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 Find, Fix, Track, and Reports 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	RFC2017018742	Yes		Yes	Yes		Yes		Yes		Yes	Yes		Category 1: 3 years Category 2 – 12: 2 years
2	RFC2017017767	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
3	RFC2018019776	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
4	RFC2018019904	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years Category 2 – 12: 2 years
5	RFC2017018129	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
6	RFC2017018130	Yes		Yes	Yes		Yes							Category 1: 3 years Category 2 – 12: 2 years
7	RFC2016016432	Yes	Yes	Yes	Yes	Yes	Yes		Yes		Yes	Yes		Category 1: 3 years Category 2 – 12: 2 years
8	RFC2017018649	Yes		Yes	Yes		Yes		Yes		Yes	Yes		Category 1: 3 years Category 2 – 12: 2 years
9	RFC2017017734	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
10	RFC2018019775	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
11	RFC2019022594	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
12	RFC2019022103	Yes	Yes	Yes	Yes		Yes			Yes				Category 1: 3 years Category 2 – 12: 2 years
13	FRCC2019021605			Yes	Yes	Yes	Yes		Yes	Yes	Yes			Category 2 – 12: 2 years
14	WECC2018020009			Yes	Yes				Yes	Yes	Yes			Category 2 – 12: 2 years
15	WEC20180200010			Yes	Yes					Yes	Yes			Category 2 – 12: 2 years
16	WECC2017018181	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
17	WECC2017018850	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years

Filing Date: August 31, 2020

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
RFC2017018742	CIP-010-2	R3	[redacted]	[redacted]	7/1/2016	11/24/2017	Self-Report	Completed

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

On November 27, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [redacted], it was in noncompliance with CIP-010-2 R3. This noncompliance includes multiple instances.

First, on September 1, 2017, as a result of providing evidence for the [redacted] discovered that a [redacted] could not be found for a server. Based on a review of available [redacted], the entity lead investigator determined that the server in question was likely in production for a longer period of time that predates the most recent [redacted] that was completed in October 2016. The entity further determined from related activities on the server build process and the series of activities leading up to the discovery of this violation that the [redacted] was likely performed in October 2016, but not documented. The entity also determined that the server was missing a patch.

Second, on September 22, 2017, as a result of providing evidence for the [redacted], the entity discovered that two of the 14 sampled [redacted] did not have [redacted] performed prior to being placed into a production environment. Both Cyber Assets went into production on July 13, 2016. The entity did not previously self-report this issue because the entity incorrectly assumed the devices were to be governed under CIP v3 Standards. After further review, the entity determined that this incident was a violation because the entity put the Cyber Assets into production after CIP v5 went into effect.

This noncompliance involves the management practices of work management, asset and configuration management, and verification. The entity was not aware of what devices would be governed by CIP v5 in relation to performing [redacted] The root cause is ineffective work management as the entity did not ensure that all [redacted] were timely and properly performed.

These noncompliances started on July 1, 2016, the date the entity was required to comply with CIP-010-2 R3. The violation ended on November 24, 2017, the date the entity completed [redacted] for all of the affected 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 based on the following factors. The risk posed is the exposure of BES Cyber System assets to security vulnerabilities resulting from the delay or failure to perform [redacted] The risk is increased because these were discovered during a [redacted] in response to questions and requests for information from the [redacted]. For the first instance, the risk was somewhat mitigated because although pre-production [redacted] were not completed, other security controls were completed prior to the affected devices being added to the Electronic Security Perimeter, including conducting baselines for installed software and ports and services and updating the devices to ensure compliance. [redacted] for these devices were completed as part of the annual [redacted] in CIP-010-2 R3.1. For the second instance, indirect references to thorough completion of [redacted] exist for the majority of daily tasks executed by SMEs, which makes it likely that the [redacted] were actually performed, but not documented. No harm is known to have occurred.

The entity has no prior violations.

Mitigation

To mitigate this noncompliance, the entity:

1) performed the [redacted] related to the identified server;
2) reviewed the server build requirements for the identified server;
3) defined the remediation plan for the identified server as determined by the assessment and implemented the patch;
4) executed the needed patch and completed the [redacted] for the identified server; and
5) initiated the following preventive measures to reduce/eliminate reoccurrence of issues:
   a. (1.1.) Commencing immediately, for all new [redacted], the [redacted] will manually add appropriate tasks to the [redacted] through [redacted] for all NERC CIP servers. Such activity will take into consideration all [redacted] related to [redacted] such as but not limited to [redacted]
   b. (1.2.) When it is determined by the [redacted] that a [redacted] will require the requested server to be located within an [redacted] the needed tasks for that build will be added from the recipe of tasks enumerated in the [redacted].
   c. (1.3.) Security vulnerability scans for the [redacted] will be executed before and after the [redacted] goes into the ESP and the results therefrom attached to each task, similar to the way it is done for the servers so the evidence could be retrieved for an [redacted]. [redacted] will automatically capture that a manager has reviewed the build tasks.

