing access controls in the entity's [redacted] documents to system administrators; 6) developed an internal control for identifying NERC CIP access permissions not authorized/tracked in [redacted] 7) confirmed that the entity's [redacted] document contains appropriate [redacted] settings for a facilitate [redacted] comparison of actual to authorized access to all individuals with access to CIP Information Repositories; 8) assessed all existing CIP Information Repositories to make sure settings and permissions conform with the entity's Access Control procedures to facilitate [redacted] comparison of actual to authorized access to all individuals with access to CIP Information Repositories; and 9) provided training to affected system administrators to reinforce procedural exceptions and to discuss changes made to policies and supporting infrastructure.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019281	CIP-004-6	R5	[redacted]	[redacted]	1/20/18	1/22/2018	Self-Report	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On February 21, 2018, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-004-6 R5. On Friday, January 19, 2018 at approximately 3:00 p.m. and 4:38 p.m., the entity's Access Administrator received requests to revoke unescorted physical access for two employees through the entity's access tool. One request was for an employee who was retiring from the entity, and the other was for a contractor who was no longer working for the entity. The Access Administrator was responsible for completing access revocation within 24 hours of receiving the requests. However, the requests were completed on Monday, January 22, 2018, at 3:00 a.m. after the Access Administrator checked his email regarding the request. This was 36 hours after the requests were received. Although the Access Administrator was aware of the access revocation requests on Friday, access was not revoked in a timely manner. The root causes were that the administrator failed to follow the procedure for revoking access, and the entity lacked sufficient controls to ensure that access was timely removed. The access tool was configured to send an email notification to initiate the removal, but was not configured to monitor timely revocation and send automated reminders if revocation did not occur. This noncompliance involves the management practices of verification, which includes having controls to help ensure that tasks are completed on time. This noncompliance started on January 20, 2018, the date by which the entity was required to remove access, and ended on January 22, 2018, when the entity removed access
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The potential risk posed by this noncompliance is that an individual who is no longer permitted to have access will use that access in a manner that will compromise the BPS. This risk is mitigated here by the following factors. First, the entity identified and corrected the noncompliance within only two days, thus reducing the period of time that there was any increased risk to the system as a result of the noncompliance. Second, the retired individual, who had access to a high impact Physical Security Perimeter, was a trusted individual who was unlikely to use his access in a manner that would compromise the Bulk Electric System. Also, the contractor separated on good terms when his two year-contract was complete, and he had only physical access to a medium impact Physical Security Perimeter. However, the entity's compliance history involves several instances of failure to timely revoke access as a result the revocation request being on a Friday or weekend. Thus, because of the recurring nature of the cause of the noncompliance, ReliabilityFirst determined that the noncompliance posed moderate risk instead of minimal risk. ReliabilityFirst also notes that the entity performed a review and confirmed that neither individual attempted to use their access following their last day of work. No harm is known to have occurred. The entity has relevant compliance history. For some of the prior violations and noncompliances, they are distinguishable from the current noncompliance because they involved different root causes. However, the entity's compliance history involves several instances of failure to timely revoke access as a result of the timing of the revocation request being on a Friday or weekend. Thus, because of the recurring nature of this type of noncompliance, ReliabilityFirst determined that the noncompliance posed moderate risk instead of minimal risk. Still, a penalty is not warranted because the noncompliance posed only moderate risk and not serious and substantial risk, and the current noncompliance involves high-frequency conduct for which the entity has demonstrated an ability to promptly identify and correct noncompliances.
