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	RFC2018020405	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 years
2	SERC2016016517			Yes	Yes					Yes				Category 2 – 12: 2 year
3	SERC2017017916			Yes	Yes					Yes				Category 2 – 12: 2 year
4	TRE2017017518	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
5	TRE2017017683	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
6	TRE2018020155	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 year
7	TRE2018020695	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
8	TRE2018019766	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
9	TRE2018019767	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
10	TRE2018019768	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
11	TRE2018019769	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
12	TRE2018020690	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
13	TRE2018020694	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 year
14	WECC2019020901			Yes	Yes								Yes	Category 1: 3 years; Category 2 – 12: 2 year

ReliabilityFirst Corporation (ReliabilityFirst) 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
RFC2018020405	CIP-007-6	R4	[redacted]	[redacted]	7/1/2016	7/20/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On September 7, 2018, the entity submitted a Self-Report stating that, [redacted], it was in noncompliance with CIP-007-6 R4. On March 29, 2018, the entity determined that [redacted] was not configured to capture the local logs from a firewall device. Two steps are necessary in order for this to occur properly. [redacted] In this case, the logs were being sent to [redacted]. However, [redacted] was not configured to read the logs and alert on them until March 29, 2018. The root cause of this noncompliance was two-fold. First, at the time the firewall was placed into service, the entity did not have a formal process for adding devices to [redacted]. Rather, the entity used [redacted], which was more susceptible to human error. Second, in this particular case, when [redacted], the [redacted] failed to act on it. This root cause involves the management practice of implementation, because this noncompliance involved failures relating to the implementation of a new device. This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-007-6 R4 and ended on July 20, 2018, when the entity committed to correct the configuration issue with [redacted].
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 posed by failing to have [redacted] read locally generated logs and alert on them is that it would delay the entity's ability to discover and review an event, had one occurred. This risk is not minimal in this case because the firewall at issue supports Electronic Security Perimeter functions. This risk is not serious or substantial in this case because local logging was still occurring and the entity could have obtained those local logs if needed. Moreover, the entity's defense-in-depth strategy also provided additional protections. Specifically in this case, [redacted] Additionally, the entity had several preventative measures in place around this firewall device including (a) [redacted]. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because, although the noncompliance is arguably similar to some prior noncompliances, the entity self-identified this noncompliance, enhanced its corresponding procedure by introducing automated controls to reduce human error, and the noncompliance posed only moderate and not serious and substantial risk to the reliability of bulk power system.
Mitigation	To mitigate this noncompliance, the entity: 1) configured [redacted] to capture events on the impacted firewall; 2) re-enforced, [redacted] the need to make sure all requests for configuring new devices to [redacted] are completed on time with current [redacted]; 3) re-enforced, during a team meeting, the need to make sure all requests for configuring new devices [redacted] are completed on time with current [redacted]; 4) developed a procedure for onboarding devices [redacted]; 5) updated existing job aid to include a change management installation plan task assigned to the appropriate [redacted] team for onboarding the device [redacted]; 6) communicated the update during the next scheduled change management meeting; and 7) confirmed all entity devices in scope of CIP-007 R4.2 alerting requirements are monitored in real time.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2016016517	CIP-002-5.1	R1, P1.2	[redacted]	[redacted]	07/01/2016	03/31/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			On November 16, 2016, [redacted] submitted a Self-Report to SERC stating that, as a [redacted], it was in noncompliance with CIP-002-5.1 R1, P1.2. The entity did not consider [redacted] Bulk Electric (BES) Cyber Assets (BCAs) when identifying its medium impact (BES) Cyber Systems (BCSs) according to Attachment 1, Section 2. On October 13, 2016, while conducting an internal control risk-based self-audit of CIP requirements, the entity discovered that it had not classified [redacted] Remote Terminal Unit (RTU) peripheral boards as BCAs, which were a part of the entity's medium impact BCSs. When the entity assessed the CIP-002 classification of the peripheral boards, it relied on a NERC-related product bulletin from the manufacturer for guidance. The bulletin did not mention that the RTU's peripheral boards were separate Cyber Assets from the RTU main board. Consequently, the entity staff initially assumed that the boards were not separately programmable. However, the entity later learned that the capability existed for direct connection of a diagnostic cable to the peripheral board. While the entity did not employ the diagnostic cable connection in the course of normal business, the connection would nonetheless enable a technician to perform programmable maintenance activities, including changing RTU configuration and status. The [redacted] RTU boards involved could have permitted changes to be made to the [redacted] substations where the boards were located. The [redacted] substations included [redacted] medium impact BCSs, also classified as [redacted] BCAs. The entity performed an extent-of-condition assessment by reviewing all CIP-002 inventory for instances of a similar nature and did not find any additional instances. This noncompliance started on July 1, 2016, when the standard became mandatory and enforceable on the entity, and ended on March 31, 2017, when the entity assessed the boards and added them to the list of BCSs. The root cause of this noncompliance was deficient procedures, which lacked specific instructions on what to review and assess when determining BCS identifications.				
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 the entity not identifying the RTU peripheral boards as BCAs, there was a potential opportunity afforded for a malicious party to access them, modify configurations, and cause a change in grid monitoring capability or unwanted operations. However, the RTU and peripheral boards had no External Routable Connectivity. Malicious activity would have required physical access to CIP-006 secured Physical Security Perimeters, as interactive access to the affected peripheral boards required a hardwired serial connection. Furthermore, the peripheral boards were not user firmware upgradable, and [redacted] control center operators monitored the real-time operational status of these devices at all times. Finally, the issue did not affect Protection System relaying. 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) assessed the peripheral boards as BCAs and added them to the list of BCSs; 2) ensured the additional details around peripheral boards are included in its CIP processes; 3) provided training prior to the Cyber Vulnerability Assessment on lessons learned for asset identification; 4) updated its CIP-002-5.1 process to include assessments of new candidate BCAs for peripheral or sub-assets, which may contain additional interfaces; and 5) shared the details of the findings and mitigating activities to other functional groups at the entity to raise awareness of the compliance concern.				

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
SERC2017017916	CIP-007-6	R1, P1.1	[redacted]	[redacted]	7/1/2016	7/7/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			On July 11, 2017, the entity submitted a Self-Report to SERC stating that, as a [redacted] and [redacted], it was in noncompliance with CIP-007-6 R1, Part 1.1. In [redacted] instances, the entity failed to enable only needed logical network accessible ports. Sometime prior to July 1, 2016, the entity enabled an unneeded network time protocol (NTP) server port on a substation gateway Bulk Electric System Cyber Asset (BCA). On June 8, 2017, the entity discovered this unneeded port while conducting its annual Cyber Vulnerability Assessment (CVA). The entity conducted an extent-of-condition assessment by assessing all configuration files for all substation gateways and security appliances associated with CIP medium impact substations. On June 23, 2017, during the extent-of-condition review for this issue, the entity discovered [redacted] additional BCAs with unneeded enabled logical network accessible ports. Specifically, sometime prior to July 1, 2016, the entity enabled an unneeded legacy status server port on another substation gateway BCA and an unneeded virtual private network (VPN) port on another substation gateway BCA. Affected Cyber Assets included [redacted] medium impact BES Cyber Systems, also classified as [redacted] BCAs, associated with [redacted] substations. The root cause of this noncompliance was inadequate training for establishing intended BCA port configurations during setup of the affected Cyber Assets. This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable on the entity, and ended on July 7, 2017, when the entity disabled the unnecessary ports.				
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 enabling only needed logical network accessible ports, the entity afforded potential avenues for hackers to maliciously exploit access to BCAs and disrupt configurations or effect command and control of BES facilities. However, the entity employed end-to-end encrypted communications and secured the BCAs in Physical Security Perimeters and Electronic Security Perimeters, which did not permit network traffic to the unneeded ports. 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) updated the affected Cyber Assets and closed the unnecessary ports; 2) for the Electronic Access Control and/or Monitory System, confirmed with the vendor that the unnecessary ports could be disabled; 3) disabled the ports that were unnecessary and capable of being disabled; 4) updated the ports spreadsheet with the necessary ports; 5) for new device installations, created a CIP compliant configuration template file to configure the substation gateway with; and 6) for training, instructed the engineers responsible for commissioning substation gateways to create the template file to ensure they are knowledgeable of the file's purpose and use.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017017518	CIP-007-6	R2: P2.2; P2.3	[redacted] (the "Entity")	[redacted]	07/12/2016	07/10/2017	Compliance Audit	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	During a Compliance Audit conducted from [redacted] Texas RE determined that the Entity, as a [redacted] was in noncompliance with CIP-007-6 R2. Specifically, the Entity failed to timely evaluate security patches for applicability and failed to either apply several security patches or create or revise a mitigation plan within 35 calendar days of the evaluation completion. In addition, the Entity created mitigation plans that did not include the Entity's planned actions to mitigate the vulnerabilities addressed by each security patch. Between August 17, 2016, and February 14, 2017, the Entity failed to timely evaluate [redacted] patches, and, for [redacted] security patches, the Entity did not timely apply the security patches or create or revise a mitigation plan. Subsequently, on March 14, 2017, the Entity created a mitigation plan indicating that it would temporarily discontinue its patching process for all Cyber Assets in order to modify its patch management system to address the issues identified during the Compliance Audit. However, in April 2017, when the Entity attempted to resume its patching program, the Entity experienced issues with its patching tool, which prevented the Entity from implementing its patching process and which was not repaired until May 22, 2017. During this period, the Entity did not evaluate or apply any security patches. On June 22, 2017, the Entity evaluated and applied the outstanding patches for several of its Cyber Assets, and, on July 7, 2017, all outstanding security patches were applied to all of the Cyber Assets managed by the Entity's patching tool. Although the Entity [redacted] as of July 7, 2017, the Entity was unable to provide the patching tool's remediation history reports for the June 2017 patching cycle. As a result, Texas RE is unable to determine the number of patches that were not timely evaluated and applied from March 14, 2017, through July 7, 2017. In addition, between July 12, 2016, and March 14, 2017, the Entity created [redacted] mitigation plans that did not include the Entity's planned actions to mitigate the vulnerabilities addressed by each security patch. This instance of noncompliance ended on July 10, 2017, when the Entity documented the completion of the final noncompliant mitigation plan. The root cause of this issue is that the Entity did not have a sufficient process for compliance with CIP-007-6 R2 when that Requirement became effective. The Entity lacked controls to ensure that the Entity's personnel devoted sufficient resources to implementing the Entity's patching process and to ensure that the Entity's Cyber Assets were patched as required. In addition, during the noncompliance, the Entity used [redacted] The duration of the noncompliance was approximately 12 months, from July 12, 2016 to July 10, 2017.
Risk Assessment	This issue posed a moderate risk and did not pose a serious or substantial risk to the bulk power system (BPS). The Entity's failure to evaluate and apply patches in a timely manner could have exposed the Entity's BES Cyber Systems to cyber security vulnerabilities such as the introduction of malicious code. This issue posed a moderate risk because of the scope and duration of the noncompliance. In particular, the scope of this issue included at least [redacted] patches that were not timely evaluated and [redacted] patches that were not timely applied. Furthermore, this issue affected all of the Entity's [redacted] Cyber Assets that are associated with the Entity's [redacted]. During the Compliance Audit, the Entity reported that it has [redacted] Cyber Assets, comprising [redacted] BES Cyber Assets, two Electronic Access Control or Monitoring Systems, [redacted] Physical Access Control Systems, and [redacted] Protected Cyber Assets. Finally, the duration of the issue increased the risk posed to the BPS. The duration of the failure to timely evaluate and apply patches was approximately 11 months, from August 17, 2016 to July 7, 2017, which included an approximately 4-month period when the Entity did not evaluate or apply any security patches. The Entity's noncompliant mitigation plans were effective for approximately 12 months, from July 12, 2016 to July 10, 2017. However, the risk to the reliability of the BPS was reduced because of the following factors. First, the Entity had other controls in place for the Cyber Assets at issue, including [redacted] During the audit period, the Entity did not detect any malicious code. Second, the Entity [redacted] In particular, the Entity [redacted], and is [redacted]. During normal operations, the Entity's [redacted] No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) evaluated and applied all applicable patches to the affected Cyber Assets; 2) documented the completion of the final noncompliant mitigation plan; 3) assigned and trained different personnel to implement the Entity's patching process; 4) [redacted]; 5) adopted revised procedure documents addressing the new control and including more specific work instructions for the Entity's patching process; and 6) revised its form and process document used for compliance with CIP-007-6 R2, Part 2.3 to include template language addressing the Entity's planned actions to mitigate the vulnerabilities addressed by each security patch. Texas RE has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017017683	CIP-007-3a	R5; R5.3.3	[redacted] (the "Entity")	[redacted]	08/05/2011	03/08/2019	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On [redacted], the Entity submitted a Self-Log stating that, as a [redacted] it was in noncompliance with CIP-007-6 R5. Specifically, the Entity failed to enforce an obligation to change passwords at least once every 15 calendar months with respect to two passwords. After conducting further review, the Entity determined that this issue included at least of 39 passwords dating back to August 5, 2011. Accordingly, this issue began, as an instance of noncompliance regarding CIP-007-3a R5 was effective and continued after CIP-007-6 R5 became effective. After subsequent review, Texas RE determined that the instances of noncompliance posed a moderate risk to the reliability of the bulk power system. As a result, Texas RE removed this issue from the Entity's self-log. The Entity discovered the issue while performing an internal spot check during November 2016. The Entity confirmed that the last password at issue either was changed or was associated with a deleted account as of March 8, 2019. The root cause of this issue is that the Entity did not have a sufficient process to review and identify passwords that are close to expiring. During the noncompliance, the Entity's process relied on personnel manually reviewing a spreadsheet to identify passwords that must be changed and then creating a task in the Entity's task management software to direct account owners to set new passwords. However, there was a flaw in the filtering formula used in the spreadsheet to highlight passwords that were close to expiring, which resulted in a failure to identify passwords that required remediation. The Entity also described an instance in which personnel identified a password that was expiring but failed to create a task in the Entity's task management software to timely remediate the issue. The Entity has addressed these issues by adopting revised procedure documents that include filtering criteria to identify passwords that will expire and a checklist to ensure remediation tasks are properly tracked. This noncompliance started on August 5, 2011, when the Entity failed to time change an applicable password, and ended on March 8, 2019, when the Entity remediated all expired passwords that were identified.
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 ensure passwords were timely changed could allow unauthorized individuals to have inappropriate access to BES Cyber Systems. The scope of this noncompliance included at least [redacted] associated with [redacted] that include [redacted]. In total, this issue affected [redacted]. In addition, the duration of the noncompliance lasted over seven years, from August 5, 2011 to March 8, 2019. However, the risk posed by this issue was also mitigated by the following factors. First, the BES Cyber Systems at issue were subject to other physical and electronic access controls, including residing in a Physical Security Perimeter and Electronic Security Perimeter. Further, this issue affected less than 1% of the passwords managed pursuant to the Entity's process pursuant to CIP-007-6 R5. No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) conducted reviews of password ages and remediated all expired passwords that were identified; 2) adopted a revised procedure document that includes filtering criteria to identify passwords that will expire, a new checklist to use when conducting reviews, and a standardized format for documenting reviews; and 3) conducted training regarding the revised process. Texas RE has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018020155	CIP-004-6	R4; P4.1.3, 4.2	[redacted] (the "Entity")	[redacted]	11/01/2016	01/22/2019	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On [redacted], the Entity submitted a Self-Report to Texas RE stating that, as a [redacted], it was in noncompliance with CIP-004-6 R4. Specifically, the Entity identified [redacted] with access to [redacted] that were not included in the quarterly or annual access reviews pursuant to CIP-004-6 R4, Part 4.2. The Entity discovered this issue [redacted]. Subsequently, during a Compliance Audit conducted from [redacted] Texas RE identified an instance of noncompliance regarding CIP-004-6 R4. Specifically, the Compliance Audit determined that the Entity did not have evidence of authorization records regarding [redacted] individuals with access to [redacted] designated storage locations for BES Cyber System Information (BCSI), as required by Part 4.1.3. Regarding the issue identified in the Self-Report, the Entity stated that [redacted]. As a result, the Entity had not included passwords for that user group in its quarterly electronic access reviews. In addition, the Compliance Audit identified another instance of noncompliance, noting that, for the third quarter of 2017, the Entity did not have evidence that it performed the quarterly review of authorization records for individuals with unescorted physical access. The Entity stated that it was unable to locate the documentation for that particular quarterly physical access review. Texas RE determined that the root cause of the Entity's noncompliance regarding Part 4.2 was an insufficient process to conduct quarterly access reviews and to maintain evidence of each review. The Entity's noncompliance regarding Part 4.2 began on November 1, 2016, which is the first day following the initial performance deadline for CIP-004-6 R4, Part 4.2. To end the noncompliance regarding Part 4.2, the Entity u[redacted] at issue, which was completed on July 18, 2018. Regarding the Entity's failure to provide evidence of certain authorization records for [redacted] individuals with access to certain BCSI storage locations, the Entity stated that there was a different root cause for each of the [redacted] individuals' access permissions. Regarding one individual, the root cause was an inadequate process for ensuring that access permissions in the Entity's document management software were correctly configured after a change was applied to the document management software. Specifically, when the Entity [redacted]. Regarding the other individual, the Entity stated that that the employee responsible for managing the BCSI storage locations added access permissions for the individual at issue without completing necessary access request documentation. To end the noncompliance, on January 22, 2019, the Entity reviewed access permissions for BCSI storage locations for the working group that includes the [redacted] individuals identified by the Compliance Audit and either removed or confirmed the [redacted] individuals' access to the [redacted] BCSI storage locations at issue. This noncompliance started on November 1, 2016, which is the first day after the deadline for the initial performance of a quarterly access review pursuant to CIP-004-6 R4, Part 4.2, and ended on January 22, 2019, when the Entity reviewed the access permissions for BCSI storage locations pursuant to CIP-004-6 R4, Part 4.1.3 for the working group that includes the [redacted] individuals identified by the Compliance Audit.
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 review authorized access as required could allow unauthorized individuals to have inappropriate physical or electronic access to BES Cyber Systems or BCSI. The noncompliance regarding CIP-004-6 R4, Part 4.2 included [redacted], which are classified as BES Cyber Assets and are associated a single [redacted] BES Cyber System that includes [redacted] control centers. In addition, the noncompliance regarding Part 4.1.3 included [redacted] employees with access to [redacted] BCSI storage locations. However, the risk posed by this issue was also mitigated by the following factors. First, the BES Cyber Assets at issue were subject to other protective controls, including residing in a Physical Security Perimeter. According to the Entity, individuals with access to the BES Cyber Assets at issue have completed required cyber security training and personnel risk assessments. No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) performed a quarterly electronic access review that included the workstations at issue [redacted]; 2) reviewed the access permissions for BCSI storage locations for the working group that includes the [redacted] individuals identified by the Compliance Audit and either removed or confirmed the [redacted] individuals' access to the [redacted] BCSI storage locations at issue; 3) revised its process for quarterly access reviews to use the Entity's [redacted]; and 4) implemented a change in the software for managing the BCSI storage locations at issue in order to [redacted]. Texas RE has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018020695	CIP-006-6	R1.3	[redacted] (the "Entity")	[redacted]	07/01/2016	10/31/2018	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			[redacted] Texas RE determined that the Entity, as a [redacted] had a potential noncompliance with CIP-006-6 R1.3. The Entity did not utilize [redacted] to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access. Specifically, to enter the Entity's Physical Security Perimeters (PSP) associated with [redacted] Access to the building where the PSP is located [redacted]. The Entity considered the use of [redacted] to meet the requirement of utilizing [redacted]. To enter the Entity's [redacted] However, the [redacted] The security personnel at the security desk are employed by the building owners and do not have access to [redacted] documentation, such as lists of personnel that are allowed to enter the [redacted]. As such, the [redacted] To remediate this noncompliance the Entity [redacted] The root cause of this noncompliance is a misunderstanding of CIP-006-6 R1.3. The Entity correctly identified that CIP-006-6 R1.3 was applicable to their environment. The Entity did not interpret [redacted] to mean that the types of access controls must be different. As such, the Entity [redacted]				
Risk Assessment			This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk arises from the potential for unauthorized individuals gaining access to [redacted] This can result in [redacted], which could lead [redacted]. The risk posed by this noncompliance is mitigated due to the following: 1) To gain access to the [redacted] an [redacted], [redacted]. a. [redacted]; and b. [redacted]; and c. [redacted]. 2) Only individuals with a need to access PSPs were given [redacted]. No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.				
Mitigation			To mitigate this noncompliance, the Entity: 1) [redacted]. Texas RE has verified the completion of all mitigation activity.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019766	CIP-005-5	R1.3	[redacted] (the "Entity")	[redacted]	07/01/2016	[redacted]	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On May 25, 2018, the Entity submitted a Self-Report stating that, as a [redacted]), it was in noncompliance with CIP-005-5 R1.3. According to the Entity, it failed to require inbound and outbound access permissions for all applicable [redacted]. Additionally, [redacted] Texas RE determined that the Entity, as a [redacted] had an additional finding of noncompliance with CIP-005-5 R1.3. The [redacted] discovered the Entity's [redacted]. This noncompliance started on July 1, 2016, when CIP-005-5 R1.3 became enforceable and ended on [redacted], when ownership [redacted] The root cause of this noncompliance was insufficient oversight and a lack of review of in-scope 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. Specifically, the failure to perform access control of traffic to and from substation ESPs has the potential to affect the reliability of the BPS by providing the opportunity for undetected compromise of BES Cyber Systems to occur, which could lead to misoperation or instability. Additionally, maintaining unjustified firewall access permissions has the potential to affect the reliability of the BPS by providing the opportunity for undetected compromise of Bulk Electric System (BES) Cyber Systems to occur, which could lead to misoperation or instability. The risks posed by these instances of noncompliance were mitigated by the following factors: 1) For the noncompliance related to the failure to implement inbound and outbound access permissions, the affected BES Cyber Systems were [redacted] where access to the [redacted] from [redacted] of the Entity's [redacted]. 2) For the noncompliance related to the failure to document the reasons for granting access for inbound and outbound access permissions, gaining access to the BES Cyber Systems from [redacted] No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) Added outbound access permissions [redacted]; 2) Added outbound access permissions [redacted]; 3) Removed [redacted] from the [redacted]; 4) Added justifications for required firewall rules on the [redacted]; 5) Removed unnecessary firewall rules from the [redacted]; and 6) Added justifications for required firewall rules on the [redacted].