To mitigate the noncompliance, the entity also:

1) performed [redacted] for the affected Cyber Assets;
2) performed an extent of condition review of all Cyber Assets that went into production after July 1, 2016, to ensure that a pre-production [redacted] were performed. The extent of condition discovered five

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
RFC2017018742	CIP-010-2	R3	[redacted]	[redacted]	7/1/2016	11/24/2017	Self-Report	Completed

additional devices that were added to a production environment without conducting a pre-production [redacted]. These five devices had the same root cause in that the entity built devices and authorized change requests using processes built for CIP v3 Standards and the devices went into production shortly after CIP-010-2 R3.3 and the CIP v5 Standards went into effect on July 1, 2016. After discovery, the entity completed active [redacted] for the five devices;

3) conducted a compliance stand down meeting to re-enforce the CIP-010-2 R3.3 [redacted] requirement and the mandatory use of the [redacted]. The [redacted] will also provide instruction to the [redacted] for how to properly complete the [redacted]
4) developed a preventative internal control to ensure the [redacted] is completed prior to devices being placed in a production environment. The preventative control will be the completion of a commissioning checklist to verify that the required [redacted] is completed prior to placing the [redacted] into production. The [redacted] and the [redacted] will be associated to the [redacted], which is used to authorize the introduction of the new device. The [redacted] will also include peer review and management level approval before the device is placed into the [redacted]; and
5) implemented the preventative control developed in Milestone 4.

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
RFC2017017767	CIP-011-2	R1	[redacted]	[redacted]	7/1/2016	8/3/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On June 12, 2017, the entity submitted Self-Report to ReliabilityFirst stating that, as a [redacted], it was in noncompliance with CIP-011-2 R1. During the course of a [redacted], a spreadsheet containing Bulk Electric System (BES) Cyber System Information (BCSI) was mistakenly sent to all project team members via an email distribution list. The information was provided in the form of a spreadsheet that was required for testing of upload into [redacted] During a team training exercise and discussion of what is protected information and who can access it, an entity employee on the [redacted] realized that they had recently received this type of protected information via email in a spreadsheet. The [redacted] had received this e-mail from a [redacted] as part of the [redacted]. The spreadsheet was a template with specific fields to be uploaded in to [redacted], [redacted] The project team member that emailed the spreadsheet made the assumption that all [redacted] had access to the information since [redacted] is the system of record for some protected information. The entity determined, however, that six members of the [redacted] did not have [redacted]. The six team members did not have any other privileges or NERC CIP training. The six team members did, however, have valid personnel risk assessments (PRAs). In addition, the spreadsheet was not labeled [redacted] This noncompliance involves the management practices of workforce management and verification. The root cause is ineffective training as the project team member that emailed the spreadsheet with BCSI incorrectly assumed that all [redacted] had access to and were authorized to view BCSI. Verification is involved because the employee did not verify that his assumption was correct before sending the email out to other [redacted]. The noncompliance started on July 1, 2016, the date the entity was required to comply with CIP-011-2 R1 and ended on August 3, 2017, the date the entity employees permanently deleted the email with the BCSI.
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 this noncompliance arises from allowing unauthorized individuals to view BCSI and that could lead to misuse of the BCSI. The risk is not minimal because of the long, more than one year duration. The risk is minimized because the data at issue was shared with trusted internal entity contractors and employees and was not shared externally. Only six individuals were not authorized to view the information and those six individuals all had valid PRAs. The information, itself, could not have resulted in the loss of BES assets directly. The email was contained completely within the entity network. No harm is known to have occurred. The entity has prior violations. ReliabilityFirst did not consider certain prior violations repeat infractions, in part, because of the amount of time that has passed since mitigation was completed for said violations, which supports the conclusion that processes and systems have evolved such that the current issues are not a result of a failure to mitigate the prior issues. ReliabilityFirst notes that some of the prior violations involved different facts, circumstances, and/or causes. Other violations resolved within this FFT arguably involve similar conduct as some of the prior violations. However, the current violation poses a lesser risk and demonstrates the entity's ability to identify and correct noncompliances, ReliabilityFirst will not consider the prior violations as an aggravating factor.
Mitigation	To mitigate this noncompliance, the entity: 1) received a written attestation regarding request for deletion of email and subject document for [redacted] and 2) released updated training course requirements for all employees and contractors. Training included identification and classification of BCSI and protection of BSCI in use, transit and storage. 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
RFC2018019776	CIP-011-2	R1	[redacted]	[redacted]	7/20/2017	3/9/2018	Self-Report	Completed

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

On May 22, 2018, [redacted] submitted a Self-Report to ReliabilityFirst stating that, as a [redacted], it was in noncompliance with CIP-011-2 R1. This noncompliance contains two instances.