Mitigation	To mitigate this noncompliance, the entity: 1) revoked access for the two individuals; 2) verified that no access or access attempts using the access cards for revoked users was made to ensure that no intentional or unintentional access was made to Physical Security Perimeters after the termination action; 3) built a monitoring functionality in the [redacted] to monitor the queue for pending revoke requests to monitor any open and approved revoke access (irrespective of the reason of termination) with a due date of equal or less than today. This query will be performed by the system every [redacted]. If any pending jobs are found, it will send a reminder to the [redacted] and [redacted]. This process will keep repeating until revoke action is taken; and 4) communicated the newly introduced functionality of [redacted]r reminder to all [redacted] ReliabilityFirst has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018409	CIP-004-6	R4	[redacted]	[redacted]	7/1/17	1/11/2018	Self-Report	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On September 21, 2017, [redacted] as a [redacted], submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-004-6 R4. Leading up to July 1, 2017, entity [redacted] performed verifications of electronic access to meet the requirements of CIP-004-6 R4.3. In the course of this work, the entity also opted to verify authorization records of access to CIP Information Repositories containing Bulk Electric System (BES) Cyber System Information (BCSI). In the review, the entity identified a number of instances (388) in which trusted employees and contractors were provisioned with access to CIP Information Repositories containing BCSI related to High Impact and Medium Impact BES Cyber Systems with External Routable Connectivity (ERC) without documented access authorization in the entity's [redacted] In these cases, all users accessing the BCSI had a valid business need for access, but did not have the proper documentation of approval required by the entity's procedures. The entity completed an extent of condition review and identified no additional instances of noncompliance. The root causes of this noncompliance are as follows: (a) for 345 of the affected users, the CIP Information Repository settings permitted access via [redacted] permissions in [redacted] groups and the CIP Information Repositories were created [redacted] launch and before the entity created a procedure to guide the commissioning of a [redacted]; [redacted] (b) for the remaining 43 affected users, administrators erred by granting access manually, which is prohibited by the entity's policy; and, (c) when the entity created the CIP Information Repositories commissioning/decommissioning procedure, the entity did not perform checks of existing CIP Information Repositories to ensure the permissions were set in a similar fashion as a new CIP Information Repositories to restrict use of [redacted] permissions. This noncompliance started on July 1, 2016, the date the entity was required to comply with CIP-004-6 R4, and ended on January 11, 2018, when the entity either requested authorization of access or removed access (because they no longer needed access at the time of discovery) for all affected users.
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk associated with failing to properly document authorization to access BCSI information is that it increases the likelihood that an unauthorized person could access, exfiltrate, or otherwise corrupt BCSI. This risk was mitigated in this case by the following factors. First, this is mostly a documentation issue because all affected users would have been granted access to the CIP Information Repositories had the entity completed the proper steps prior to the launch of [redacted] In other words, the users would have been granted access had they gone through the proper access request and approval process. Second, at the time access was granted, although not required by the standard for information access, the majority of the users had current personnel risk assessments and were up-to-date with the entity's NERC Annual Training as a result of prior or existing NERC CIP access. These factors reduce the likelihood that these users would have used the BCSI for any improper purpose. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances either arose from different root causes or constitute high frequency conduct that ReliabilityFirst determined did not warrant an alternative disposition method.
Mitigation	To mitigate this noncompliance, the entity: 1) performed an extent of condition to identify users who have NERC CIP information access without documented authorization; 2) created a role for [redacted] system administrators in the entity's [redacted] to allow administrators to have authorized access to [redacted] systems with the entity NERC CIP Protected information; 3) created tickets and authorized the [redacted] administrators and shared accounts to be added to the role; 4) requested authorization of access through the entity's [redacted] tool or remove access for the users identified in milestone one; 5) reinforced expectations for documenting and authorizing access controls in the entity's [redacted] documents to system administrators; 6) developed an internal control for identifying NERC CIP access permissions not authorized/tracked in [redacted] 7) confirmed the entity's [redacted] document contains the [redacted] settings that are appropriate for a facilitate [redacted] comparison of actual to authorized access to all individuals with access to CIP Information Repositories; 8) assessed all existing CIP Information Repositories to make sure settings and permissions conform with the entity's Access Control procedures to facilitate [redacted] comparison of actual to authorized access to all individuals with access to CIP Information Repositories; and 9) provided training to affected system administrators to reinforce procedural exceptions and to discuss changes made to policies and supporting infrastructure.