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019767	CIP-005-5	R2.1; R2.2	[redacted] (the "Entity")	[redacted]	07/01/2016	04/30/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On May 25, 2018, the Entity submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-005-5 R2.1. According to the Entity, it failed to utilize an [redacted] does not directly access an applicable Cyber Asset in accordance with CIP-005-5 R2, Part 2.1. Additionally, the Entity stated that it did not utilize encryption that terminates at an Intermediate System as required by CIP-005-5 R2, Part 2.2. Specifically, the Entity's [redacted] The Entity discovered this noncompliance after hiring a third-party consultant to perform an independent review of the Entity's state of compliance. This noncompliance started on July 1, 2016, when CIP-005-5 R2.1 and R2.2 became enforceable and ended on April 30, 2018, when the Entity implemented an Intermediate System. The root cause of this issue was a misunderstanding of requirements CIP-005-5 R2.1. The Entity believed that requiring users to authenticate to a separate device, such as a firewall, would satisfy the Intermediate System requirement in CIP-005-5 R2.1. CIP-005-5 R2.2 requires that an entity utilize encryption that terminates at an Intermediate System. As the Entity was not using an Intermediate System, the Entity was unable to demonstrate compliance with this requirement.
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. [redacted] increases the risk that BES Cyber Assets could be compromised and either rendered inoperable or used for unauthorized interactive access to other systems, which could lead to misoperation or instability. The risk of this noncompliance is mitigated due to the following: 1) Prior to accessing BES Cyber Assets [redacted]. No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) [redacted]; and 2) Added an Intermediate System and required its use to access BES Cyber Assets.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019768	CIP-007-6	R2.1; R2.2; R2.3	[redacted] (the "Entity")	[redacted]	07/01/2016	04/18/2019	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On May 25, 2018, the Entity submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-007-6 R2.1. According to the Entity, it failed to have a patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. In particular, the Entity stated that patches for all third-party applications [redacted]. Additionally, [redacted], Texas RE determined that the Entity had additional instances of noncompliance with CIP-007-6 R2.1, and was also in noncompliance with CIP-007-6 R2.2 and CIP-007-6 R2.3. For CIP-007-6 R2.3 Texas RE determined that the Entity's dated mitigation plans did not include the Entity's planned actions to mitigate the vulnerabilities addressed by each security patch. This noncompliance started on July 1, 2016, when CIP-007-6 R2 became enforceable, and ended on April 18, 2019. The root cause of this noncompliance was a failure to follow and enforce the Entity's patch management procedure.
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. For CIP-007-6 R2.1, failure to track the patch sources for installed software can result in an entity being unaware that security fixes are available for installed software. This can lead to known vulnerabilities being exploited, creating conditions where BES Cyber Assets or EACMSs can be rendered unavailable, degraded, or misused. For CIP-007-6 R2.2, failure to evaluate security patches at least once every 35-calendar days can result in known vulnerabilities remaining available for exploit, creating conditions where BES Cyber Assets or EACMS can be rendered unavailable, degraded, or misused. For CIP-007-6 R2.3, failure to install applicable security patches results in known vulnerabilities remaining available for exploit, creating conditions where BES Cyber Assets or EACMS can be rendered unavailable, degraded, or misused. Similarly, a failure to create a dated mitigation plan that includes the Entity's planned actions to mitigate the vulnerabilities addressed by each security patch also results in known vulnerabilities remaining available for exploit. The risk posed by this noncompliance is mitigated due to the following: 1) The Entity [redacted]; and 2) For CIP-007-6 R2.2, [redacted]. No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) Removed unneeded applications and documented its patch sources for remaining applications; 2) For certain applications the Entity began evaluating security patches for applicability and for other applications the Entity has acquired the services of a third-party vendor to evaluate security patches; 3) [redacted]; and 4) [redacted]rabilities.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018019769	CIP-010-2	R2	[redacted] (the "Entity")	[redacted]	08/06/2016	[redacted]	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On May 25, 2018, the Entity submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-010-2 R2.1. Specifically, the Entity did not monitor at least once every 35-calendar days for changes to the baseline configuration for the applicable systems in CIP-010-2 R2.1. This noncompliance started on August 6, 2016, which is the first day after CIP-010-2 R2.1 became enforceable, and ended on [redacted], when the Entity [redacted] The root cause of this noncompliance is a failure to ensure that documented procedures are written in a manner to ensure that the evidence produced meets the evidentiary requirements of the CIP Standards. The Entity has a documented procedure to perform a scan of the Entity's BES Cyber Systems, [redacted] at intervals not to exceed 35-calendar days. The Entity has a separate procedure document that details the specific plugins that will be used by the scanner. Scans conducted prior to April 2018 do not contain baseline related information such as installed software or installed security patches. Information was given about security vulnerabilities present in installed or running software, but the scans could not be used to detect newly installed software for which no known security vulnerabilities existed, nor could they be used to detect the installation of new security patches for which a vulnerability was not previously detected. Scans conducted after April 2018 do not contain baseline related information such as installed security patches applicable specifically to the Windows operating system, and as such the scans cannot be used to detect the installation of new security 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 risk in not monitoring for unauthorized changes is this can allow an attacker or other unauthorized individual to make unauthorized changes to Cyber Assets that are not detected and subsequently left in place. These unauthorized changes could potentially lead to compromise of one or more devices and ultimately have a negative impact on the bulk power system. The risk posed by this noncompliance is mitigated due to the following: 1) The Entity was performing monthly vulnerability scans that gave the Entity information such as open ports, running services, and available patches to resolve security vulnerabilities. No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) The Entity [redacted], as such [redacted] Therefore, the Entity does not [redacted] that are required to be compliant with CIP-004 through CIP-011. Texas RE has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018020690	CIP-010-2	R1.1; R1.2; R1.3; R1.4; R1.5	[redacted] (the "Entity")	[redacted]	07/1/2016	[redacted]	Compliance Audit	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			During a [redacted] Texas RE determined that the Entity, as a [redacted] was in noncompliance with CIP-010-2, sub-requirements R1.1, R1.2, R1.3, R1.4, and R1.5. Specifically, for R1.1 the Entity was unable to provide evidence of complete baseline configuration documentation on or before July 1, 2016. In addition, for R1.2 the Entity was unable to provide evidence of authorizing the changes. Moreover, for R1.3 the Entity was unable to provide evidence of updating baseline configurations within 30 calendar days of completing changes. Also for R1.4, the Entity was unable to provide documentation of the results of the verification that the cyber security controls identified in R1.4.1 were not adversely affected. The Entity was unable to provide evidence that it had documented the results of the testing conducted in CIP-010-2 R1.5.1. This noncompliance started on July 1, 2016, when CIP-010-2 R1 became enforceable and ended on [redacted] when [redacted]. The root cause of this noncompliance was a failure to follow established procedures and a lack of sufficient oversight to discover and correct deficiencies.				
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 risk associated with the failure to maintain a complete configuration baseline has the potential to affect the reliability of the BPS by providing an opportunity for unauthorized and undetected modifications to be made to applicable Bulk Electric System (BES) Cyber Systems, which could introduce system instability or affect the functionality of such systems. The risk associated with the failure to authorize and document changes that deviate from the existing baseline configuration is this could allow for unmonitored, unapproved, or untested changes that could harm the BPS. The risk associated with the failure to update baseline configuration changes within thirty calendar days is this can allow an attacker to make unauthorized changes to the Cyber Assets that can subsequently go unnoticed. The risk associated with a failure to document the results of the verification that cyber security controls were unaffected by a change is this can lead to a situation where changes that do adversely affect the cyber security controls of a Cyber Asset are left undocumented and are not corrected. The risk associated with a failure to document the results of the pre-implementation testing of CIP-005 and CIP-007 cyber security controls is this can result in implementing changes in a production environment that will adversely impact the Entity's existing CIP-005 and CIP-007 cyber security controls. The risks posed by these instances of noncompliance are mitigated due to the following: 1) The Entity was performing [redacted]. No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.				
Mitigation			To mitigate this noncompliance, the Entity: 1) For R1.1 the [redacted] 2) For R1.2 the Entity reversed the unauthorized changes; 3) For R1.3 the Entity updated the baselines for devices which experienced a baseline change; 4) For R1.4 the Entity performed post-implementation verification of the cyber security controls for the affected cyber assets; and 5) For R1.5 the Entity performed post-implementation verification of the cyber security controls for the affected cyber assets.				