First, on July 20, 2017, an entity employee sent an [redacted] an unencrypted email that contained confidential Bulk Electric System (BES) Cyber System Information (BSCI) while working with the [redacted] on a project involving a [redacted] The entity employee sent the [redacted] the [redacted] so they could discuss the design plan of the project work while both viewing the [redacted]. The diagram contained [redacted]

The vendor recipient had a "need to know" as well as a completed personnel risk assessment (PRA) which is required to obtain access to BCSI. The [redacted] also completed the entity's NERC CIP training. The [redacted] was working with the employee on a contracted engagement for construction work involving the [redacted]. The entity's detection software, [redacted] triggered a flag based upon predetermined words and or phrases when the email was sent. The email was logged, a copy made and quarantined, then sent on to the recipient in an unencrypted state. The entity discovered this mistake during the standard process of reviewing log files conducted by the [redacted]. That discovery and review occurred on August 1, 2017.

Second, on March 9, 2018, an entity employee was gathering baseline information for the [redacted]. While doing this task, he inadvertently sent an email externally without encryption when he failed to manually add the required [redacted] statement on the email Subject Line in order to encrypt the email. The email he sent should have been encrypted. The employee emailed himself a document containing [redacted] so that he could continue working on gathering the baseline information while working on his corporate laptop after he disconnected from the network. The employee sent the email from his corporate account to his private email account in violation of the entity's policy and procedure. The email contained 52 assets names ([redacted]

The entity discovered this violation while using its [redacted]. The entity [redacted] discovered the email during their periodic verification of flagged emails. This email contained SCADA data deemed "[redacted]."

This noncompliance involves the management practices of workforce management and work management. The root cause was entity personnel's lack of awareness of the entity's [redacted] Specifically, entity personnel did not understand that encryption is a manual process that the user needs to invoke when emails are used for sharing and transporting BCSI. Although the employee at issue was aware of the [redacted] and had taken the required annual [redacted] the employees had inadequate awareness of the encryption process.

The noncompliance started on July 20, 2017, the date the entity employee sent the [redacted] to the vendor's email. The noncompliance ended on March 9, 2018, the date the entity employee in the second instance deleted the email and attachment from all his email account folders after sending the email to himself.

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 is allowing a potential bad actor access to BCSI thereby compromising BPS security. The risk is somewhat mitigated for the first instance because of the short, 12 day duration and the information was sent to a vendor with a right to view the information who had a valid PRA and up to date NERC CIP Training. For the second instance, the risk is somewhat mitigated because of the short, one day duration. Additionally, the sender was both the sender and recipient and immediately deleted the email after discovering the mistake. Lastly, the sender had a valid PRA and up-to-date NERC CIP training. No harm is known to have occurred.

The entity has prior violations. ReliabilityFirst did not consider certain prior violations repeat infractions, in part, because of the amount of time that has passed since mitigation was completed for said violations, which supports the conclusion that processes and systems have evolved such that the current issues are not a result of a failure to mitigate the prior issues. ReliabilityFirst notes that some of the prior violations involved different facts, circumstances, and/or causes. Other violations resolved within this FFT arguably involve similar conduct as some of the prior violations. However, the current violation poses a lesser risk and demonstrates the entity's ability to identify and correct noncompliances, ReliabilityFirst will not consider the prior violations as an aggravating factor.

Mitigation

To mitigate this noncompliance, the entity:

1) confirmed that the recipient deleted the email and attachment (Incident 1). The entity also deleted the email from the subject matter expert's personal, external email account and checked all email folders to ensure no remnants of the email existed (Incident 2);
2) added a [redacted]. Each [redacted] will contain information about a NERC CIP requirement and what the reader should do to ensure compliance with the requirement. Each month a new article will be submitted and included in the [redacted] that is sent via email to all employees as well as be available via internal website. This can be validated for any direct email sent using [redacted]. This will allow us to find out how many people an email was sent to, how long they interacted with it and what device they used to access it;
3) designed and implemented a rule set within the [redacted] to identify and block attempts to send outbound, unencrypted email(s) that are themselves, or include attachments that are, classified as "[redacted]", including variants of such phrase. Blocked attempts will include an auto-response notification to the sender alerting to the proper method of encrypting