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019255	CIP-007-6	R1	[redacted]	[redacted]	7/1/2016	7/27/2017	Self-Report	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On February 19, 2018, [redacted] submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R1. The entity discovered that five unnecessary logical network accessible ports were enabled. The ports were left open as part of the devices' original configurations, which occurred prior to the devices coming into scope for the CIP Standards. Three of the five instances occurred as part of initial device configuration and the other two instances occurred because of a firmware update. The entity discovered these five instances while conducting its first Cyber Vulnerability Assessment (CVA) after CIP v5 went into effect. The five instances are as follows: a) Two instances involved an open port relating to a [redacted]. These ports were enabled on July 1, 2016 and disabled on July 27, 2017. b) The third instance involved an open port relating to a [redacted]. This port was enabled on July 1, 2016 and disabled on June 29, 2017. c) The fourth instance involved an opened port on a [redacted] This port was enabled on October 20, 2016 and disabled on June 30, 2017. d) The fifth instance involved an opened port on a [redacted]. This port was enabled on October 25, 2016 and the device was retired on June 15, 2017. This noncompliance involves the management practices of work management and verification as the entity did not have a sufficient process in place to detect unnecessary ports for devices that are not connected to the entity's configuration management tool. The entity relied on employees to manually identify and disable the ports involved. That reliance on manual verification by employees is a root cause of this noncompliance. This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-007-6 R1 and ended on July 27, 2017 when the entity disabled all of the ports at issue in each of the five instances.
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The risk posed by this noncompliance is creating opportunities for unauthorized access through unidentified open ports that could negatively affect the reliable operation of the BPS. The risk is not minimal because of the long duration which reflects ineffective detective controls and the number of instances in this noncompliance. The risk is lessened because all of the devices were protected within CIP Electronic Security Perimeters (ESPs) for the duration of the noncompliance. Additionally, three of the five devices were protected within a CIP Electronic PSP and two of those three were protected by firewalls. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because of the different causes of the prior noncompliances.
Mitigation	To mitigate this noncompliance, the entity: 1) disabled all ports in question; and 2) reviewed with applicable personnel procedures related to manually confirming enabled ports. The entity has recently implemented [redacted] scanning of the [redacted] Servers by the entity's [redacted] application. Any detected changes to [redacted] Server baseline ports will trigger a notification to maintenance personnel for investigation and follow-up. [redacted]. ReliabilityFirst has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019256	CIP-010-2	R1	[redacted]	[redacted]	7/1/2016	5/18/2017	Self-Report	Completed

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On February 19, 2018, [redacted] submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-010-2 R1. While conducting its Cyber Vulnerability Assessment after CIP v5 went into effect, the entity discovered that it did not include a commercially available executable in its documented baseline configuration of High Impact Bulk Electric System Cyber Workstations as required in R1.1.2. [redacted] The entity determined that an executable present during the initial baseline configuration was not documented because it was not detected by the entity's configuration management tool. The executable was not detected because it did not register [redacted]. The entity's further investigation revealed that this executable was identified as being required on the workstations and was approved, but missed being documented in the approved baseline configuration. There have been no changes in this executable since its original deployment. The entity discovered this issue using [redacted] tool as part of the entity's annual cyber vulnerability assessment process on July 20, 2017. This noncompliance involves the management practices of validation and verification. The entity did not have an effective verification internal control in place to ensure that this executable was properly documented in the approved baseline configuration. That lack of an effective verification control is a root cause of this noncompliance. This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-010-2 R1 and ended on May 18, 2017, when the entity documented this executable on the configuration management tool and added it to the workstation baseline configuration.
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The risk posed by this noncompliance is that the entity was not checking for updates to configurations and applying those updates in a timely manner, which could allow changes to be made to software that could negatively affect the BPS without the entity's knowledge. The risk is not minimal because of the long duration which reflects ineffective detective controls. The risk is lessened because the executable that was installed and not documented had previously been approved for installation and had been deemed necessary by entity staff. Additionally, all workstations affected by this executable were protected within CIP Electronic Security Perimeters and Physical Security Perimeters. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because of the different causes of the prior noncompliances.