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2018020694	CIP-007-6	R1.1	[redacted] (the "Entity")	[redacted]	07/01/2016	02/27/2019	Compliance Audit	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	During a [redacted] Texas RE determined that the Entity, as a [redacted] was in noncompliance with CIP-007-6 R1. In particular, for the sampled Cyber Assets the Entity was unable to demonstrate that it had determined all enabled network accessible ports were needed. This noncompliance started on July 1, 2016, when CIP-007-6 R1.1 became enforceable and ended on February 27, 2019, when the Entity documented evidence of its determination that the logical network accessible ports were needed. The root cause of this noncompliance was a misunderstanding of the requirement around the determination of need. The Entity documented the network ports that were enabled and logically accessible on their applicable Cyber Assets. The Entity would then attempt to determine the process that was causing the network port to be enabled and logically accessible. If the Entity were able to determine the process that was causing the port to be enabled and logically accessible then the Entity would document this process as the justification for why the enabled logically accessible port was needed. If the Entity was unable to determine the process that was causing the port to be enabled and logically accessible then the Entity would [redacted] its justification for why an enabled logically accessible network port was needed.
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. Failure to document the determination of need for enabled logically accessible network ports can result in unneeded ports being left enabled and logically accessible. These network ports may act as an attack vector, which can subsequently lead to the compromise of a BES Cyber System and a negative impact on the bulk power system. The risk posed by this noncompliance is mitigated due to the following: 1) The network ports for which the Entity had not documented its determination of need was subsequently determined to be needed and left enabled. No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) Documented its determination of why logical network accessible ports were needed. Texas RE has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2019020901	CIP-004-6	R5	[redacted]	[redacted]	10/6/2018	10/12/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On January 3, 2019, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-004-6 R5. Specifically, a contract employee resigned from the entity on Friday, October 5, 2018. The staffing company notified the entity after 5 pm on that same day, which was a holiday weekend, and staffing was limited. As a result, removal of the contract employee's ability for unescorted physical access and Interactive Remote Access (IRA) was not initiated and completed until October 12, 2018, seven days later. The contract employee had unescorted physical and IRA access to High Impact Bulk Electric System (BES) Cyber Systems (HIBCS) located within the primary Control Center. The duration of the noncompliance was extended while an entity manager investigated options for retaining the terminated contract employee. The root cause of this violation was no established process to respond timely to termination notices received from staffing companies outside of normal business hours. After reviewing all relevant information, WECC Enforcement determined the entity failed to initiate and complete unescorted physical and IRA access removals within 24 hours of a termination action, as required by CIP-004-6 R5 Part 5.1. This violation began on October 6, 2018 when access removals should have been initiated and ended on October 12, 2018 when access removals were completed, for a total of seven days of noncompliance.
Risk Assessment	WECC determined this issue posed a moderate risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to initiate and complete unescorted physical and IRA access removals within 24 hours of a termination action, as required by CIP-004-6 R5 Part 5.1. The IRA access included local administrator privileges to system servers and high privilege/unrestricted access to modify or control the Automatic Generation Control development platform. The entity had implemented strong preventive controls for termination notifications in its Master Contract for service providers that were followed by the staffing company. However, the entity's own processes were lacking controls to prevent the noncompliance from occurring during non-business hours. As compensation, the entity tried to retain the contract employee as an entity employee, which lends to the character and trust of the contract employee. The individual had also completed CIP training and had a current Personnel Risk Assessment. The termination was voluntary, and the contract employee made no attempts to gain access after the termination date. No harm is known to have occurred.
Mitigation	To remediate and mitigate this violation, the entity has: 1) completed the access removals for the contract employee in scope; 2) implemented a coverage process for separation notifications that are received outside of the entity's normal business hours which includes having the contractor staffing companies notify the entity by phone if there is a termination action; and 3) communicated the process to all contractor staffing companies. WECC considered the entity's compliance history in its designation of this remediated issue as an FFT. The entity's relevant compliance history with CIP-004-6 R5 includes NERC Violation IDs: [redacted]. WECC determined that [redacted] compliance history should not serve as a basis for applying a penalty as the root cause and fact patterns of this instance is separate and distinct from the entity's prior CIP-004-6 R5 noncompliance.

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 Find, Fix, Track, and Reports 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	MRO2018020274	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
2	RFC2017018843	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 years
3	RFC2017018844	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 years
4	RFC2017018845	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 years
5	RFC2017018846	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 years
6	SERC2017017593			Yes										Category 2 – 12: 2 year
7	WECC2018019138	YES	YES	YES	YES						YES			Category 1: 3 years; Category 2 – 12: 2 year
8	WECC2018019143	YES	YES	YES	YES						YES			Category 1: 3 years; Category 2 – 12: 2 year
9	WECC2018019146	YES	YES	YES	YES						YES			Category 1: 3 years; Category 2 – 12: 2 year
10	WECC2018019149	YES	YES	YES	YES						YES			Category 1: 3 years; Category 2 – 12: 2 year
11	WECC2018019151	YES	YES	YES	YES						YES			Category 1: 3 years; Category 2 – 12: 2 year
12	WECC2017017460	YES		YES	YES						YES	YES	YES	Category 1: 3 years; Category 2 – 12: 2 year

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018020274	CIP-007-6	R3	[redacted] (the Entity)	[redacted]	7/1/2016	8/22/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On June 5, 2018, the Entity submitted a Self-Report stating that as a [redacted], it was in noncompliance with CIP-007-6 R3. The Entity [redacted] The Entity reported that it did not have a process in place for updating the signatures or patterns used by its malicious code prevention method as required by P3.3. The cause of the noncompliance is that the Entity's documented process lacked sufficient detail about updating the signatures of patterns, including who is responsible for performing the update, how the updates will be received, and details for performing and documenting the testing of the updates. The noncompliance began on July 1, 2016, when the Requirement became enforceable, and ended on August 22, 2018, when the signatures or patterns were updated.
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 noncompliance was not minimal because the duration of the noncompliance represents a significant delay which exposed the Entity to evolving malicious code threats. However, the noncompliance was not serious or substantial as the antivirus agent and management console was detecting code based on the last received signatures or patterns during the period of noncompliance. Further, the Entity reports that it has [redacted], and other network protections in place that reduced the risk of the outdated signatures or patterns. Finally, the Entity's [redacted] No harm is known to have occurred. The Entity has no relevant history of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) updated the signatures or patterns used by its malicious code prevention method; 2) updated its process and procedures for updating the signatures or patterns; and 3) provided training to personnel on these changes. MRO has verified the completion of all mitigation activity.

ReliabilityFirst Corporation (ReliabilityFirst) 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
RFC2017018843	CIP-007-6	R4	[redacted]	[redacted]	6/1/2017	1/24/2018	Self-Report	Completed

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

On December 7, 2017, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R4. As part of compliance review activities, on August 31, 2017, the entity discovered that [redacted] in the [redacted] were not reporting failed/successful login events to the [redacted] These devices are separated into 3 groups according to the specific issues involved.

The first group consists of [redacted] connected to the [redacted] located at one entity data center and include [redacted]. On June 1, 2017, this group of devices stopped sending security events to the [redacted] due to a hung process. On September 6, 2017, the entity rebooted the [redacted] to clear the hung process, which restored [redacted]. However, the reboot did not correct the issue for the [redacted]. The issue with the [redacted] was corrected when the entity [redacted] on January 24, 2018. (In the interim time period, the entity ensured that [redacted].)

The second group consists of [redacted]. For the [redacted], beginning on June 1, 2017, a corrupted file prevented the capture of events. This corrupted file was deleted and replaced on September 7, 2017, which corrected the issue with the [redacted]. The [redacted] were configured for object access logging, which resulted in a high number of expected security events (including both successful and failed object access). Due to the high number of events, the devices were [redacted] The issue with the [redacted] was corrected when the entity [redacted] on January 24, 2018. (In the interim time period, the entity ensured that [redacted].)

The third group consists of [redacted] located in 3 entity data centers. For this group of devices, beginning on June 1, 2017, events were not captured due to a configuration error. Specifically, [redacted], which was not initially considered at installation and was not explicitly detailed in the associated job aids. The entity corrected the issue on September 7, 2017, by [redacted].

The root causes of this noncompliance generally related to equipment difficulty such as a hung process, corrupted files, and case syntaxes. These root causes involve the management practice of asset and configuration management, which includes defining asset and configuration item attributes.

This noncompliance started on June 1, 2017, the first date on which a device was not forwarding events properly and ended on January 24, 2018, when the entity made corrections to address the issues with the first and second group of devices.

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 potential risk associated with the failure of automated logging of successful/unsuccessful login attempts is that it would impede the entity's ability to identify and respond to a cyber attack in real-time and to conduct after-the-fact investigations of those types of situations. This risk is not minimal in this case due to the real-time nature of the issue as well as the duration (i.e., approximately 7 months). However, this risk is not serious and substantial based on the following mitigating factors. First, the affected devices are all Electronic Access Control and Monitoring Systems (EACMS), which are located at data center and do not directly control the BPS. Second, although [redacted] was not automatically receiving logs, the impacted devices were still [redacted]. Therefore, in the event of a security incident, the entity could have [redacted]. ReliabilityFirst also notes that during the time frame of this issue, the entity did not experience any security incidents. 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 arose from different causes.

Mitigation

To mitigate this noncompliance, the entity:

1) rebooted the [redacted] to eliminate the error per [redacted] recommendation;
2) replaced the corrupt file;
3) corrected [redacted];
4) issued an awareness bulletin. The entity reinforced the need to leverage the [redacted] job aid when installing [redacted] on devices reporting to the [redacted];
5) upgraded [redacted]
6) upgraded [redacted]
7) updated Job Aid: [redacted] to state that device [redacted] within the [redacted] and communicated the update to [redacted]
8) ran Software Inventory Report showing [redacted] before the upgrade, and after the upgrade to confirm upgrade is complete. [redacted] report showing [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
RFC2017018843	CIP-007-6	R4	[redacted]	[redacted]	6/1/2017	1/24/2018	Self-Report	Completed
			9) configured a subscription report for [redacted] for devices reporting to [redacted] 10) updated the existing [redacted] Job Aid to include the review of the [redacted] report mentioned in corrective Milestone 9; 11) communicated and implemented new procedures resulting from the [redacted] Job Aid with the [redacted]; and 12) updated process document documenting the specific events to be collected in addition to those required by the standard. ReliabilityFirst has verified the completion of all mitigation activity.					

ReliabilityFirst Corporation (ReliabilityFirst) 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
RFC2017018844	CIP-007-6	R4	[redacted]	[redacted]	6/1/2017	1/24/2018	Self-Report	Completed

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

On December 7, 2017, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R4. As part of compliance review activities, on August 31, 2017, the entity discovered that [redacted] in the [redacted] were not reporting failed/successful login events to the [redacted]. These devices are separated into 3 groups according to the specific issues involved.

The first group consists of [redacted] connected to the [redacted] located at one entity data center and include [redacted]. On June 1, 2017, this group of devices stopped sending security events to the [redacted] due to a hung process. On September 6, 2017, the entity rebooted the [redacted] to clear the hung process, which restored [redacted]. However, the reboot did not correct the issue for the [redacted]. The issue with the [redacted] was corrected when the entity [redacted] on January 24, 2018. (In the interim time period, the entity ensured that [redacted]

The second group consists of [redacted]. For the [redacted], beginning on June 1, 2017, a corrupted file prevented the capture of events. This corrupted file was deleted and replaced on September 7, 2017, which corrected the issue with the [redacted]. The [redacted] were configured for object access logging, which resulted in a high number of expected security events (including both successful and failed object access). Due to the high number of events, the devices were [redacted]. The issue with the [redacted] was corrected when the entity [redacted] on January 24, 2018. (In the interim time period, the entity ensured that [redacted].)

The third group consists of [redacted] located in 3 entity data centers. For this group of devices, beginning on June 1, 2017, events were not captured due to a configuration error. Specifically, [redacted], which was not initially considered at installation and was not explicitly detailed in the associated job aids. The entity corrected the issue on September 7, 2017, by [redacted].

The root causes of this noncompliance generally related to equipment difficulty such as a hung process, corrupted files, and case syntaxes. These root causes involve the management practice of asset and configuration management, which includes defining asset and configuration item attributes.

This noncompliance started on June 1, 2017, the first date on which a device was not forwarding events properly and ended on January 24, 2018, when the entity made corrections to address the issues with the first and second group of devices.

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 potential risk associated with the failure of automated logging of successful/unsuccessful login attempts is that it would impede the entity's ability to identify and respond to a cyber attack in real-time and to conduct after-the-fact investigations of those types of situations. This risk is not minimal in this case due to the real-time nature of the issue as well as the duration (i.e., approximately 7 months). However, this risk is not serious and substantial based on the following mitigating factors. First, the affected devices are all Electronic Access Control and Monitoring Systems (EACMS), which are located at data center and do not directly control the BPS. Second, although [redacted] was not automatically receiving logs, the impacted devices were still [redacted]. Therefore, in the event of a security incident, the entity could have [redacted]. ReliabilityFirst also notes that during the time frame of this issue, the entity did not experience any security incidents. 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 arose from different causes.

Mitigation

To mitigate this noncompliance, the entity:

1) rebooted the [redacted] to eliminate the error per [redacted] recommendation;
2) replaced the corrupt file;
3) corrected [redacted];
4) issued an awareness bulletin. The entity reinforced the need to leverage the [redacted] job aid when installing [redacted] on devices reporting to the [redacted]
5) upgraded [redacted]
6) upgraded [redacted]
7) updated Job Aid: [redacted] to state that device [redacted] within the [redacted] and communicated the update to [redacted];

ReliabilityFirst Corporation (ReliabilityFirst) 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
RFC2017018844	CIP-007-6	R4	[redacted]	[redacted]	6/1/2017	1/24/2018	Self-Report	Completed
			8) ran Software Inventory Report showing [redacted] before the upgrade, and after the upgrade to confirm upgrade is complete. [redacted] report showing [redacted]; 9) configured a subscription report for [redacted] for devices reporting to [redacted] 10) updated the existing [redacted] Job Aid to include the review of the [redacted] report mentioned in corrective Milestone 9; 11) communicated and implemented new procedures resulting from the [redacted] Job Aid with the [redacted]; and 12) updated process document documenting the specific events to be collected in addition to those events required by the standard. ReliabilityFirst has verified the completion of all mitigation activity.					