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
RFC2018019776	CIP-011-2	R1	[redacted]	[redacted]	7/20/2017	3/9/2018	Self-Report	Completed

outbound email transmissions and auto-encryption of the email. Repeated attempts to send outbound, email transmissions classified as [redacted]" will be reviewed and, if appropriate, result in escalation to management;

4) developed an endpoint data classification tool to assist in the classification of company documents, including BCSI, and reinforcing guidelines on the proper labeling of documents actively managed in [redacted]

5) [redacted] and

6) deployed the data classification tool to all company-issued workstations and laptops that have authenticated access to the entity network.

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
RFC2018019904	CIP-002-5.1	R1	[redacted]	[redacted]	7/1/2016	12/13/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On June 7, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [redacted], it was in noncompliance with CIP-002-5.1 R1. In 2013, the entity installed approximately [redacted] These devices are for manual operation only and are necessary because the switches are so large, making manual cranking not possible or desirable. The [redacted]. Prior to July 1, 2016, the entity determined, based on the drawings provided by the vendor that the devices did not fall within the definition of a Bulk Electric System (BES) Cyber Asset and therefore did not protect the devices accordingly. These devices should have been classified as [redacted] The entity, however, did not have the [redacted] applicable to [redacted] in place for these devices because the entity incorrectly believed the devices were not BES Cyber Assets. As background, in the initial analysis, the entity determined that the [redacted] for these devices could not initiate an open [redacted]; the controls just level the speed once it is in motion. Based off of this analysis and the initial drawings, the entity did not believe the devices fell within the definition of BES Cyber Assets. However, in 2018, the entity determined that the [redacted] could accept [redacted], [redacted] Likewise, the devices could be programed, and affect downstream devices. In addition, the devices, if misused, could prevent operation of the facility. Therefore, the devices are BES Cyber Assets. This noncompliance involves the management practice of asset and configuration management. The root cause for this noncompliance is the fact that when the initial evaluation was done, the entity used drawings that were incorrect, causing the entity to not include these devices as BES Cyber Assets. Verification is involved because the entity did not verify that they were using the correct drawings. This noncompliance started on July 1, 2016, the date the entity was required to comply with CIP-002-5.1 R1. The noncompliance ended on December 13, 2018, the date the entity classified and protected these devices as BES 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 (BPS) based on the following factors. The risk posed by this noncompliance is that not identifying (and thus not protecting) these switches makes it easier to exploit these devices and potentially harm the BPS. The risk is not minimal because the entity did not have the [redacted] without [redacted] in place for these devices. The risk is lessened because the only way to manipulate these devices is to make adjustments directly on the devices; the devices do not have [redacted] Additionally, these devices were located in the station yard at [redacted] and physical access to the devices was restricted by the perimeter fence and lock at each substation. No harm is known to have occurred. The entity has no prior violations.
Mitigation	To mitigate this noncompliance, the entity: 1) secured the devices by [redacted]; 2) communicated the actions taken to station personnel; 3) will use another vendor to purchase such devices; 4) performed an extent of condition and found no additional instances; 5) enhanced and documented an annual review collaboration meeting to reaffirm exclusions; and 6) created a checklist to be used before installing equipment in BES facilities. 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
RFC2017018129	CIP-004-6	R4	[redacted]	[redacted]	7/1/2016	12/6/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On August 1, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [redacted], it was in noncompliance with CIP-004-6 R4. This noncompliance involves three separate instances. First, on September 7, 2016, the entity discovered that 6 employees had been given Administrator privileges to [redacted] without prior authorization, as required. The incident occurred because the access was provisioned at the server level rather than domain level. The discrepancy was not identified by the daily automated control which reconciles domain level access against the entity's access management system. An entity system administrator reviewing system permissions on an Electronic Access Control Monitoring System (EACMS) identified anomalies between users provisioned locally on the asset and the users provisioned access to the asset using [redacted] The entity removed access for 2 of the employees and reauthorized access for 4 of the employees as of September 22, 2016. Second, on September 14, 2016, the entity discovered that access to an EACMS had not been properly attributed in accordance with the entity's access management program. This incident is the result of a gap in the process of implementing access management for assets that were brought into CIP scope as a part of the transition from CIP v3 to CIP v5. Here, roles that provide electronic access to the EACMS were not designated as Bulk Electric System (BES) Cyber System related access; the processes and controls for BES Cyber System access were not applied. The error was corrected on September 27, 2016, after which access to that system was properly classified and managed as required for an EACMS. The entity discovered this instance when a review of the entity's [redacted] identified that access to an EACMS associated with a [redacted] was erroneously configured as non-CIP access. This was detected because a manager reported an anomaly when he did not see the EACMS access that he expected to see on a staff member's access profile. The investigation of the missing access role determined the issue was with the configuration of the EACMS access roles in the entity's electronic access management system. Third, on October 13, 2016, the entity discovered that an application used to view vulnerabilities on BES Cyber Assets was not managed and monitored as a BES Cyber System Information (BCSI) storage location per CIP-004 R4.1.3. The entity failed to ensure that access to the application was managed in accordance with the entity's [redacted]. This incident is the result of a gap in the process of implementing access management for assets that were brought into CIP scope as a part of the transition for CIP v3 to CIP v5. The attributes of the repository were not adjusted accordingly when the assets were brought into scope. The entity discovered this instance while it conducted a review of locations designated as BCSI repositories. During that review, the entity identified a system known to contain BCSI missing from the repository list. This noncompliance involves the management practices of planning, reliability quality management, and implementation. The root cause is the entity ineffectively preparing to ensure there were no gaps as it transitioned from CIP v3 compliance to CIP v5 compliance. The entity also did not have effective controls in place to ensure that all personnel followed the entity's [redacted] The violation began on July 1, 2016, the date the entity was required to comply with CIP-004-6 R4 because an application used to view vulnerabilities on BES Cyber Assets was not managed and monitored during the transition from CIP v3 to CIP v5 and ended on December 6, 2017, the date the entity finished revoking all improperly given access and began managing and monitoring the application used to view vulnerabilities on BES Cyber Assets as a BCSI storage location.
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 this noncompliance is allowing unauthorized personnel to access BES Cyber Systems or BCSI which could lead to the compromise of the entity's systems. The risk is minimized because with regard to unauthorized access, the provisioned access was needed by each employee. In all instances, the employees had a valid Personnel Risk Assessment (PRA) and had completed the required NERC CIP training. For the first incident, the individuals needed the Administrator privileges to do their job. With regard to the EACMS, the entity afforded the EACMS all of the required protections per the CIP Standards. With regard to the application being a BSCI location, the users of the application can only scan and pull data from BES Cyber Systems; no other action that could affect a BES Cyber System is possible. No harm is known to have occurred. The entity has prior violations. ReliabilityFirst did not consider certain prior violations repeat infractions, in part, because of the amount of time that has passed since mitigation was completed for said violations, which supports the conclusion that processes and systems have evolved such that the current issues are not a result of a failure to mitigate the prior issues. ReliabilityFirst notes that some of the prior violations involved different facts, circumstances, and/or causes. However, the current violation poses a lesser risk and demonstrates the entity's ability to identify and correct noncompliances, ReliabilityFirst will not consider the prior violations as an aggravating factor.
Mitigation	To mitigate this noncompliance, the entity: 1) corrected the reported issues; 2) amended the [redacted] change management process by adding steps to evaluate access impacts; 3) performed an extent of condition within [redacted]; 4) developed and implemented a process to ensure consistency in how access is provisioned; and