Mitigation	To mitigate this noncompliance, the entity: 1) documented the executable on the configuration management tool and added it to the workstation baseline configuration; 2) performed an extent of condition review to verify there were no other executables overlooked. All CIP workstations and servers were evaluated as part of the annual cyber vulnerability assessment. That extent of condition found that no other executables were overlooked; and 3) created a new technical control that inventories workstation executables, stores the inventory to the enterprise configuration management tool, and performs a nightly differential scan. ReliabilityFirst has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018415	CIP-004-6	R4	[redacted]	[redacted]	7/1/2016	1/11/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On September 22, 2017, [redacted] as a [redacted], submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-004-6 R4. Leading up to July 1, 2017, entity [redacted] performed verifications of electronic access to meet the requirements of CIP-004-6 R4.3. In the course of this work, the entity also opted to verify authorization records of access to CIP Information Repositories containing Bulk Electric System (BES) Cyber System Information (BCSI). In the review, the entity identified a number of instances (388) in which trusted employees and contractors were provisioned with access to CIP Information Repositories containing BCSI related to High Impact and Medium Impact BES Cyber Systems with External Routable Connectivity (ERC) without documented access authorization in the entity's [redacted] In these cases, all users accessing the BCSI had a valid business need for access, but did not have the proper documentation of approval required by the entity's procedures. The entity completed an extent of condition review and identified no additional instances of noncompliance. The root causes of this noncompliance are as follows: (a) for 345 of the affected users, the CIP Information Repository settings permitted access via [redacted] permissions in [redacted] groups and the CIP Information Repositories were created [redacted] launch and before the entity created a procedure to guide the commissioning of a [redacted]; [redacted] (b) for the remaining 43 affected users, administrators erred by granting access manually, which is prohibited by the entity's policy; and, (c) when the entity created the CIP Information Repositories commissioning/decommissioning procedure, the entity did not perform checks of existing CIP Information Repositories to ensure the permissions were set in a similar fashion as a new CIP Information Repositories to restrict use of [redacted] permissions. This noncompliance started on July 1, 2016, the date the entity was required to comply with CIP-004-6 R4, and ended on January 11, 2018, when the entity either requested authorization of access or removed access (because they no longer needed access at the time of discovery) for all affected users.						
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk associated with failing to properly document authorization to access BCSI information is that it increases the likelihood that an unauthorized person could access, exfiltrate, or otherwise corrupt BCSI. This risk was mitigated in this case by the following factors. First, this is mostly a documentation issue because all affected users would have been granted access to the CIP Information Repositories had the entity completed the proper steps prior to the launch of [redacted] In other words, the users would have been granted access had they gone through the proper access request and approval process. Second, at the time access was granted, although not required by the standard for information access, the majority of the users had current personnel risk assessments and were up-to-date with the entity's NERC Annual Training as a result of prior or existing NERC CIP access. These factors reduce the likelihood that these users would have used the BCSI for any improper purpose. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances either arose from different root causes or constitute high frequency conduct that ReliabilityFirst determined did not warrant an alternative disposition method.						