ReliabilityFirst Corporation (ReliabilityFirst) 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
RFC2017018845	CIP-007-6	R4	[redacted]	[redacted]	6/1/2017	1/24/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On December 7, 2017, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R4. As part of compliance review activities, on August 31, 2017, the entity discovered that [redacted] in the [redacted] were not reporting failed/successful login events to the [redacted]. These devices are separated into 3 groups according to the specific issues involved. The first group consists of [redacted] connected to the [redacted] located at one entity data center and include [redacted]. On June 1, 2017, this group of devices stopped sending security events to the [redacted] due to a hung process. On September 6, 2017, the entity rebooted the [redacted] to clear the hung process, which restored [redacted]. However, the reboot did not correct the issue for the [redacted]. The issue with the [redacted] was corrected when the entity [redacted] on January 24, 2018. (In the interim time period, the entity ensured that [redacted].) The second group consists of [redacted]. For the [redacted], beginning on June 1, 2017, a corrupted file prevented the capture of events. This corrupted file was deleted and replaced on September 7, 2017, which corrected the issue with the [redacted]. The [redacted] were configured for object access logging, which resulted in a high number of expected security events (including both successful and failed object access). Due to the high number of events, the devices were [redacted]. The issue with the [redacted] was corrected when the entity [redacted] on January 24, 2018. (In the interim time period, the entity ensured that [redacted].) The third group consists of [redacted] located in 3 entity data centers. For this group of devices, beginning on June 1, 2017, events were not captured due to a configuration error. Specifically, [redacted], which was not initially considered at installation and was not explicitly detailed in the associated job aids. The entity corrected the issue on September 7, 2017, by [redacted] The root causes of this noncompliance generally related to equipment difficulty such as a hung process, corrupted files, and case syntaxes. These root causes involve the management practice of asset and configuration management, which includes defining asset and configuration item attributes. This noncompliance started on June 1, 2017, the first date on which a device was not forwarding events properly and ended on January 24, 2018, when the entity made corrections to address the issues with the first and second group of devices.
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 potential risk associated with the failure of automated logging of successful/unsuccessful login attempts is that it would impede the entity's ability to identify and respond to a cyber attack in real-time and to conduct after-the-fact investigations of those types of situations. This risk is not minimal in this case due to the real-time nature of the issue as well as the duration (i.e., approximately 7 months). However, this risk is not serious and substantial based on the following mitigating factors. First, the affected devices are all Electronic Access Control and Monitoring Systems (EACMS), which are located at data center and do not directly control the BPS. Second, although [redacted] was not automatically [redacted] the impacted devices were still [redacted]. Therefore, in the event of a security incident, the entity could have reviewed the local logs manually. ReliabilityFirst also notes that during the time frame of this issue, the entity did not experience any security incidents. 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 arose from different causes.
Mitigation	To mitigate this noncompliance, the entity: 1) rebooted the [redacted] to eliminate the error per [redacted] recommendation; 2) replaced the corrupt file; 3) corrected [redacted]; 4) issued an awareness bulletin. The entity reinforced the need to leverage the [redacted] job aid when installing [redacted] on devices reporting to the [redacted]; 5) upgraded [redacted] 6) upgraded [redacted] 7) updated Job Aid: [redacted] to state that device [redacted] within the [redacted] and communicated the update to [redacted];

ReliabilityFirst Corporation (ReliabilityFirst) 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
RFC2017018845	CIP-007-6	R4	[redacted]	[redacted]	6/1/2017	1/24/2018	Self-Report	Completed
			8) ran Software Inventory Report showing [redacted] before the upgrade, and after the upgrade to confirm upgrade is complete. Ran [redacted] report showing [redacted]; 9) configured a subscription report for [redacted] devices reporting to [redacted] 10) updated the existing [redacted] Job Aid to include the review of the [redacted] report mentioned in corrective Milestone 9; 11) communicated and implemented new procedures resulting from the [redacted] Job Aid with the CIP operations team; and 12) updated process document documenting the specific events to be collected in addition to those events required by the standard. ReliabilityFirst has verified the completion of all mitigation activity.					

ReliabilityFirst Corporation (ReliabilityFirst) 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
RFC2017018846	CIP-007-6	R4	[redacted]	[redacted]	6/1/2017	1/24/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On December 8, 2017, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R4. As part of compliance review activities, on August 31, 2017, the entity discovered that [redacted] in the [redacted] were not reporting failed/successful login events to the [redacted]. These devices are separated into 3 groups according to the specific issues involved. The first group consists of [redacted] connected to the [redacted] located at one entity data center and include [redacted]. On June 1, 2017, this group of devices stopped sending security events to the [redacted] due to a hung process. On September 6, 2017, the entity rebooted the [redacted] to clear the hung process, which restored [redacted]. However, the reboot did not correct the issue for the [redacted]. The issue with the [redacted] was corrected when the entity [redacted] on January 24, 2018. (In the interim time period, the entity ensured that [redacted] The second group consists of [redacted] For the [redacted], beginning on June 1, 2017, a corrupted file prevented the capture of events. This corrupted file was deleted and replaced on September 7, 2017, which corrected the issue with the [redacted]. The [redacted] were configured for object access logging, which resulted in a high number of expected security events (including both successful and failed object access). Due to the high number of events, the devices were [redacted]. The issue with the [redacted] was corrected when the entity [redacted] on January 24, 2018. (In the interim time period, the entity ensured that [redacted] The third group consists of [redacted] located in 3 entity data centers. For this group of devices, beginning on June 1, 2017, events were not captured due to a configuration error. Specifically, [redacted] which was not initially considered at installation and was not explicitly detailed in the associated job aids. The entity corrected the issue on September 7, 2017, by [redacted] The root causes of this noncompliance generally related to equipment difficulty such as a hung process, corrupted files, and case syntaxes. These root causes involve the management practice of asset and configuration management, which includes defining asset and configuration item attributes. This noncompliance started on June 1, 2017, the first date on which a device was not forwarding events properly and ended on January 24, 2018, when the entity made corrections to address the issues with the first and second group of devices.
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 potential risk associated with the failure of automated logging of successful/unsuccessful login attempts is that it would impede the entity's ability to identify and respond to a cyber attack in real-time and to conduct after-the-fact investigations of those types of situations. This risk is not minimal in this case due to the real-time nature of the issue as well as the duration (i.e., approximately 7 months). However, this risk is not serious and substantial based on the following mitigating factors. First, the affected devices are all Electronic Access Control and Monitoring Systems (EACMS), which are located at data center and do not directly control the BPS. Second, although [redacted] was not automatically receiving logs, the impacted devices were still [redacted]. Therefore, in the event of a security incident, the entity could have [redacted]. ReliabilityFirst also notes that during the time frame of this issue, the entity did not experience any security incidents. 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 majority of the prior noncompliances arose from different causes.
Mitigation	To mitigate this noncompliance, the entity: 1) rebooted the [redacted] to eliminate the error per [redacted] recommendation; 2) replaced the corrupt file; 3) corrected [redacted]; 4) issued an awareness bulletin. The entity reinforced the need to leverage the [redacted] job aid when installing [redacted] on devices reporting to the [redacted]; 5) upgraded [redacted] 6) upgraded [redacted] 7) updated Job Aid: [redacted] to state that device [redacted] within the [redacted] and communicated the update to [redacted]

ReliabilityFirst Corporation (ReliabilityFirst) 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
RFC2017018846	CIP-007-6	R4	[redacted]	[redacted]	6/1/2017	1/24/2018	Self-Report	Completed
			8) ran Software Inventory Report showing [redacted] before the upgrade, and after the upgrade to confirm upgrade is complete. [redacted] report showing [redacted]; 9) configured a subscription report for [redacted] devices reporting to [redacted] 10) updated the existing [redacted] Job Aid to include the review of the [redacted] report mentioned in corrective Milestone 9; 11) communicated and implemented new procedures resulting from the [redacted] Job Aid with the [redacted]; and 12) updated process document documenting the specific events to be collected in addition to those events required by the standard. ReliabilityFirst has verified the completion of all mitigation activity.					

SERC Reliability Corporation (SERC) 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
SERC2017017593	CIP-007-3a	R5.2	[redacted]	[redacted]	05/05/2015	04/25/2017	Self-Report	Completed 06/29/2017

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On May 18, 2017, the Entity submitted a Self-Report stating that, as a [redacted] and [redacted] it was in noncompliance with CIP-007-3a R5.2. The Entity did not implement a policy to manage the scope and acceptable use of shared account privileges for 16 Physical Access Control System (PACS) accounts. Specifically, on December 8, 2016, during preparation of an upgrade to its (PACS), the Entity conducted a review of all default accounts and discovered that on May 5, 2015, it erroneously configured 16 shared system accounts to allow interactive user access on 16 PACS accounts on three PACS servers and six PACS workstations. The Entity thought these accounts were generic system (service) accounts without the capability of interactive user access. The Entity identified 13 users that were capable of accessing any of the PACS Cyber Assets, including the PACS production server, through any one of the 16 PACS accounts. The noncompliance started on May 5, 2015, when the Entity erroneously enabled user access to shared accounts, and ended on April 25, 2017, when the Entity disabled user access to shared accounts. The root cause of this violation was a procedural deficiency, specifically, the implementation of specific steps to identify interactive user access capabilities when implementing new system (service) accounts.
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 provisioning 16 shared system accounts to allow interactive user access, any one of the 13 individuals could have used such accounts by by-passing the two-factor authentication security control to access the PACS servers and/or workstations and powered down the servers and workstations and shut-down the PACS system. Additionally, these individuals could have modified the server settings and monitoring capabilities. However, these individuals did not have the ability to access the PACS application [redacted], which eliminated the potential for the individuals to create, modify, or delete Physical Security Perimeter (PSP) physical access controls. Had a loss of communications occurred between the PACS application server and PSP controller panels, the panels would have maintained a localized dataset of authorized personnel credentials and continued to control PSP access points. Additionally, a loss of communications would have generated communication failure alarms, which would have initiated recovery response processes in accordance with CIP-009. As a result, unauthorized access of a PACS server or monitoring workstation would likely have had minimal actual impact to the BES Cyber Assets, Electronic Access Control or Monitoring Systems, or Protected Cyber Assets contained within PSPs. In addition, the affected PACS Cyber Assets employed redundancy and had alarms that would have triggered in the event of any loss of monitoring. The 13 personnel provisioned with interactive user access were unaware of its existence and were employees in IT security. Eleven of the personnel completed all prerequisites for CIP access in other areas and systems. Moreover, the entity had electronic monitoring and alarming of PACS in place. No harm is known to have occurred. SERC considered the Entity's compliance history and determined that there are no prior relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) removed all interactive user access capability for the affected PACS service accounts; 2) revised its procedures to include process steps to identify and remove interactive user access capability when implementing new service accounts; and 3) trained applicable personnel on updates to its procedures.

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC) 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
WECC2018019138	CIP-004-6	R4	[redacted]	[redacted]	10/1/2016	5/11/2018	Compliance Audit	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	During a Compliance Audit conducted [redacted] WECC auditors determined the entity, as a [redacted] and [redacted] had a potential noncompliance with CIP-004-6 R4 Part 4.2 as it related to the entity's verification processes for its hard-key authorization. Specifically, the audit team determined that, although the entity had a process for how it authorized hard-keys used for accessing its Medium Impact BES Cyber System (MIBCS) Physical Security Perimeter (PSP) in its documented program, it was not verifying at least once each calendar quarter that individuals with active hard-keys for unescorted physical access to said PSP, had an authorization record because that was not part of its verification program. After reviewing all relevant information, WECC Enforcement agreed with the audit findings. Therefore, the entity failed to verify at least once each calendar quarter that individuals with unescorted physical access via the use of a hard-key had authorization records, as required by CIP-004-6 R4 Part 4.2. The root cause of this issue was a less than adequate procedure. Specifically, the entity did not include in its work flows reminders, a verification of authorization records to include individuals who had been issued unescorted physical access via hard-keys. The noncompliance began on October 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on May 11, 2018, when the entity verified individuals with hard-keys had authorization records, for a total of 588 days of noncompliance.
Risk Assessment	WECC determined this noncompliance posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to verify at least once each calendar quarter that individuals with unescorted physical access via use of a hard-key had authorization records, as required by CIP-004-6 R4 Part 4.2. However, as compensation, the number of individuals issued hard-keys was limited to four and those individuals also had authorized electronic access to the MIBCS and authorized unescorted physical access to the PSP. No harm is known to have occurred. The entity has no relevant previous violations of this or similar Standards and Requirements.
Mitigation	To mitigate this noncompliance, the entity: 1) verified individuals with hard-keys had authorization records; 2) re-keyed all PSP access points and PACS panels to ensure control of physical hard-keys access; 3) created and implemented a new [redacted], which is incorporated into the overall [redacted], to document a clear process to incorporate controls around the authorization, review, and revocation of hard-keys; 4) limited the number of staff that have access to physical hard-keys to authorized individuals, as defined the [redacted]; 5) updated its onboarding roles matrix to implement PSP physical hard-key access controls to comply with its [redacted]; 6) conducted an internal review and revisions to its [redacted] that focuses on functional activities and instructions performed to comply with CIP-004; 7) reviewed and updated its quarterly validation report to account for PSP physical hard-key access roles and assignments; and 8) updated appropriate users within its updated [redacted] with PSP physical hard-key access. WECC has verified the completion of all mitigation activity.

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC) 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
WECC2018019143	CIP-006-6	R1	[redacted]	[redacted]	7/1/2016	6/27/2018	Compliance Audit	Completed

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

During a Compliance Audit conducted [redacted] WECC auditors determined the entity, as a [redacted] and [redacted] had a potential noncompliance with CIP-006-6 R1.

Specifically, WECC found several issues with the entity's Physical Security Plan:

a. the entity distributed and utilized hard-keys to access two Physical Security Perimeters (PSPs) containing MIBCS. Seven keys were distributed to individuals; one key was located in a [redacted] and the remaining spare keys were secured in the [redacted] The Physical Security Plan lacked acceptable use instructions for the hard-keys and only contained a "for emergency use only" statement. No hard-key management, inventory, or log records were available. The entity's Physical Security Plan stated that physical access into each PSP access point was controlled by an ID Badge Physical Access Control System (PACS) and did not address the secondary hard-key access which was available, and at times used by the personnel with hard-keys (Part 1.2);

b. the entity's Physical Security Plan states that all PSP access points at the [redacted] were electronically monitored 24 hours a day, seven days a week. However, it was observed that several egress access points were constructed to only be monitored by a local crash bar sounder, and upon testing, one door failed to indicate an alarm condition when it was opened, and no alarm was displayed by the PACS. An additional egress door produced a local alarm in the crash bar but again, was not displayed to the dispatch operators. At the [redacted] an egress door was unmarked; had no local sounder; and was unmonitored by the PACS or the [redacted] dispatch operator (Part 1.4);

c. a review of evidence alarm logs showed that no recorded alarm events were ever acknowledged within 15 minutes of sounding. Operators have PACS viewing screens for PACS alarms events, however, alarm events were not monitored or assessed within 15 minutes and the only activity the [redacted] operators were doing was contacting facilities personnel to investigate alarms which was not occurring within 15 minutes of the alarm (Part 1.5);

d. the tamper alarm on the panel controlling access to the [redacted] PSP was generating alarms; however, the alarms were not being monitored (Part 1.6);

e. because the generated alarms on the access control panel to the [redacted] PSP was not being monitored, unauthorized access was not being detected and no response was being performed within 15 minutes of when the entity should have detected the unauthorized access. Additionally, the entity's Physical Security Plan did not mention the 15-minute time requirement when monitoring for unauthorized access (Part 1.7);

f. the entity was not able to provide information to identify individuals and date and time of entry into PSPs for individuals who utilized hard-keys. The PACS was only able to record a "door forced" alarm event when a hard-key was used. This was indistinguishable from any other cause for a forced door event and none of the log requirements were recorded in the PACS. Additionally, the entity was not monitoring alarm events in real time and did not provide any comments as a manual addendum, no details existed for logging access, authorized or not, with any method that did not involve an authorized ID badge (Part 1.8); and

g. the entity did not capture, electronically via the PACS or manually, any physical access log information when hard-keys were used. As such, no log files existed for at least 90 calendar days, or at all in some cases, to record entry of individuals with authorized unescorted physical access into each PSP when utilizing a hard-keys (Part 1.9).