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
RFC2017018129	CIP-004-6	R4	[redacted]	[redacted]	7/1/2016	12/6/2017	Self-Report	Completed
			5) created, piloted and implemented a detective control. Also as part of mitigation, the entity modified its change management process to perform an access and a BSCI evaluation when new devices are onboarded to ensure that access is properly attributed in the entity's access management system and BCSI repositories are properly identified. 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
RFC2017018130	CIP-004-6	R5	[redacted]	[redacted]	7/1/2016	7/23/2019	Self-Report	Completed

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

On August 1, 2017 and January 27, 2020 the entity submitted Self-Reports to ReliabilityFirst stating that, as a [redacted], it was in noncompliance with CIP-004-6 R5. This noncompliance involves seven instances of noncompliance.

The entity runs a [redacted] to verify whether or not employees that no longer require NERC CIP cyber or physical access have had their access removed within the required time frame. Six of the seven discrepancies were found as a result of reviewing this report, which is used as a detective control. The seventh incident was discovered as a part of a [redacted], which is another detective control.

First, on July 25, 2016, the entity discovered that electronic access for an employee that was transferred to a different department was not revoked within a calendar day after the employee no longer required such access. The entity should have completed the revocation on July 23, 2016, but did not complete the revocation until July 25, 2016.

Second, on September 8, 2016, the entity discovered that an employee's electronic access had not been revoked within a calendar day after the employee no longer required such access. The entity should have completed the revocation on September 7, 2016, but did not complete the revocation until September 8, 2016.