Mitigation	To mitigate this noncompliance, the entity: 1) performed an extent of condition to identify users who have NERC CIP information access without documented authorization; 2) created a role for [redacted] system administrators in the entity's [redacted] to allow administrators to have authorized access to [redacted] systems with the entity NERC CIP Protected information; 3) created tickets and authorized the [redacted] administrators and shared accounts to be added to the role; 4) requested authorization of access through the entity's [redacted] tool or removed access for the users identified in milestone one; 5) reinforced expectations for documenting and authorizing access controls in the entity's [redacted] documents to system administrators; 6) developed an internal control for identifying NERC CIP access permissions not authorized/tracked in [redacted] 7) confirmed that the entity's [redacted] document contains appropriate [redacted] settings for a facilitate [redacted] comparison of actual to authorized access to all individuals with access to CIP Information Repositories; 8) assessed all existing CIP Information Repositories to make sure settings and permissions conform with the entity's Access Control procedures to facilitate [redacted] comparison of actual to authorized access to all individuals with access to CIP Information Repositories; and 9) provided training to affected system administrators to reinforce procedural exceptions and to discuss changes made to policies and supporting infrastructure.						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016171	CIP-005-5	R1; P1.2	[redacted]	[redacted]	7/1/2016	9/16/2016	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On September 20, 2016, [redacted] submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-005-5 R1, Part 1.2. For a Medium Impact Bulk Electric System (BES) Cyber System, the entity did not ensure all external routable traffic went through an identified Electronic Access Point (EAP) before entering two Electronic Security Perimeters (ESPs). On September 15, 2016, while conducting a review of the Medium Impact network configurations due to detected unusual network traffic, the entity discovered External Routable Connectivity that was allowed to enter the ESPs without first going through an EAP. Specifically, sometime prior to July 1, 2016, the entity established Ethernet connections with access points within two ESPs (one at the primary control center and one at the backup control center) that terminated on Cyber Assets that resided outside the ESPs. The entity did not route the Ethernet connections through identified EAPs. These connections allowed the two energy management system (EMS) front end processors (FEPs), which resided inside the ESPs, to monitor access point traffic and display real time telemetry on the quality assurance system (QAS) network outside the ESPs. When originally deployed, the entity believed the data traffic was only one way from within the ESPs to outside the ESPs, and thus not considered External Routable Connectivity, due to documentation from the vendor. However, the connection allowed bi-directional communication into and out of the ESPs. On September 16, 2016, the entity disconnected the Ethernet connections to both the primary and backup control center ESPs. The bi-directional connection between the two FEP devices at the two control centers to the QAS network involved seven QAS Cyber Assets that were within the QAS environment. The noncompliance could have potentially affected one BES Cyber System (the EMS) with 48 BES Cyber Assets, 10 Protected Cyber Assets, 22 Electronic Access Control or Monitoring System Cyber Assets, and 4 Physical Access Control System Cyber Assets. The entity conducted an extent of condition review of all network configuration diagrams and determined no other similar connectivity existed. SERC determined that the root-cause was inadequate procedural controls to assess assets and their networking capabilities. This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable on the entity, and ended September 16, 2016, when the entity disconnected the Ethernet connections to the ESPs.
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The entity's failure to route all externally connected ESP traffic through an identified EAP could have permitted unsecured traffic to cross into and out of the ESPs and led to data mining or the introduction of malicious code into the most protected network. However, after investigating, the entity and its vendor concluded the unidentified bi-directional capability of the connection was not exploited during the noncompliance. Further, the connection was not configured as bi-directional. In addition, the QAS resided within a secure Physical Security Perimeter and had access controls in place, including malware protection with security logging and alerting. Finally, the QAS was subject to change management procedures and [redacted]. SERC considered the entity's compliance history and determined that there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1) disconnected the offending connections and added port blocks to the device; 2) sent a request to its SCADA vendor to confirm the potential risk and received confirmation; 3) confirmed with SERC that Self Reporting was the correct approach to report the potential violation; and 4) created a cable change request form to note any changes made to the network cabling so they can be included in the network documentation and reconciled with the authorized change(s).

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016418	CIP-007-6	R2; P2.2	[redacted]	[redacted]	7/1/2016	10/24/2016	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			On October 27, 2016, [redacted] submitted a Self-Report stating that, [redacted], it was in noncompliance with CIP-007-6 R2, Part 2.2. The entity failed to, at least once every 35 days, evaluate security patches for applicability that had been released since the last evaluation. On October 19, 2016, the entity discovered this noncompliance while performing a documentation review for future system upgrades. On July 1, 2016, Microsoft released two updated service packs, and on July 26, 2016, Microsoft released one updated service pack for certain production software on certain entity Cyber Assets within the primary and backup control centers and two data centers. However, the entity did not assess or install these service packs or their related security patches until October 24, 2016. The noncompliance involved one medium impact Bulk Electric System (BES) Cyber System (the energy management system), 44 BES Cyber Assets, 8 Protected Cyber Assets, 20 Electronic Access Control or Monitoring System Cyber Assets, and 3 Physical Access Control System Cyber Assets. The entity conducted an extent-of-condition and determined there were no additional instances of noncompliance. The root cause of this noncompliance was inadequate training to ensure staff selected the correct options in the patching tool applicability report when conducting security patch applicability assessments. The entity's documented patch management process required that service packs be included in the patching tool applicability report for security patch evaluation. However, entity staff did not select the "service packs" option in the patching applicability tool, and therefore the tool did not flag the new service pack releases for patch management program review. For this reason, the entity created a more detailed and granular workflow process and trained all affected personnel. This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable on the entity, and ended on October 24, 2016, when the entity completed its security patch assessment for the missed patches and applied applicable patches.				