After reviewing all relevant information, WECC Enforcement agreed with the audit findings. Therefore, the entity failed to adequately document and implement one or more physical security plan(s) that collectively included the applicable requirement parts of CIP-006-6 R1, that is, Parts 1.2, 1.4, 1.5, 1.6, 1.7, 1.8, and 1.9. Part 1.1 and Part 1.3 are not in scope of these violations.

The root cause of the noncompliance was less than adequate documentation. Specifically, the entity's Physical Security Plan was ineffective in ensuring compliance with the Standards and Requirements in that it was written in direct conflict with what was actually being performed by the personnel responsible for implementation of the Physical Security Plan.

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC) 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
WECC2018019143	CIP-006-6	R1	[redacted]	[redacted]	7/1/2016	6/27/2018	Compliance Audit	Completed

Risk Assessment	WECC determined this noncompliance posed a moderate risk and did not pose a serious and substantial risk to the reliability of the BPS. Specifically, the entity failed to adequately document and implement one or more physical security plan(s) that collectively included the applicable requirement parts of CIP-006-6 R1, that is, Parts 1.2, 1.4, 1.5, 1.6, 1.7, 1.8, and 1.9. Part 1.1 and Part 1.3 are not in scope of this noncompliance. However, the entity implemented good compensating controls in the form of System Security Management. Specifically, for the MIBCS, the entity locked down unneeded physical and logical ports; implemented malicious code prevention and detection; monitored security events; and ensured passwords were enforced and met length and complexity requirements. Though these controls would not prevent the noncompliance from occurring, they would reduce the likelihood of a malicious actor infiltrating and compromising the entity's Energy Management System (EMS). No harm is known to have occurred. The entity has no relevant previous violations of this or similar Standards and Requirements.
Mitigation	To mitigate this noncompliance, the entity: 1) re-keyed all PSP access points and PACS panels to ensure control of physical hard-keys access; 2) created and implemented a new Physical Hard-keys Procedure, which is incorporated into the overall Physical Security Plan, to document a clear process; 3) logged entry of each individual with physical hard-keys access into each PSP, with information to identify the individual and date and time of entry; 4) retained physical hard-keys access logs of entry of individuals with authorized unescorted physical access into each PSP for at least ninety calendar days; 5) incorporated controls around the storage, access, issuance, monitoring, and use of the hard-keys; 6) installed additional cameras and sensors to assist in monitoring, and to increase security and situational awareness of all PSP access points and PACS; 7) improved real time monitoring of PSP access points by transitioning the physical security monitoring role from its Power System Controllers to dedicated Security Guards staffed 24x7; 8) expanded the role of third party Security Guards to enforce controls, monitor PSP access points, to include applicable cameras, sensors and alarms, and document acknowledgement and responses to detected unauthorized access; 9) decreased the number of PACS to reduce the risks and potential points of failure, and updated PSP diagrams to reflect the changes; 10) increased the number of staff that support compliance and physical security responsibilities. The two employees (renamed as Safety and Security Specialists) in these positions will be Subject Matter Experts (SMEs) for CIP-006-6 and will be responsible for, among other things, training, implementation, controls and oversight associated with the Physical Hard-keys Procedure and processes for acknowledging and responding to alarms for detected unauthorized access; 11) developed and provided training to Security Guards to monitor physical access controls via PACS and security cameras; 12) developed and implemented a training program for Security Guards on event handling and escalation matrix; 13) provided physical security control system training to Power System Controllers; 14) trained CIP-006-6 SMEs on the updated Physical Security Procedure; 15) retained third party physical security consultants to evaluate and provide threat and vulnerability assessment of PSPs; 16) reconfigured and tested PACS software to confirm door alarms are audible; 17) confirmed that external facing hinges on access points, including the [redacted] emergency door, are hardened; 18) reduced timeframe of door-held-open results in alarm from 75 seconds to 30 seconds; 19) increased security awareness by posting signage and providing training for all employees; 20) implemented a periodic process for physical hard-keys inventory, as defined in the Physical Security Procedure; and 21) implemented a review process to validate acknowledgment of unauthorized access to PSPs and PACS was performed within 15 minutes and that appropriate compliance evidence exists, as defined in in the Physical Security Procedure. WECC has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019146	CIP-006-6	R1	[redacted]	[redacted]	7/1/2016	6/27/2018	Compliance Audit	Completed

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

During a Compliance Audit conducted [redacted] WECC auditors determined the entity, as a [redacted] and [redacted] had a potential noncompliance with CIP-006-6 R1.

Specifically, WECC found several issues with the entity's Physical Security Plan:

a. the entity distributed and utilized hard-keys to access two Physical Security Perimeters (PSPs) containing MIBCS. Seven keys were distributed to individuals; one key was located in a [redacted] ([redacted] dispatch area; and the remaining spare keys were secured in the [redacted] The Physical Security Plan lacked acceptable use instructions for the hard-keys and only contained a "for emergency use only" statement. No hard-key management, inventory, or log records were available. The entity's Physical Security Plan stated that physical access into each PSP access point was controlled by an ID Badge Physical Access Control System (PACS) and did not address the secondary hard-key access which was available, and at times used by the personnel with hard-keys (Part 1.2);

b. the entity's Physical Security Plan states that all PSP access points at the [redacted] were electronically monitored 24 hours a day, seven days a week. However, it was observed that several egress access points were constructed to only be monitored by a local crash bar sounder, and upon testing, one door failed to indicate an alarm condition when it was opened, and no alarm was displayed by the PACS. An additional egress door produced a local alarm in the crash bar but again, was not displayed to the dispatch operators. At the [redacted] an egress door was unmarked; had no local sounder; and was unmonitored by the PACS or the [redacted] dispatch operator (Part 1.4);

c. a review of evidence alarm logs showed that no recorded alarm events were ever acknowledged within 15 minutes of sounding. Operators have PACS viewing screens for PACS alarms events, however, alarm events were not monitored or assessed within 15 minutes and the only activity the [redacted] operators were doing was contacting facilities personnel to investigate alarms which was not occurring within 15 minutes of the alarm (Part 1.5);

d. the tamper alarm on the panel controlling access to the [redacted] PSP was generating alarms; however, the alarms were not being monitored (Part 1.6);

e. because the generated alarms on the access control panel to the [redacted] PSP was not being monitored, unauthorized access was not being detected and no response was being performed within 15 minutes of when the entity should have detected the unauthorized access. Additionally, the entity's Physical Security Plan did not mention the 15-minute time requirement when monitoring for unauthorized access (Part 1.7);

f. the entity was not able to provide information to identify individuals and date and time of entry into PSPs for individuals who utilized hard-keys. The PACS was only able to record a "door forced" alarm event when a hard-key was used. This was indistinguishable from any other cause for a forced door event and none of the log requirements were recorded in the PACS. Additionally, the entity was not monitoring alarm events in real time and did not provide any comments as a manual addendum, no details existed for logging access, authorized or not, with any method that did not involve an authorized ID badge (Part 1.8); and

g. the entity did not capture, electronically via the PACS or manually, any physical access log information when hard-keys were used. As such, no log files existed for at least 90 calendar days, or at all in some cases, to record entry of individuals with authorized unescorted physical access into each PSP when utilizing a hard-keys (Part 1.9).

After reviewing all relevant information, WECC Enforcement agreed with the audit findings. Therefore, the entity failed to adequately document and implement one or more physical security plan(s) that collectively included the applicable requirement parts of CIP-006-6 R1, that is, Parts 1.2, 1.4, 1.5, 1.6, 1.7, 1.8, and 1.9. Part 1.1 and Part 1.3 are not in scope of these violations.

The root cause of the noncompliance was less than adequate documentation. Specifically, the entity's Physical Security Plan was ineffective in ensuring compliance with the Standards and Requirements in that it was written in direct conflict with what was actually being performed by the personnel responsible for implementation of the Physical Security Plan.

The noncompliance began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on June 27, 2018, when the entity completed mitigating activities, for a total of 727 days of noncompliance.

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC) 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
WECC2018019146	CIP-006-6	R1	[redacted]	[redacted]	7/1/2016	6/27/2018	Compliance Audit	Completed

Risk Assessment

WECC determined this noncompliance posed a moderate risk and did not pose a serious and substantial risk to the reliability of the BPS. Specifically, the entity failed to adequately document and implement one or more physical security plan(s) that collectively included the applicable requirement parts of CIP-006-6 R1, that is, Parts 1.2, 1.4, 1.5, 1.6, 1.7, 1.8, and 1.9. Part 1.1 and Part 1.3 are not in scope of this noncompliance.

However, the entity implemented good compensating controls in the form of System Security Management. Specifically, for the MIBCS, the entity locked down unneeded physical and logical ports; implemented malicious code prevention and detection; monitored security events; and ensured passwords were enforced and met length and complexity requirements. Though these controls would not prevent the noncompliance from occurring, they would reduce the likelihood of a malicious actor infiltrating and compromising the entity's Energy Management System (EMS). No harm is known to have occurred.

The entity has no relevant previous violations of this or similar Standards and Requirements.

Mitigation

To mitigate this noncompliance, the entity:

1) re-keyed all PSP access points and PACS panels to ensure control of physical hard-keys access;
2) created and implemented a new Physical Hard-keys Procedure, which is incorporated into the overall Physical Security Plan, to document a clear process;
3) logged entry of each individual with physical hard-keys access into each PSP, with information to identify the individual and date and time of entry;
4) retained physical hard-keys access logs of entry of individuals with authorized unescorted physical access into each PSP for at least ninety calendar days;
5) incorporated controls around the storage, access, issuance, monitoring, and use of the hard-keys;
6) installed additional cameras and sensors to assist in monitoring, and to increase security and situational awareness of all PSP access points and PACS;
7) improved real time monitoring of PSP access points by transitioning the physical security monitoring role from its Power System Controllers to dedicated Security Guards staffed 24x7;
8) expanded the role of third party Security Guards to enforce controls, monitor PSP access points, to include applicable cameras, sensors and alarms, and document acknowledgement and responses to detected unauthorized access;
9) decreased the number of PACS to reduce the risks and potential points of failure, and updated PSP diagrams to reflect the changes;
10) increased the number of staff that support compliance and physical security responsibilities. The two employees (renamed as Safety and Security Specialists) in these positions will be Subject Matter Experts (SMEs) for CIP-006-6 and will be responsible for, among other things, training, implementation, controls and oversight associated with the Physical Hard-keys Procedure and processes for acknowledging and responding to alarms for detected unauthorized access;
11) developed and provided training to Security Guards to monitor physical access controls via PACS and security cameras;
12) developed and implemented a training program for Security Guards on event handling and escalation matrix;
13) provided physical security control system training to Power System Controllers;
14) trained CIP-006-6 SMEs on the updated Physical Security Procedure;
15) retained third party physical security consultants to evaluate and provide threat and vulnerability assessment of PSPs;
16) reconfigured and tested PACS software to confirm door alarms are audible;
17) confirmed that external facing hinges on access points, including the [redacted] emergency door, are hardened;
18) reduced timeframe of door-held-open results in alarm from 75 seconds to 30 seconds;
19) increased security awareness by posting signage and providing training for all employees;
20) implemented a periodic process for physical hard-keys inventory, as defined in the Physical Security Procedure; and
21) implemented a review process to validate acknowledgment of unauthorized access to PSPs and PACS was performed within 15 minutes and that appropriate compliance evidence exists, as defined in in the Physical Security Procedure.

WECC has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019149	CIP-006-6	R1	[redacted]	[redacted]	7/1/2016	6/27/2018	Compliance Audit	Completed

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

During a Compliance Audit conducted [redacted] WECC auditors determined the entity, as a [redacted] and [redacted] had a potential noncompliance with CIP-006-6 R1.

Specifically, WECC found several issues with the entity's Physical Security Plan:

a. the entity distributed and utilized hard-keys to access two Physical Security Perimeters (PSPs) containing MIBCS. Seven keys were distributed to individuals; one key was located in a [redacted] dispatch area; and the remaining spare keys were secured in the [redacted] The Physical Security Plan lacked acceptable use instructions for the hard-keys and only contained a "for emergency use only" statement. No hard-key management, inventory, or log records were available. The entity's Physical Security Plan stated that physical access into each PSP access point was controlled by an ID Badge Physical Access Control System (PACS) and did not address the secondary hard-key access which was available, and at times used by the personnel with hard-keys (Part 1.2);

b. the entity's Physical Security Plan states that all PSP access points at the [redacted] were electronically monitored 24 hours a day, seven days a week. However, it was observed that several egress access points were constructed to only be monitored by a local crash bar sounder, and upon testing, one door failed to indicate an alarm condition when it was opened, and no alarm was displayed by the PACS. An additional egress door produced a local alarm in the crash bar but again, was not displayed to the dispatch operators. At the [redacted] an egress door was unmarked; had no local sounder; and was unmonitored by the PACS or the [redacted] dispatch operator (Part 1.4);

c. a review of evidence alarm logs showed that no recorded alarm events were ever acknowledged within 15 minutes of sounding. Operators have PACS viewing screens for PACS alarms events, however, alarm events were not monitored or assessed within 15 minutes and the only activity the [redacted] operators were doing was contacting facilities personnel to investigate alarms which was not occurring within 15 minutes of the alarm (Part 1.5);

d. the tamper alarm on the panel controlling access to the [redacted] PSP was generating alarms; however, the alarms were not being monitored (Part 1.6);

e. because the generated alarms on the access control panel to the [redacted] PSP was not being monitored, unauthorized access was not being detected and no response was being performed within 15 minutes of when the entity should have detected the unauthorized access. Additionally, the entity's Physical Security Plan did not mention the 15-minute time requirement when monitoring for unauthorized access (Part 1.7);

f. the entity was not able to provide information to identify individuals and date and time of entry into PSPs for individuals who utilized hard-keys. The PACS was only able to record a "door forced" alarm event when a hard-key was used. This was indistinguishable from any other cause for a forced door event and none of the log requirements were recorded in the PACS. Additionally, the entity was not monitoring alarm events in real time and did not provide any comments as a manual addendum, no details existed for logging access, authorized or not, with any method that did not involve an authorized ID badge (Part 1.8); and

g. the entity did not capture, electronically via the PACS or manually, any physical access log information when hard-keys were used. As such, no log files existed for at least 90 calendar days, or at all in some cases, to record entry of individuals with authorized unescorted physical access into each PSP when utilizing a hard-keys (Part 1.9).

After reviewing all relevant information, WECC Enforcement agreed with the audit findings. Therefore, the entity failed to adequately document and implement one or more physical security plan(s) that collectively included the applicable requirement parts of CIP-006-6 R1, that is, Parts 1.2, 1.4, 1.5, 1.6, 1.7, 1.8, and 1.9. Part 1.1 and Part 1.3 are not in scope of these violations.