Third, on October 10, 2016, the entity discovered that an employee's electronic access had not been revoked within a calendar day after the employee no longer required such access. The entity should have completed the revocation on October 8, 2016, but did not complete the revocation until October 10, 2016.

Fourth, on October 28, 2016, the entity discovered that an employee's physical and electronic access had not been revoked within a calendar day after the employee no longer required such access. The employee's last day with the entity was on October 22, 2016 and the entity should have completed the revocation on October 23, 2016. [redacted] on October 22, 2016, but did not remove electronic and physical access until October 28, 2016.

Fifth, on January 4, 2017, the entity discovered that an employee's physical and electronic access had not been revoked within a calendar day after the employee no longer required such access. The employee transferred to a different department within the entity on December 17, 2016. The entity should have revoked physical and electronic access on December 18, 2016, but did not remove physical access until January 4, 2017 and did not revoke electronic access until January 9, 2017.

Sixth, on January 31, 2017, the entity discovered that an employee's physical access had not been revoked within a calendar day after the employee no longer required such access. The entity should have revoked physical access on February 1, 2017, but did not remove physical access until February 7, 2017.

Seventh, on June 16, 2017, the entity discovered that an employee's electronic access had not been revoked within a calendar day after the employee no longer required such access. The entity should have revoked electronic access on September 1, 2016. When the new version of the entity's access management system was implemented, however, this employee's access profile was not imported into the new system. This meant that when the transfer of the employee occurred, the employee's existing authorized electronic access was omitted from the transfer review process, which would have occurred on August 27, 2016. In this instance, the system owner rejected the user's access which led to the identification of the missing access issue in the entity's access management system. The entity did not remove the employee's access until June 19, 2017.

While performing an extent of condition connected with the Mitigation Plan, the entity discovered an additional seven instances of provisioned NERC CIP electronic access missing from the entity's [redacted] for access to the [redacted] (5 instances) and [redacted] (2 instances) [redacted] This means existing authorized electronic access was omitted from an employee's transfer review, quarterly certification process, and the access revocation process.

This noncompliance involves the management practices of implementation, validation, and verification. The entity did not implement its access revocation processes effectively as evidenced by the seven instances in this violation. The root cause is an ineffective validation and verification process as the entity did not confirm that it was timely revoking employee's physical and electronic access rights. (A contributing cause was determined to be that the request to remove access happened during a weekend in three instances 1, 3 and 4). In two of those instances, the revocation was processed the following business day. Employees were not aware that they should check their emails for notices of revocation during weekends or holidays. Regarding the employee who resigned (4), the manager collected everything from the employee on his last day; however, he did not take the additional step of notifying the [redacted]. Regarding the employees who transferred (2, 5 and 6), the employees' new manager reviewed and stated that the employees did not need the access. However, the person responsible for removing access missed the notification. In this case the emails requesting the revocations were missed by the employee responsible for removing the access. The cause for incident 7 was when the new version of the entity's asset management was implemented, the employee's [redacted] was not imported into the system. Therefore, it was omitted from the transfer review due to the access portion of asset not being migrated for CIP v5.)