Risk Assessment			This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The entity's failure to evaluate security patches for applicability at least once every 35 calendar days could have potentially provided security holes that could have resulted in the occurrence of malicious activity. [redacted] In addition, malware protection, baseline monitoring, and security logging were in place to thwart intruders. SERC considered the entity's compliance history and determined that there were no relevant instances of noncompliance.				
Mitigation			To mitigate this noncompliance, the entity: 1) added service packs to the patching tool applicability report option and determined it had several CIP cyber assets with SQL service packs available for evaluation. The entity applied the applicable service packs; 2) reviewed the entity's documented processes regarding patching and determined the language was sufficient for the review of "security patch" and "service pack"; 3) The patching tool applicability report template has to be populated each month and the options for "security patch" and "service pack" need to be selected. The entity's BES cyber support team made the change to the monthly patch process workflow; and 4) discussed the change to the monthly patch process work flow during the next CIP meeting, held each Monday. At this meeting, the entity made its BES cyber support team members aware of the revised monthly patch process work flow. The BES cyber support team will implement this version going forward, ensuring the service packs will be selected in the patching tool applicability report options.				

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018724	CIP-007-6	R2; P2.3	[redacted]	[redacted]	8/23/2017	11/20/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			On November 28, 2017, [redacted] submitted a Self-Report to SERC stating that, [redacted] it was in noncompliance with CIP-007-6 R2, Part 2.3. The entity did not did not apply a patch to two Bulk Electric System (BES) Cyber Assets within 35 calendar days of completing its evaluation. On July 18, 2017, the entity reviewed a security patch for applicability and found it to be applicable, but failed to apply the patch to two BES Cyber Assets within 35 days of the assessment. The two involved BES Cyber Assets were housed within a backup control center and a data center and were part of one Medium Impact BES Cyber System. On November 20, 2017, the entity discovered this noncompliance while reviewing energy management system (EMS) July security patches as part of a workflow execution internal control. The internal control involved reconciling implemented patch configuration changes against the new documented baseline. Upon discovering an inconsistency, the entity promptly applied the overdue July patch the same day. The entity performed an extent-of-condition review by broadly applying the internal control that resulted in the discovery of the compliance issue. Specifically, the entity reviewed all past patch evaluations and applications of security patches and did not find any additional issues. The root cause of this noncompliance was insufficiently robust workflow tools and associated training. This noncompliance started on August 23, 2017, when the entity failed to apply a security patch within 35 days of determining it was applicable, and ended on November 20, 2017, when the entity applied the missed security patch.				
Risk Assessment			This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The entity's failure to apply a security patch for approximately 90 days after determining it was applicable created a potential for intruders to exploit security vulnerabilities, install malware or otherwise gain control over Cyber Assets and bulk power system facilities, and potentially create an unstable grid. However, the entity and its EMS vendor determined the late patch addressed minor risks. The entity employed the affected Cyber Assets primarily as backup control center assets. Additionally, the entity utilized electronic access controls, malware protection, logging and alerting, and housed the assets in Electronic and Physical Security Perimeters. SERC considered the entity's compliance history and determined that there were no relevant instances of noncompliance.				