The root cause of the noncompliance was less than adequate documentation. Specifically, the entity's Physical Security Plan was ineffective in ensuring compliance with the Standards and Requirements in that it was written in direct conflict with what was actually being performed by the personnel responsible for implementation of the Physical Security Plan.

The noncompliance began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on June 27, 2018, when the entity completed mitigating activities, for a total of 727 days of noncompliance.

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC) 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
WECC2018019149	CIP-006-6	R1	[redacted]	[redacted]	7/1/2016	6/27/2018	Compliance Audit	Completed

Risk Assessment

WECC determined this noncompliance posed a moderate risk and did not pose a serious and substantial risk to the reliability of the BPS. Specifically, the entity failed to adequately document and implement one or more physical security plan(s) that collectively included the applicable requirement parts of CIP-006-6 R1, that is, Parts 1.2, 1.4, 1.5, 1.6, 1.7, 1.8, and 1.9. Part 1.1 and Part 1.3 are not in scope of this noncompliance.

However, the entity implemented good compensating controls in the form of System Security Management. Specifically, for the MIBCS, the entity locked down unneeded physical and logical ports; implemented malicious code prevention and detection; monitored security events; and ensured passwords were enforced and met length and complexity requirements. Though these controls would not prevent the noncompliance from occurring, they would reduce the likelihood of a malicious actor infiltrating and compromising the entity's Energy Management System (EMS). No harm is known to have occurred.

The entity has no relevant previous violations of this or similar Standards and Requirements.

Mitigation

To mitigate this noncompliance, the entity:

1) re-keyed all PSP access points and PACS panels to ensure control of physical hard-keys access;
2) created and implemented a new Physical Hard-keys Procedure, which is incorporated into the overall Physical Security Plan, to document a clear process;
3) logged entry of each individual with physical hard-keys access into each PSP, with information to identify the individual and date and time of entry;
4) retained physical hard-keys access logs of entry of individuals with authorized unescorted physical access into each PSP for at least ninety calendar days;
5) incorporated controls around the storage, access, issuance, monitoring, and use of the hard-keys;
6) installed additional cameras and sensors to assist in monitoring, and to increase security and situational awareness of all PSP access points and PACS;
7) improved real time monitoring of PSP access points by transitioning the physical security monitoring role from its Power System Controllers to dedicated Security Guards staffed 24x7;
8) expanded the role of third party Security Guards to enforce controls, monitor PSP access points, to include applicable cameras, sensors and alarms, and document acknowledgement and responses to detected unauthorized access;
9) decreased the number of PACS to reduce the risks and potential points of failure, and updated PSP diagrams to reflect the changes;
10) increased the number of staff that support compliance and physical security responsibilities. The two employees (renamed as Safety and Security Specialists) in these positions will be Subject Matter Experts (SMEs) for CIP-006-6 and will be responsible for, among other things, training, implementation, controls and oversight associated with the Physical Hard-keys Procedure and processes for acknowledging and responding to alarms for detected unauthorized access;
11) developed and provided training to Security Guards to monitor physical access controls via PACS and security cameras;
12) developed and implemented a training program for Security Guards on event handling and escalation matrix;
13) provided physical security control system training to Power System Controllers;
14) trained CIP-006-6 SMEs on the updated Physical Security Procedure;
15) retained third party physical security consultants to evaluate and provide threat and vulnerability assessment of PSPs;
16) reconfigured and tested PACS software to confirm door alarms are audible;
17) confirmed that external facing hinges on access points, including the [redacted] emergency door, are hardened;
18) reduced timeframe of door-held-open results in alarm from 75 seconds to 30 seconds;
19) increased security awareness by posting signage and providing training for all employees;
20) implemented a periodic process for physical hard-keys inventory, as defined in the Physical Security Procedure; and
21) implemented a review process to validate acknowledgment of unauthorized access to PSPs and PACS was performed within 15 minutes and that appropriate compliance evidence exists, as defined in in the Physical Security Procedure.

WECC has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018019151	CIP-007-6	R2	[redacted]	[redacted]	7/1/2016	6/20/2018	Compliance Audit	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	During a Compliance Audit conducted [redacted] WECC auditors determined the entity, as [redacted] and TOP, had a potential noncompliance with CIP-007-6 R2 Part 2.3. Specifically, the audit team identified three BES Cyber Assets (BCAs) in the MIBCS at the entity's [redacted] for which there were four security patches for software identified as applicable but not applied, nor was there a dated mitigation plan created, or an existing mitigation plan revised, within 35 calendar days of the evaluation completion. After reviewing all relevant information, WECC Enforcement agreed with the audit finding. Therefore, the entity failed for applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, to take one of the following actions: apply the applicable patches; create a dated mitigation plan; or revise an existing mitigation plan, as required by CIP-007-6 R1 Part 2.3. Additionally, WECC determined that the entity failed to include the identification of a source that the entity tracks for the release of cyber security patches, as required by CIP-007-6 R2 Part 2.1, and failed to at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1, as required by CIP-007-6 R2 Part 2.2. Regarding Part 2.1, the entity initially did not include a patching source for software on three Cyber Assets because it did not know the software had security updates; however, the software should have been tracked for the release of cyber security patches. The Cyber Assets in scope included 14 BCAs in the MIBCS at the [redacted], and one EACMS associated with the MIBCS [redacted] There was a total of 111 patches subject to this violation. The root cause of the noncompliance was less than adequate documentation. Specifically, the entity's Security Patch Management Program was not sufficient to meet compliance with the Standards. Additionally, the processes and procedures to support the Security Patch Management Program to ensure compliance were not well defined. The noncompliance began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on June 20, 2018, when the entity completed mitigating activities, for a total of 720 days of noncompliance.
Risk Assessment	WECC determined this issue posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to include the identification of a source that the entity tracks for the release of cyber security patches, as required by CIP-007-6 R2 Part 2.1; at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1, as required by CIP-007-6 R2 Part 2.2.; and for applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: apply the applicable patches; create a dated mitigation plan; or revise an existing mitigation plan, as required by CIP-007-6 R1 Part 2.3. However, the entity implemented good compensating controls in the form of System Security Management. Specifically, the entity locked down unneeded physical and logical ports; implemented malicious code prevention and detection; monitored security events; and ensured passwords were enforced and met length and complexity requirements. Though these controls would not prevent the noncompliance from occurring, they would reduce the likelihood of a malicious actor infiltrating and compromising the entity's EMS. No harm is known to have occurred. The entity has no relevant previous violations of this or similar Standards and Requirements.
Mitigation	To mitigate this noncompliance, the entity: 1) installed all security patches evaluated as applicable where evidence of installation was not provided at audit; 2) installed additional security patches evaluated as applicable, discovered as additional scope while mitigating; 3) reviewed and revised Security Management Procedure to include a more standardized and controlled patching process, to include, but not limited to: a) the SME is required to record the evaluation date and the installation date of a security patch on a per asset basis; b) cyber security patches will be evaluated for applicability every 35 calendar days and what actions to take when evaluating; c) addresses patch source identification and its tracking; and d) desk level procedures which walk responsible individuals through how to perform patch installs and how to track and record for compliance obligations; 4) reviewed and revised evidence collection process(es) to ensure proper compliance documentation is created and retained; and 5) provided training to all SMEs responsible for patch management to ensure they understand the updated and what is required of them to meet compliance. WECC has verified the completion of all mitigation activity.

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC) 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
WECC2017017460	CIP-010-2	R1: P1.1; P1.2; P1.3	[redacted]	[redacted]	7/1/2016	2/26/2018	Self-Report	Completed

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

On [redacted], the entity submitted a Self-Report stating, as [redacted], and [redacted], it was in violation of CIP-010-2 R1. The conversion to CIP Version 5 resulted in a large increase in the entity's inventory of Cyber Assets. Following the implementation of CIP Version 5, the entity validated its Configuration Management Database (CMDB) using a combination of internal reviews, Cyber Vulnerability Assessments (CVA), and Change Control testing and monitoring. During these internal reviews, the entity identified instances where the baseline for various Cyber Assets, including software lists, and ports and services, were not correct or were not updated within the allowed timeframe. Due to the size of the implementation related to the entity's substation Electronic Security Perimeters, the time it took to physically verify was lengthy. The challenges presented with the identification of ports and services; new software requirements on the jump host; and support requirements of cross-functional teams contributed to this violation.

Additionally, the entity's CMDB application was upgraded and included a redesign of the CMDB tables during the same period as the conversion to CIP Version 5. This application tracked the entity's change control processes, including preventative controls such as approvals, testing, validation, and reviews. With the upgrade to the system, all information had to be exported, re-imported, and combined with new in-coming Cyber Assets. The volume of data and the manual process for validating the import caused some initial load errors; however, in most cases, the Cyber Assets were correctly configured. The entity increased the scope of the violation by [redacted] additional Cyber Assets in the High Impact Bulk Electric System (BES) Cyber System (HIBCS) and Medium Impact BES Cyber System (MIBCS) which it discovered while preparing its Mitigation Plan. Lastly, during the entity's [redacted] WECC audit, WECC auditors confirmed an additional [redacted] Cyber Assets as being in scope of this violation. The final scope of this violation was [redacted] Cyber Assets as described in Table 1:

Table 1

Device Count	Device Type*	BCS Impact Rating	Part 1.1 Sub-Part 1.1.4	Part 1.2	Part 1.3	Part 1.1 Sub-Part 1.1.4 and Part 1.2
[redacted]	BCA with ERC	High	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	BCA with ERC	Medium	[redacted]		[redacted]	[redacted]
[redacted]	EACMS	High	[redacted]			
[redacted]	EACMS	Medium	[redacted]	[redacted]		
[redacted]	EAP	Medium	[redacted]			
[redacted]	PACS	High	[redacted]	[redacted]		
[redacted]	PCA	High	[redacted]			
[redacted]	PCA	Medium	[redacted]			
[redacted]			[redacted]	[redacted]	[redacted]	[redacted]

*BES Cyber Asset with External Routable Connectivity (BCA with ERC), Electronic Access Control or Monitoring System (EACMS), Electronic Access Point (EAP), Physical Access Control System (PACS), and Protected Cyber Asset (PCA)

After reviewing all relevant information, WECC determined that for the Cyber Assets listed in Table 1, the entity failed to develop baseline configurations that included any logical network accessible ports, as required by CIP-010-2 R1 Part 1.1 Sub-Part 1.1.4.; failed to authorize and document changes that deviate from the existing baseline configuration for, as required by CIP-010-2 R1 Part 1.2; and failed to update the baseline configuration for a change that deviated from the existing baseline configuration within 30 calendar days of completing the change, as required by CIP-010-2 R1 Part 1.3.

The root cause of the noncompliance was an insufficient time for workers to complete all required tasks. Specifically, the entity planned its CMDB upgrade during the same timeframe as its CIP Version 5 implementation. This did not allow enough time for the entity to organize its upgrade and ensure that compliance was met with the Standards and Requirements of CIP Version 5.

This noncompliance started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable, and ended on February 26, 2018, when the entity met all the applicable parts of the Requirement, for a total of 606 days of noncompliance.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017017460	CIP-010-2	R1: P1.1; P1.2; P1.3	[redacted]	[redacted]	7/1/2016	2/26/2018	Self-Report	Completed

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. In this instance, the entity failed to develop a baseline configuration, including any logical network accessible ports, as required by CIP-010-2 R1 Part 1.1 Sub-Part 1.1.4; failed to authorize and document changes that deviate from the existing baseline configuration for, as required by CIP-010-2 R1 Part 1.2; and failed to update the baseline configuration for a change that deviated from the existing baseline configuration within 30 calendar days of completing the change, as required by CIP-010-2 R1 Part 1.3. The entity implemented weak internal controls. Specifically, the entity did not have an adequate change review and approval process to ensure compliance with the baseline configuration requirements. Additionally, the entity did not make the appropriate changes to the baseline configurations until several months after the issues were first discovered. However, the entity had implemented an internal review process that included a combination of internal reviews, assessments reviews, and change control testing and monitoring of Cyber Assets, which is how this violation was discovered. As further compensation, the applicable Cyber Assets were within a PSP and were monitored 24 hours a day; individuals with access had the proper authorization and had completed personnel risk assessments; the [redacted]; and remote access required two-factor authentication. No harm is known to have occurred. The entity's relevant prior compliance history with CIP-010-2 R1 includes NERC Violation ID [redacted] which WECC determined should not serve as a basis for applying a penalty. Regarding NERC Violation ID [redacted] and [redacted] these violations had a root causes of less than adequate processes, which was distinct, separate, and not relevant to the root cause of this Notice.
Mitigation	To mitigate this noncompliance, the entity: 1) developed baseline configurations that included any logical network accessible ports for the Cyber Assets in scope; 2) authorized, and documented changes that deviated from the existing baseline configurations for the Cyber Assets in scope; 3) updated changes to baseline configurations for the Cyber Assets in scope; 4) conducted a training with the device owners to go over the new device class workflow and the existing device change control workflow to assist with future prevention of the missed requirements; 5) provided reference material for the change management process to all device owners; 6) updated its change management templates, to provide more detail for each task required for the change; 7) updated its process for monitoring change controls so that the Compliance Program Management Office team is aware of change controls that are pending and the planned end dates; 8) conducted weekly meetings with management to ensure device owners were provided ongoing awareness, training, and best practice guidance; and 9) updated its supervisory review checklist which provides specific guidance for reviewing change controls. WECC has verified the completion of all mitigation activity.