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2017018130	CIP-004-6	R5	[redacted]	[redacted]	7/1/2016	7/23/2019	Self-Report	Completed
			The noncompliance started on July 1, 2016, the date the entity was required to comply with CIP-004-6 R5 and ended on July 23, 2019, the date the entity completed the last access revocation.					
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 this violation is allowing individuals to retain electronic and or physical access to Bulk Electric System (BES) Cyber Systems when those individuals are no longer authorized to have such access. The risk is not minimal because of the number of instances and the same causes for the first, third, and fourth instances (not checking emails over the weekend). The risk posed by this violation is not serious because each of the seven individuals involved in this violation remained employees except for one. During the noncompliance, each of the seven individuals had current Personnel Risk Assessments and the required annual CIP training. None of the seven instances were initiated by a cause for termination. For the one employee that left the entity, he left voluntarily, and the day he left the entity, his supervisor collected his [redacted] The risk is lessened for the seven individuals identified as part of the extent of condition because all seven impacted employees were in good standing with the entity for the duration of the noncompliance and were intended to maintain their NERC CIP electronic access. These actions significantly reduce the risk that any of the impacted individuals could gain unauthorized electronic or physical access to BES Cyber Systems. No harm is known to have occurred. The entity has prior violations. ReliabilityFirst did not consider certain prior violations repeat infractions, in part, because of the amount of time that has passed since mitigation was completed for said violations, which supports the conclusion that processes and systems have evolved such that the current issues are not a result of a failure to mitigate the prior issues. ReliabilityFirst notes that some of the prior violations involved different facts, circumstances, and/or causes. However, the current violation poses a lesser risk and demonstrates the entity's ability to identify and correct noncompliances, ReliabilityFirst will not consider the prior violations as an aggravating factor.					
Mitigation			To mitigate this noncompliance, the entity: 1) removed all cyber and/or physical CIP NERC access as soon as discrepancies were discovered; 2) sent an email communication to all [redacted] employees, re-emphasizing the importance of revoking all CIP access within the required time of the notice that the access is no longer needed; 3) held a stand down meeting with all [redacted] personnel responsible for removing access to ensure employees understood the obligation of the standard and what is required of each employee to meet such requirement. Additionally, the attendees were reminded of their responsibility to review email notifications over weekends or holidays as revocations can occur outside business hours; 4) amended the notification process to include the [redacted] provisioner and his/her manager along with the provisioner to receive the notification to revoke that is generated immediately upon a completion of an access review by a [redacted] who states that the access is no longer needed. This process includes an email notification improvement and provides pertinent information regarding the revoke request. In addition, it enables the manager to complete the task or reassign the task if the provisioner is unavailable; and 5) amended the relevant change management process to include the evaluation of access changes (additions, modifications or removals) resulting from changes to applicable BES Cyber System or Electronic Access Control or Monitoring Systems. 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
RFC2016016432	CIP-006-6	R1	[redacted]	[redacted]	7/1/2016	8/26/2016	Self-Report	Completed

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

On October 21, 2016, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [redacted], it was in noncompliance with CIP-006-6 R1. The entity submitted the Self-Report to ReliabilityFirst under an existing [redacted] There are two instances of noncompliance in this violation

First, on June 20, 2016, the entity discovered that the [redacted] was no longer reading badges, making it only a single factor form of authentication. At that time, a ticket was submitted with the [redacted] On June 29, 2016, the entity technician arrived on-site and determined that the reader could not be repaired and that a replacement one was needed. The [redacted] that were deployed were no longer available for purchase, so the entity decided to replace the [redacted]

As of July 1, 2016, CIP-006-6 R1.3 required two or more different physical access controls to collectively allow unescorted physical access into Physical Security Perimeters (PSPs). As a result of the [redacted] at issue no longer reading badges ([redacted]) beginning on June 20, 2016, the entity did not have two or more physical access controls in place for this door. Therefore, the entity was in noncompliance with CIP-006-6 R1.3 beginning on July 1, 2016.

On July 29, 2016, the entity installed and tested a [redacted]. The entity [redacted] directed his staff to leave the [redacted] off and advise everyone who had access to the room that they needed to set their [redacted]. [redacted] gave individuals until August 22, 2016 to set a [redacted] before turning the [redacted] This decision was based on the fact that entity [redacted] did not know the [redacted] of the room. During this time period, anyone with approved unescorted access only needed to present their card to the reader to gain access ([redacted]

On August 16, 2016, the entity became aware of the potential non-compliance with CIP-006-6 R1.3 and promptly enabled the two or more different physical access controls, bringing the entity back into compliance. During the data collection for the [redacted], a list of PSPs in scope was provided to entity [redacted]. On that list were several [redacted] in the [redacted] At that time, entity [redacted] contacted [redacted] to discuss why certain rooms were on the list and why they were considered [redacted]. The entity determined that these rooms, including the [redacted] at issue in this instance, had Cyber Assets inside that were included in [redacted]. At that time, [redacted] turned on the [redacted] feature which required two-factor authentication to enter the room.

Second, the entity became noncompliant with CIP-006-6 R1.3 for the [redacted] as of July 1, 2016. The entity identified this while completing an extent of condition as part of the Mitigation Plan for this noncompliance. On August 21, 2016, while collecting evidence of [redacted], entity [redacted] discovered that there was only a [redacted] installed on the main door for the [redacted]

On August 22, 2016, entity [redacted] confirmed the [redacted] contained Cyber Assets that support a [redacted] The [redacted] r immediately instructed his staff to get a [redacted]. On August 24, 2016, after realizing the vendor had brought the wrong part to complete the installation of the [redacted] implemented temporary controls to take the [redacted] offline and require anyone needing access to call the [redacted] and verify two factors ([redacted]) while the correct part was ordered. On August 26, 2016, the vendor arrived with the correct part and installed the [redacted] (two-factor) and the temporary controls were discontinued.