Mitigation			To mitigate this noncompliance, the entity: 1) applied the missed security patch to the applicable software; and 2) implemented a process for all subject matter experts to use a check list which will be attached to the asset and resource management tool case.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017016970	CIP-010-2	R1; P1.2; P1.4	[redacted]	[redacted]	12/13/2016	2/8/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On February 8, 2017, [redacted] submitted a Self-Report to SERC stating that, [redacted] it was in noncompliance with CIP-010-2 R1, Parts 1.2 and 1.4. The entity did not authorize and document changes that deviated from the existing baseline configuration (1.2) and did not determine, verify, and document any adverse effects related to changes that deviated from the existing baseline (1.4). On December 13, 2016, the entity made modifications to a custom script reflecting a revised load shed plan and then deployed the script to four Bulk Electric System (BES) Cyber Assets, [redacted] Similarly, on December 19, 2016, the entity made modifications to a different custom script implementing [redacted] and deployed the script to the same four BES Cyber Assets. The four involved BES Cyber Assets were part of one Medium Impact BES Cyber System and were located at the primary and backup control centers and data centers. Although all of the modifications to the baseline configurations were technically necessary and correct from an operations standpoint, the entity did not implement them in conformance with its documented procedures and the baseline configuration change requirements of CIP-010-2 R1, Parts 1.2 and 1.4. The entity did not authorize and document the changes that deviated from the existing baseline configuration and did not determine and verify that CIP-005 and CIP-007 cyber security controls were not adversely impacted after the changes. On February 6, 2017, the entity discovered this noncompliance during an internal control reconciliation process, where every 31 days it compared actual baseline configurations with its change control management system, and noticed an actual configuration that was inconsistent with the expected baseline configuration. On February 8, 2017, the entity performed the baseline configuration change management procedures for these four BES Cyber Assets. As the extent-of-condition review, the entity reviewed all change control records in the change management system for proper adherence to procedures and did not find any additional failures. The root cause of this noncompliance was shortfalls in training related to consistently following baseline change control procedures. This noncompliance started on December 13, 2016, when the entity made configuration changes without following change control procedures, and ended on February 8, 2017, when the entity completed change control procedures.
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The entity not evaluating security controls could result in modifications to the existing security infrastructure that would enable misoperation or unauthorized access to BES Cyber Systems, which could adversely impact the BPS. However, a monthly internal control led to discovery. All of the modifications to the baseline configurations were technically necessary and correct from an operations standpoint. SERC considered the entity's compliance history and determined that there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1) interviewed the involved operations engineer and re-reviewed all change records in the change management system to determine the extent of condition, which confirmed no other custom script changes were made and not reconciled; 2) made the operations engineer fully aware of the existing policy that the custom script changes require a case within the asset and resource management tool, for review and approval; and 3) created a case within the asset and resource management tool to complete the required review and approval process for the changes to the baseline.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018599	CIP-010-2	R1; P1.1; P1.2; P1.3; P1.4	[redacted]	[redacted]	7/1/2016	1/18/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On November 7, 2017, [redacted] submitted a Self-Report to SERC stating that, [redacted] it was in noncompliance with CIP-002-5.1a R1, Part 1.2. However, SERC determined that the entity was instead in noncompliance with CIP-010-2 R1, Part 1.1 – 1.4 because it failed to identify and develop baseline configurations for Physical Access Control Systems (PACS). On September 28, 2017, as a follow up from a 2016 Cyber Vulnerability Assessment (CVA), the entity's Bulk Electric System (BES) cyber support group reviewed Cyber Assets located at the primary control center data center and discovered that it had not identified two Remote Terminal Units (RTUs) as components of the PACS. The two RTUs transmitted alarming signals from the PACS to the Supervisory Control and Data Acquisition system, which then provided the physical security status, alerts, and alarms to the electric system dispatchers for monitoring. Because the entity used the two RTUs to transmit alarming, they were components of the PACS and required to be protected under CIP-010-2 R1, Part 1.1 – 1.4. The noncompliance affected four facilities, including the primary and back-up control centers and their associated data centers, which contained medium impact Bulk Electric System (BES) Cyber Systems. The entity conducted an extent-of-condition assessment and determined there were no other instances of unidentified or misclassified Cyber Assets. The failure to identify the RTUs as PACS resulted in the entity not affording the RTUs the protections required by CIP-010-2 R1, Part 1.1 -1.4 (baselines), CIP-010-2 R3, Parts 3.1 and 3.4 (vulnerability assessments), CIP-007-6, R1 Part 1.1 (justified ports), CIP-007-6 R2, Parts 2.1-2.4 (security patch management), CIP-007-6 R3, Parts 3.1-3.3 (malicious code prevention), CIP-007-6 R4, Parts 4.1 and 4.2 (event logging and alerting), CIP-007-6 R5, Part 5.2 (document default or generic accounts), and CIP-007-6 R5, Parts 5.5-5.7 (password complexity, change process, and technical feasibility exception). The root-cause of this noncompliance was a lack of formal guidance, such as procedures and checklists, to evaluate and classify all Cyber Assets within the CIP program. This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable on the entity, and ended on January 18, 2018, when the entity provided all appropriate CIP protections to the PACS Cyber Assets.						