COVER PAGE

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the 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	FRCC2019021012			Yes	Yes								Yes	Category 2 – 12: 2 years
2	MRO2018019478	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
3	RFC2016015631			Yes	Yes									Category 2-12: 2 years
4	RFC2017017371			Yes	Yes									Category 2-12: 2 years
5	RFC2017018457	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
6	RFC2017018001	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
7	RFC2017018003	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
8	RFC2017018006	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-12: 2 years
9	RFC2018019050	Yes												Category 1: 3 years
10	RFC2018019119	Yes												Category 1: 3 years
11	TRE2017016866	Yes		Yes	Yes							Yes		Category 1: 3 years; Category 2 – 12: 2 year

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2019021012	CIP-010-2	R2. 2.1.	[redacted] ("the Entity")	[redacted]	5/26/2018	10/22/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed noncompliance.)	On January 30, 2019, the Entity submitted a Self-Report stating that, as a [redacted] it was in violation of CIP-010-2 R2 Part 2.1. This violation started on May 26, 2018, when the Entity failed to monitor the baseline configurations of six (6) EACMS firewalls for changes at least once every 35 calendar days as required by Part 2.1 and ended on October 22, 2018, when all six (6) EACMS firewall baseline configurations had been successfully reviewed. The duration of late review for each EACMS varied from 53 to 150 days. The Entity initially discovered one (1) of the EACMS firewall and it was determined that the account password used for the process to perform the automated review of the baseline configuration had unknowingly expired preventing the process from properly completing. Subsequent extent of condition review identified five (5) additional EACMS firewalls with the same expired password situation bringing the total to six (6) EACMS firewalls out of the total Cyber Assets reviewed. The cause for this violation was an oversight upon the commissioning of the account used for the process that monitored these EACMS, which resulted in the account not being excluded from the global password expiration policy. There was a gap in accounting for this scenario through the Entity's change management controls.
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 (BPS). Specifically, the Entity's failure to monitor the baseline configurations of the EACMS could have allowed unknown changes to go undetected which could introduce vulnerabilities providing attack vectors that once exploited would allow unauthorized access or misuse of the EACMS affecting the reliability of the BPS. The risk was reduced because many other layers of protection were in place. Also, other security tools were actively monitoring the various activities of the EACMS devices during the periods when the Entity was not monitoring for baseline changes to OS version information. No harm is known to have occurred as no CIP-005 and CIP-007 security controls were impacted during this period nor were any unauthorized changes to the baselines made. The Region determined that the Entity's compliance history should not serve as a basis for applying a penalty. Prior noncompliance (FRCC2018020697) was a compliance exception which is not applicable to compliance history and should not be used as an aggravating factor.
Mitigation	To mitigate this violation, the Entity: 1) changed the service account password to not expire; 2) performed an extent of condition review; 3) determined root cause; 4) created preventative control to include a question in the checklist to review service accounts. "If any functional (service) accounts were created, did you ensure that passwords have no expiration?"; and 5) performed preventative control communication with applicable personnel to not use accounts that expire for monitoring purposes.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
MRO2018019478	CIP-007-6	R2	[redacted]	[redacted]	8/4/2016	11/21/2017	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 4, 2018, [redacted] submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R2. [redacted]. The noncompliance occurred in [redacted]. Specifically, [redacted] reports that in preparation for an internal audit, it discovered 95 occasions where patches were not evaluated within 35 days of a prior evaluation as required by P2.2. The patches were evaluated between one day late and 183 days late; 93 of the 95 patches were evaluated within two evaluation periods (approximately 70 days). The noncompliance was caused by [redacted] failure to sufficiently train personnel on the applicable period in which patches must be evaluated; staff believed that the applicable period was 35 days from the date of the work order system notification, leading to many late evaluations. Additionally, [redacted] did not implement internal controls (such as status reports) to track patch evaluation status and detect late patch evaluations. The noncompliance began on August 4, 2016, 36 days after the prior evaluation, and ended on November 21, 2017, when the last patch was evaluated.
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 noncompliance was not minimal due to the scope of the noncompliance. Specifically, the noncompliance impacted all of [redacted] Control Center Cyber Assets and involved 95 instances where a security patch was not timely evaluated. Additionally, two of the 95 patches were not evaluated for 153 and 183 days respectively. [redacted]. This restricted electronic access is a strong and uncommon control for a registered entity of [redacted] size. No harm is known to have occurred. [redacted] has no relevant history of noncompliance. .
Mitigation	To mitigate this noncompliance, [redacted]: 1) performed a comprehensive review to identify lapsed patch evaluations; 2) completed all lapsed patch evaluations; 3) developed three new reports to aid the regular review of patch evaluations, applications, and patch mitigation plan development; 4) improved existing reporting; 5) provided reinforcement training to applicable SMEs; and 6) instituted a weekly patch review meeting with managers responsible for oversight of the patch management process. MRO verified the completion of mitigating activities.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2016015631	CIP-007-3a	R1	[redacted]	[redacted]	6/30/2015	2/2/2016	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On March 23, 2016, the entity submitted a Self-Report to ReliabilityFirst stating that as a [redacted], it was in noncompliance with CIP-007-3a R1. The entity identified four instances of noncompliance over a six month period. The entity identified the first two instances on October 13, 2015. These two instances concern the same two non-critical Cyber Assets CIP assets (servers). In the first instance, on June 30, 2015, an employee opened a change ticket to uninstall and reinstall software on the two assets, but the employee did not mark the ticket as a "significant change" as he should have. While the employee questioned whether the uninstallation and reinstallation of software constituted a "significant change," the entity's documentation did not address uninstalling and reinstalling software. Thus, the change requested was not recognized as a significant change, and therefore test procedures were not performed as required. In the second instance, on August 6, 2015, an employee opened a change ticket to install patches for the two servers, but the employee mistakenly did not mark the ticket as a "significant change" due to a miscommunication between departments regarding the servers. As a result, the installation of patches was not identified as a significant change and therefore test procedures were not performed as required. The third instance concerns a CIP asset that was mislabeled as "non-CIP" in the entity's system. As a result, on October 7, 2015, the entity applied patches to the asset without performing test procedures. The root cause that led to this issue was a misunderstanding between the entity's security and compliance team and the infrastructure support team around new CIP version 5 nomenclature, which led to the asset being labeled as non-CIP. Pursuant to the CIP version 5 nomenclature, the asset was marked as "elevated" (meaning the asset must be compliant with CIP standards, but is not a Critical Cyber Asset as specified in the version 3 standards) in the entity's asset management system. The fourth instance was identified during a security review on February 2, 2016 that occurred as a result of a proposed change to cyber assets associated with the entity's password vault (Electronic Access Control or Monitoring System). At the time of the noncompliance, an analyst executed all of the password vault-specific tasks within the test procedures, but not the tasks relating to all Windows systems (evaluate Windows accounts). After identifying the instance, the analyst determined that he failed to perform the necessary tests on two occasions, once on October 15, 2015 and once on November 19, 2015. A root cause to the noncompliance was human error, in addition to procedural deficiencies. These changes were the first changes that the analyst performed on the new password vault cyber assets and he mistakenly assumed that only the procedure steps specifically listed for the password vault needed to be performed and checked during the security review. In all four instances, the entity performed test procedures immediately upon discovery and these procedures confirmed that there were no adverse effects to security controls. In addition to the contributing factors specified above with each instance, an additional contributing factor was ineffective workforce management practices. More specifically, additional training regarding the entity's systems and procedures could have alleviated some of the errors that led to the instances. The noncompliance began on June 30, 2015, the date of the first instance, and ended on February 2, 2016, when the entity performed test procedures in the last instance.
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. Applying patches or executing changes on CIP assets without properly executing test procedures could potentially introduce vulnerabilities. Additionally, uninstalling software without first conducting tests could result in dependency issues. However, these risks were mitigated by the following factors. In all instances, redundant cyber assets were available if the changes negatively affected the cyber assets at issue and, therefore, the negative effects would have been limited. Additionally, the entity has implemented detective controls such as daily compliance scans that verify the state of cybersecurity controls on its Cyber Assets. Further, in the first instance, the entity was uninstalling and re-installing software that had already been in service at the entity, thus reducing the likelihood the changes would negatively affect the entity's systems. In the second instance, the patches were supplied by a known vendor for assets on which the entity previously installed patches from the same vendor, thus reducing the likelihood the changes would negatively affect the entity's systems. The third instance was an isolated issue that resulted from lack of understanding around new CIP Version 5 nomenclature. In the fourth instance, the entity performed most of the tests and only missed a subset of tests. Accordingly, the issue posed only moderate risk to the BPS. The entity has relevant compliance history. However, ReliabilityFirst determined that the current noncompliance qualifies for FFT treatment because it posed only moderate risk and the entity's compliance history should not serve as a basis for applying a penalty. Although the entity's compliance history is relevant to and contributed to the determination of FFT treatment, it is not indicative of a systemic issue.
Mitigation	To mitigate this noncompliance, the entity:

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2016015631	CIP-007-3a	R1	[redacted]	[redacted]	6/30/2015	2/2/2016	Self-Report	Completed
			1) evaluated the change management ticketing system and associated process for improvement; 2) updated Inclusion/Exclusion documentation to address the re-installation of software; 3) updated the Corporate Test procedures document adding clarity around proper execution of procedure; and 4) reviewed current requirements for test procedures and identification of CIP assets which require test procedures with applicable employees. ReliabilityFirst has verified the completion of all mitigation activity.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017017371	CIP-010-2	R1	[redacted]	[redacted]	9/14/2016	1/27/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On March 30, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [redacted], it was in noncompliance with CIP-010-2 R1. This noncompliance involves two instances. In the first instance, the entity did not add four [redacted] to its tool for baseline configuration scans upon their classification as Electronic Access Control or Monitoring Systems (EACMS) on October 5, 2016. As a result of not adding each of the four firewalls to its tool for baseline configuration scans, the entity did not develop a baseline configuration as required under CIP-010-2 R1 Part 1.1. The [redacted] were not protecting the Electronic Security Perimeter (ESP), but rather were protecting assets containing management tools for managing the entity's Electronic Access Points. The root cause was, in part, human error as the four cyber assets were mistakenly added to a larger request of other EACMS and the approver did not notice the four assets in order to approve them. They were classified as EACMS prematurely before the request for baselines was submitted. After identifying the issue, the entity updated the baselines for two of the [redacted] on January 3, 2017 and the remaining two on January 27, 2017 (the latter two required additional change management and [redacted] changes in order for the tool to gain access to the cyber assets). These cyber assets had previously been CIP cyber assets (EACMS-EAP) and were removed from scope when the associated ESP networks were retired. They were returned to CIP scope (EACMS) to be used as a management platform for other CIP cyber assets (EACMS-EAP). The configuration of security controls required for CIP remained in place during the period of time when the devices were corporate cyber assets. In the second instance, two servers became Bulk Electric System (BES) Cyber Assets on September 14, 2016. Because of the type of assets at issue, the entity was required to track the assets' firmware version (CIP-010-2 R1 Part 1.1.1) and accessible ports (CIP-010-2 R1 Part 1.1.4). While the entity correctly developed a baseline configuration for the associated firmware for these servers, it did not develop a baseline configuration for the ports. The root cause was that the analyst mistakenly implemented only one of the two required baseline components. After identifying the issue, the entity updated the baselines on January 4, 2017. The entity identified both instances during a quarterly review, which occurred on January 3, 2017, to compare what cyber assets are in its tool against its list of CIP-scoped assets. The subject noncompliance involves the management practice of verification as the entity lacked verification controls to ensure all baselines requirements are met before placing assets in production. The noncompliance began on September 14, 2016, the first date the entity failed to maintain a baseline, and ended on January 27, 2017, when the entity completed baselines for the assets at issue.
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. Not maintaining accurate baselines has the potential to affect the reliability of the bulk electric system by reducing the entity's ability to identify unauthorized activity, changes, or vulnerabilities and by introducing system instability when making changes to assets. The risks here are somewhat mitigated because there were other protections in place to detect malicious activity and prevent compromise of the assets. In the first instance, other than creating and maintaining baselines, the assets were afforded all protections required by the CIP Standards (e.g., patching, monitoring, logging, change control, etc.). Regarding the second instance, other than creating and maintaining baselines and monitoring of ports, the assets were afforded all protections required by the CIP Standards. The entity has relevant compliance history. However, for the reasons set forth above, ReliabilityFirst determined that the current noncompliance qualifies for FFT treatment because it posed only moderate risk, and the entity's compliance history should not serve as a basis for applying a penalty. Although the entity's compliance history is relevant to and contributed to the determination of FFT treatment, it is not indicative of a systemic issue.
Mitigation	To mitigate this noncompliance, the entity: 1) discussed the importance of capturing a full baseline for the entity's CIP-scoped Cyber Assets with the analysts; 2) updated the tool to include full baselines for the six cyber assets; 3) implemented a new service that prohibits EACMS (and other CIP-scoped assets) from being classified as such without ensuring a baseline has been completed. The service also ensures all other cyber security controls are in place. The service is implemented via another tool as an electronic workflow with gates that require a successful implementation and confirmation of CIP cyber security controls prior to being used as a CIP scoped asset; 4) updated the pre-production baseline inspection practices to include validation that all necessary parts of the baseline are being documented by the tool; and 5) trained the appropriate personnel on the update to the pre-production baseline inspection practices. ReliabilityFirst has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018457	CIP-010-2	R1	[redacted]	[redacted]	8/20/2016	8/29/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On September 29, 2017, the entity submitted a Self-Report stating that, as a [redacted] and [redacted], it was in noncompliance with CIP-010-2 R1. On May 12, 2017, during routine baseline configuration monitoring review, the entity discovered that a [redacted] associated with a [redacted] Bulk Electric System Cyber System was listed in "pre-production" status in the system, but had been in production since August 20, 2016. When the entity placed the [redacted] into production on August 20, 2016, the responsible team failed to complete the documentation for their assessment in the system. The failure to close this assessment out in the system resulted in a failure to properly update the baseline. However, the entity performed all of its other change management activities for this device, including security controls testing before and after the change. The root cause of this noncompliance was the failure to follow change management protocols. [redacted] This major contributing factor involves the management practice of asset and configuration management, which includes controlling changes to assets and configuration items and baselines. This noncompliance started on August 20, 2016, when the entity placed the [redacted] into production and ended on August 29, 2017, when the entity updated the system database to accurately reflect the current state of the [redacted].
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 posed by the entity having outdated baseline information is that it could rely on incorrect information when performing subsequent tasks and be unable to properly monitor for unintended or unauthorized changes. This risk was mitigated in this case by the following factors. First, the entity performed all of its other change management activities for this device, including security controls testing before and after the change. Second, access to these [redacted] from external connections would require passing through at least two other [redacted] before reaching these [redacted], [redacted]. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances were either the result of different root causes or constitute high frequency conduct, which ReliabilityFirst determined did not warrant an alternative disposition method.
Mitigation	To mitigate this noncompliance, the entity: 1) corrected the device status in system from "pre-production" to "production"; 2) updated the system record associated with the [redacted] following the completed assessment; 3) communicated to device managers and device assessors the need for following proper change management processes to ensure a device is properly commissioned to production which includes updates to the system record and assessment; 4) met with responsible personnel to reinforce how to enter information into the system to reduce risk while guidance is created; 5) reviewed device status in the system for the fields of Record Status, Device Status, and Assessment for accuracy and completeness; 6) enhanced guidance to performers to address specific scenarios/use cases for proper handling of device status changes (including retirement of devices); 7) enhanced/communicated procedure to address timeframe for performing, completing and approving assessments; and 8) conducted a training session with device managers/assessors to enhance understanding of the new guidance addressing proper handling of device updates (scenarios/use cases). The entity will also address what standard are reliant upon the system data. ReliabilityFirst has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018001	CIP-010-2	R1	[redacted]	[redacted]	11/2/2016	7/14/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On July 14, 2017, the entity submitted a Self-Report stating that, as a [redacted] and [redacted], it was in noncompliance with CIP-010-2 R1. During periodic baseline reviews, the entity identified five issues with its change management and baseline updating process. Two of these changes involved changes to switches and the remaining three changes involved firewall updates or changes to a firewall manager. In four instances, a change was completed without proper authorization. Because the change management application triggers the need for baseline updates, there were no immediate notifications that a baseline update was required. Consequently, the baselines were not updated within 30 calendar days of completing the change as required by CIP-010-2 R1 [redacted]. In the fifth instance, a change was properly authorized and completed, but the responsible individual failed to update the baseline within the required time frame [redacted]. The root cause of this noncompliance was two-fold. First, the four instances involving improper change management were the result of the responsible individuals failing to properly execute the change management process either due to a lack of understanding or oversight. Second, the instance involving only the late baseline update was the result of the responsible individual failing to follow the baseline update process due to insufficient awareness. This noncompliance started on November 2, 2016, when the first change was made, and ended on July 14, 2017, when the entity made the last update to the impacted baselines.
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 making unauthorized changes is that they could adversely impact the security or functionality of the impacted assets. The risk associated with failing to update baselines within the required timeframe is that the entity may have incorrect or outdated information to appropriately analyze future changes. In this case, the risk posed by this noncompliance is not minimal because the impacted assets [redacted] perform critical security functions on high impact Bulk Electric System Cyber Assets at three entities. The risk was mitigated in this case by the fact that, in most cases, the entity identified and corrected these errors within a reasonable time following the 30 day deadline. ReliabilityFirst also notes that, during the period of noncompliance, no changes occurred on the impacted devices. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances either arose from different causes or because ReliabilityFirst determined that the conduct at issue constituted high frequency conduct that the entity quickly detected and corrected.
Mitigation	To mitigate this noncompliance, the entity: 1) conducted a meeting with the compliance team staff. The key manager for the group, and staff managers, strongly emphasized the criticality of ensuring changes are properly reviewed, authorized, and evidenced; 2) conducted in-person training to members of the compliance team to review process for baseline reviews/updates. Class included a hands-on review/baseline update of actual changes; 3) completed baseline updates to the impacted issues; 4) conducted a meeting with relevant staff to emphasize the importance of effective change management. The key manager for the group, and staff managers, strongly emphasized the criticality of ensuring changes are properly reviewed, authorized, and evidenced; 5) conducted in person training to members of the relevant compliance team assigned to CIP changes on proper NERC CIP change management procedures; 6) [redacted]; 7) added a field in database to note when baseline evidence is due [redacted]); 8) conducted extent of condition review from Q3 2016 to July 2017 to identify additional change management issues for relevant staff; and 9) conducted a quality review and sampling of change tickets 90 days from the last corrective completion date to evaluate if changes are updated to Pending Production status within [redacted]. ReliabilityFirst has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018003	CIP-010-2	R1	[redacted])	[redacted]	11/2/2016	7/14/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On July 14, 2017, the entity submitted a Self-Report stating that, as a [redacted] and [redacted], it was in noncompliance with CIP-010-2 R1. During periodic baseline reviews, the entity identified five issues with its change management and baseline updating process. Two of these changes involved changes to switches and the remaining three changes involved firewall updates or changes to a firewall manager. In four instances, a change was completed without proper authorization. Because the change management application triggers the need for baseline updates, there were no immediate notifications that a baseline update was required. Consequently, the baselines were not updated within 30 calendar days of completing the change as required by CIP-010-2 R1 [redacted]. In the fifth instance, a change was properly authorized and completed, but the responsible individual failed to update the baseline within the required time frame [redacted]. The root cause of this noncompliance was two-fold. First, the four instances involving improper change management were the result of the responsible individuals failing to properly execute the change management process either due to a lack of understanding or oversight. Second, the instance involving only the late baseline update was the result of the responsible individual failing to follow the baseline update process due to insufficient awareness. This noncompliance started on November 2, 2016, when the first change was made, and ended on July 14, 2017, when the entity made the last update to the impacted baselines.
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 making unauthorized changes is that they could adversely impact the security or functionality of the impacted assets. The risk associated with failing to update baselines within the required timeframe is that the entity may have incorrect or outdated information to appropriately analyze future changes. In this case, the risk posed by this noncompliance is not minimal because the impacted assets [redacted] perform critical security functions on high impact Bulk Electric System Cyber Assets at three entities. The risk was mitigated in this case by the fact that, in most cases, the entity identified and corrected these errors within a reasonable time following the 30 day deadline. ReliabilityFirst also notes that, during the period of noncompliance, no changes occurred on the impacted devices. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances either arose from different causes or because ReliabilityFirst determined that the conduct at issue constituted high frequency conduct that the entity quickly detected and corrected.
Mitigation	To mitigate this noncompliance, the entity: 1) conducted a meeting with the compliance team staff. The key manager for the group, and staff managers, strongly emphasized the criticality of ensuring changes are properly reviewed, authorized, and evidenced; 2) conducted in-person training to members of the compliance team to review process for baseline reviews/updates. Class included a hands-on review/baseline update of actual changes; 3) completed baseline updates to the impacted issues; 4) conducted a meeting with relevant staff to emphasize the importance of effective change management. The key manager for the group, and staff managers, strongly emphasized the criticality of ensuring changes are properly reviewed, authorized, and evidenced; 5) conducted in person training to members of the compliance team assigned to CIP changes on proper NERC CIP change management procedures; 6) [redacted]; 7) added a field in the database to note when baseline evidence is due [redacted] 8) conducted extent of condition review from Q3 2016 to July 2017 to identify additional change management issues for relevant staff; and 9) conducted a quality review and sampling of change tickets 90 days from the last corrective completion date to evaluate if changes are updated to Pending Production status within [redacted]. ReliabilityFirst has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018006	CIP-010-2	R1	[redacted]	[redacted]	11/2/2016	7/14/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On July 14, 2017, the entity submitted a Self-Report stating that, as a [redacted] and [redacted], it was in noncompliance with CIP-010-2 R1. During periodic baseline reviews, [redacted] identified five issues with its change management and baseline updating process. Two of these changes involved changes to switches and the remaining three changes involved firewall updates or changes to a firewall manager. In four instances, a change was completed without proper authorization. Because the change management application triggers the need for baseline updates, there were no immediate notifications that a baseline update was required. Consequently, the baselines were not updated within 30 calendar days of completing the change as required by CIP-010-2 R1 [redacted]. In the fifth instance, a change was properly authorized and completed, but the responsible individual failed to update the baseline within the required time frame [redacted]. The root cause of this noncompliance was two-fold. First, the four instances involving improper change management were the result of the responsible individuals failing to properly execute the change management process either due to a lack of understanding or oversight. Second, the instance involving only the late baseline update was the result of the responsible individual failing to follow the baseline update process due to insufficient awareness. This noncompliance started on November 2, 2016, when the first change was made, and ended on July 14, 2017, when [redacted] made the last update to the impacted baselines.
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 making unauthorized changes is that they could adversely impact the security or functionality of the impacted assets. The risk associated with failing to update baselines within the required timeframe is that the entity may have incorrect or outdated information to appropriately analyze future changes. In this case, the risk posed by this noncompliance is not minimal because the impacted assets [redacted] perform critical security functions on high impact Bulk Electric System Cyber Assets at three entities. The risk was mitigated in this case by the fact that, in most cases, the entity identified and corrected these errors within a reasonable time following the 30 day deadline. ReliabilityFirst also notes that, during the period of noncompliance, no changes occurred on the impacted devices. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances either arose from different causes or because ReliabilityFirst determined that the conduct at issue constituted high frequency conduct that the entity quickly detected and corrected.
Mitigation	To mitigate this noncompliance, the entity: 1) conducted a meeting with the compliance team staff. The key manager for the group, and staff managers, strongly emphasized the criticality of ensuring changes are properly reviewed, authorized, and evidenced; 2) conducted in-person training to members of the compliance team to review process for baseline reviews/updates. Class included a hands-on review/baseline update of actual changes; 3) completed baseline updates to the impacted issues; 4) conducted a meeting with relevant staff to emphasize the importance of effective change management. The key manager for the group, and staff managers, strongly emphasized the criticality of ensuring changes are properly reviewed, authorized, and evidenced; 5) conducted in person training to members of the compliance team assigned to CIP changes on proper NERC CIP change Management procedures; 6) [redacted]; 7) added a field in the database to note when baseline evidence is due [redacted] 8) conducted extent of condition review from Q3 2016 to July 2017 to identify additional change management issues for relevant staff; and 9) conducted a quality review and sampling of change tickets 90 days from the last corrective completion date to evaluate if changes are updated to Pending Production status within [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
RFC2018019050	CIP-010-2	R1	[redacted]	[redacted]	7/1/2016	1/31/2018	Self-Report	Completed
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On January 11, 2018, [redacted] submitted a Self-Report stating that, as a [redacted] and [redacted], it was in noncompliance with CIP-010-2 R1. The entity uses a Standard Configuration Guide as its location for authoritative baseline configuration information. On December 17, 2015, new Industrial Defender, Advanced Services Appliances (ASA), and Network Intrusion Detection Service (NIDS) devices were installed at an entity substation. On February 7, 2017, during a Cyber Vulnerability Assessment (CVA), the entity discovered that, while Industrial Defender contained all relevant baseline information for these devices, the entity did not update its Standard Configuration Guide, which the entity used as its authoritative source and location for baseline configuration information for all devices. For the devices at issue, the Standard Configuration Guide was not updated to reflect certain software that was specific to these devices at this substation. The root cause of this noncompliance was a failure in the manual part of the baseline management process. (In its mitigation plan, the entity states that it transitioned to an automated process within ID to manage baselines.) This major contributing factor involves the management practice of asset and configuration management, which includes establishing inventory and configuration baselines. This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-010-2 R1 and ended on January 30, 2018, when the entity updated the SCG baselines for all affected devices.						
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 in this case is that by not documenting baselines, the entity could apply future changes that could adversely affect system-to-system communications or break communication paths between Operational Technology and Information Technology devices. This could prevent hardware and software from communicating in proper manner, loss of devices, or otherwise open unneeded ports. This risk was mitigated in this case by the fact that the baselines contained in Industrial Defender were accurate and up-to-date. Furthermore, the entity's defense-in-depth strategy protects the devices at issue behind multiple firewalls and two-factor authentication, preventing exploitation from an attacker. 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 ReliabilityFirst has determined that this conduct constitutes high frequency conduct and the entity identified this noncompliance through its internal detective controls.						
Mitigation	To mitigate this noncompliance, the entity: 1) corrected the Standard Configuration Guide to include the items that were in conflict with the Industrial Defender baseline; 2) added 35-day baseline monitoring for Medium-Impact Electronic Access Control & Monitoring System (EACMS); 3) added 35-day baseline monitoring for Medium-Impact EACMS to monitoring process procedure(s); 4) corrected the Standard Configuration Guide to include the items that were in conflict with the Industrial Defender baseline; 5) modified the entity IT NERC CIP Authoritative Baseline Management and Approval document to ensure that devices which support baseline maintenance in Industrial Defender are tracked there; and 6) communicated changes of process, procedures and program updates to affected personnel.						

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2018019119	CIP-010-2	R3	[redacted]	[redacted]	2/7/2017	12/18/2017	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 January 26, 2018, [redacted] submitted a Self-Report stating that, as a [redacted] and [redacted], it was in noncompliance with CIP-010-2 R3. During its 2017 Cyber Vulnerability Assessment (CVA), the entity discovered that the same devices from [redacted] (i.e., new Industrial Defender, Advanced Services Appliances (ASA), and Network Intrusion Detection Service (NIDS) devices) had been missed during the 2017 CVA. Therefore, they were not entered into the remediation action tracking plan that resulted from that CVA. The entity identified this miss on September 22, 2017, and corrected the issue by following through on remediation efforts on December 18, 2017. The root cause of this noncompliance was a lack of clarity in the corporate process that defines roles for tracking during the CVA. Additionally, miscommunication among responsible groups occurred while entering actions into action tracking at the completion of the CVA and resulted in the miss. This noncompliance started on February 7, 2017, when the entity was required to have included these items in its annual CVA and ended on December 18, 2017, when the entity completed the remediation efforts.
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 in this case is that failing to include these devices in the annual CVA increases the likelihood that corrective actions are either delayed or missed. This risk was mitigated in this case because the corrective actions at issue in this case involved aligning baseline configurations in multiple sources or databases. The entity employs parallel processes (i.e., Industrial Defender) to verify the baselines of these assets to ensure that there were no unauthorized changes. The baselines contained in Industrial Defender were accurate and up-to-date. Furthermore, the entity's defense-in-depth strategy protects the devices at issue behind multiple firewalls and two-factor authentication preventing exploitation from an attacker. No harm is known to have occurred. While the mitigation is pending, the entity is reducing the risk posed by this noncompliance by performing parallel processes to verify the baselines of these assets to ensure that no unauthorized changes occur. 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 ReliabilityFirst has determined that this conduct constitutes high frequency conduct and the entity identified this noncompliance through its internal detective controls.
Mitigation	To mitigate this noncompliance, the entity: 1) ensured that the 2017 CVA Report has all action items and CVA Action Plan ownership assigned; 2) conducted an internal meeting to discuss changes to NERC CIP Cyber Vulnerability Assessment Process RC-AC-PCS3-011 and NERC CIP Vulnerability Assessment Procedure RC-AC-PCD3-013; 3) updated NERC CIP Cyber Vulnerability Assessment Process RC-AC-PCS3-011 and NERC CIP Vulnerability Assessment Procedure RC-AC-PCD3-013 to clearly define roles and responsibilities and to document the Action Plan maintenance and tracking activities; 4) generated a training deck on the updated CVA documents; 5) provided training to individuals responsible for implementing CVA Action Plans.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date
TRE2017016866	CIP-010-2	R1	[redacted]	[redacted]	July 1, 2016	August 31, 2017	Self-Report	January 19, 2018
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	[redacted], during a Compliance Audit, [redacted] submitted a Self-Report to Texas RE stating that, [redacted], it was in noncompliance with CIP-010-2 R1. In particular, [redacted] stated that it did not develop baseline configurations as required by CIP-010-2 R1, Part 1.1. Additionally, during the Compliance Audit, Texas RE determined that [redacted] failed to provide sufficient documentation to demonstrate compliance with the baselining requirements of CIP-010-2 R1, Parts 1.2 through 1.4. During the transition to CIP Version 5 NERC Reliability Standards, [redacted] implemented a software tool for compliance with CIP-010-2 R1. Subsequently, [redacted], [redacted] discovered the noncompliance during a mock audit conducted by a third-party. [redacted] determined that the software tool used for compliance with CIP-010-2 R1 [redacted] ended the noncompliance by implementing a [redacted] The root cause of this noncompliance was an insufficient process to ensure compliance with CIP-010-2 R1. Specifically, the software tool [redacted] used for compliance with CIP-010-2 R1 did not adequately document baseline configurations and [redacted]. This noncompliance started on July 1, 2016, when CIP-010-2 R1 became enforceable, and ended on August 31, 2017, when [redacted] implemented a new software tool for compliance with CIP-010-2 R1.						
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. Although the noncompliance was discovered by [redacted] approximately three months after the start of the noncompliance, the duration of the noncompliance was approximately 14 months. Further, the noncompliance impacted all of the Cyber Assets associated with [redacted] Medium Impact BES Cyber Systems – [redacted]. However, the risk to the reliability of the BPS was reduced because of the following factors. First, while [redacted] does not have documentation to demonstrate compliance with CIP-010-2 R1, Parts 1.1 through 1.4, [redacted] stated that for the time period at issue it had [redacted]. Second, [redacted] also stated that changes to Cyber Assets were required to go through its [redacted]. Third, [redacted] does not own generation and is a small entity that operates approximately [redacted] transmission lines. No harm is known to have occurred.						
Mitigation	To mitigate this noncompliance, [redacted]: 1) documented baseline configurations by implementing a new software tool that has the required functionalities to ensure compliance with CIP-010-2 R1; and 2) updated its process documentation to reflect the implementation of its new software tool. Texas RE has verified the completion of all mitigation activity.						

COVER PAGE

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the 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.

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
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.					