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. By not identifying and fully protecting the PACS Cyber Assets, the entity created a potential that an attack could destroy, damage, or degrade Critical Infrastructure within the entity's facilities via weaknesses in security on the two RTUs responsible for generating alerts and alarms for physical security problems. However, the entity did physically secure the two RTUs at issue within a Physical Security Perimeter, shielding them from general access. The entity also enforced local authentication for access and did not allow access to any shared accounts on the two RTUs. Although the entity did not document default accounts, it did change all default passwords on the two RTUs. The System Operators also monitored the health and status of the two RTUs at issue in real-time. Any abnormal operations or changes to the RTUs would have resulted in an alarm to the operator to investigate. During the noncompliance, the RTUs operated as intended to send alerts and alarms to the System Operators. SERC considered the entity's compliance history and determined that there were no relevant instances of noncompliance.						
Mitigation	To mitigate this noncompliance, the entity: 1) reviewed the NERC Standard requirements applicable to a BES Cyber Asset to determine if the current RTU is capable of meeting these requirements when the RTU is added to the entity's CIP-002 BES Cyber Asset list. The entity confirmed the current RTU does not support the NERC Cyber Security requirements associated with a BES Cyber Asset and would require a Technical Feasibility Exception (TFE). Therefore, the entity purchased a new RTU compatible with the current NERC Cyber Security requirements and moved the BES Cyber Asset into the Electronic Security Perimeter (ESP); 2) reviewed the functionality of the RTU and associated analog and status data points to confirm if [redacted] functional type data was transmitted through the RTU to SCADA for use by the electric system operators; 3) the entity's BES cyber support group developed the CIP-002 Medium Impact Cyber Asset evaluation flow chart The BES cyber support group members are the employees that will be using the evaluation flow chart; 4) updated the Cyber Asset list to include the dispatch and strip chart RTUs; 5) updated the Cyber Asset list to remove the dispatch RTU. The entity removed the dispatch RTU from Medium BES Cyber System sheet and moved it to the retired assets sheet; 6) added the involved RTU to the Medium BES Cyber System list and moved the strip chart RTU to the retired assets sheet; 7) completed all required steps prior to placing the asset on the network. The entity will place the asset on the FEP network in order to test the log collection and aggregation tool for logging and alerting. Once the entity configures logging, it will place the asset into full service on the BES;						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017018599	CIP-010-2	R1; P1.1; P1.2; P1.3; P1.4	[redacted]	[redacted]	7/1/2016	1/18/2018	Self-Report	Completed
			8) updated and approved the remaining documentation upon successful completion of new baseline reports per CIP-010-2 Part 1.1. The entity will manage the new asset by its configuration change management process; 9) reviewed and approved the Cyber Asset provisioning checklist. The entity configured logging and alerting for the asset connected to the ESP; 10) implemented a new RTU asset which is now performing BES functionality; 11) received information on why the specific communication protocol is required and opened a port for internal communications only per port guide; and 12) closed the related asset and resource management tool workflow case and provided a summary of actions taken by the entity for the deployment of the new RTU with dates.					