This noncompliance involves the management practices of asset and configuration management and verification. The root cause was that the entity did not verify whether or not the rooms contained assets that support [redacted] and therefore did not ensure that those rooms required multi-factor authentication for access.

The noncompliance started on July 1, 2016, the date the entity was required to comply with CIP-006-6 R1. The noncompliance ended on August 26, 2016, when the entity re-enabled two-factor authentication to end the second 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 based on the following factors. The risk posed by this violation is providing the opportunity to unauthorized personnel to more easily access Cyber Assets inside a PSP when multi-factor authentication is not required to gain access into a PSP. The risk is lessened in the first instance because the [redacted] was still active, requiring individuals to use an authorized card before permitting entry. Additionally, the building is located within the fenced area of the [redacted] The PSP was also monitored continuously. The risk is lessened in the second instance because the [redacted] was still active and the PSP was monitored continuously. The entity was still following the Physical Security Plan with the only exception being the lack of two-factor authentication. [redacted] No harm is known to have occurred.

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
RFC2016016432	CIP-006-6	R1	[redacted]	[redacted]	7/1/2016	8/26/2016	Self-Report	Completed
			The entity has prior violations. ReliabilityFirst did not consider certain prior violations repeat infractions, in part, because of the amount of time that has passed since mitigation was completed for said violations, which supports the conclusion that processes and systems have evolved such that the current issues are not a result of a failure to mitigate the prior issues. ReliabilityFirst notes that some of the prior violations involved different facts, circumstances, and/or causes. However, the current violation poses a lesser risk and demonstrates the entity's ability to identify and correct noncompliances, ReliabilityFirst will not consider the prior violations as an aggravating factor.					
Mitigation			To mitigate this noncompliance, the entity: 1) enabled two-factor authentication for the [redacted]; 2) completed extent of condition reviews to confirm the list of PSPs with [redacted] from each [redacted] and ensure two-factor is in place where required. The extent of condition review discovered the second instance [redacted] in this noncompliance and no others; 3) implemented temporary controls by taking the [redacted] offline and requiring anyone needing access to the [redacted] to call the [redacted] and verify two factors [redacted] 4) implemented preferred two-factor authentication for the [redacted] by installing the [redacted]; 5) implemented a procedural control by sending a memo to all applicable [redacted] to ensure that [redacted] is notified of the impact level of the BES Cyber Systems within the new PSP during the PSP commissioning process and that any changes to existing impact ratings impacting a PSP must be communicated to [redacted] prior to making those changes; 6) updated the entity [redacted] to include the new procedural control; and 7) designed and implemented a detective control to periodically validate the PSP impact ratings. 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
RFC2017018649	CIP-010-2	R3	[redacted]	[redacted]	7/1/2016	11/24/2017	Self-Report	Completion

Description of the Noncompliance (For purposes of this 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 2, 2017 and November 27, 2017, the entity submitted Self-Reports to ReliabilityFirst stating that, as a [redacted], it was in noncompliance with CIP-010-2 R3. This noncompliance includes multiple instances.

First, on September 1, 2017, as a result of providing evidence for the [redacted] discovered that a [redacted] could not be found for a server. Based on a review of available [redacted] the entity lead investigator determined that the server in question was likely in production for a longer period of time that predates the most recent [redacted] that was completed in October 2016. The entity further determined from related activities on the server build process and the series of activities leading up to the discovery of this violation that the [redacted] was likely performed in October 2016, but not documented. The entity also determined that the server was missing a patch.

Second, on September 22, 2017, as a result of providing evidence for the [redacted], the entity discovered that two of the 14 sampled [redacted] did not have [redacted] performed prior to being placed into a production environment. Both Cyber Assets went into production on July 13, 2016. The entity did not previously self-report this issue because the entity incorrectly assumed the devices were to be governed under CIP v3 Standards. After further review, the entity determined that this incident was a violation because the entity put the Cyber Assets into production after CIP v5 went into effect.

This noncompliance involves the management practices of work management, asset and configuration management, and verification. The entity was not aware of what devices would be governed by CIP v5 in relation to performing [redacted]. The root cause is ineffective work management as the entity did not ensure that all [redacted] were timely and properly performed.

These noncompliances started on July 1, 2016, the date the entity was required to comply with CIP-010-2 R3. The violation ended on November 24, 2017, the date the entity completed [redacted] for all of the affected 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 based on the following factors. The risk posed is the exposure of BES Cyber System assets to security vulnerabilities resulting from the delay or failure to perform [redacted]. The risk is increased because these were discovered during a [redacted] in response to questions and requests for information from the [redacted] For the first instance, the risk was somewhat mitigated because although pre-production [redacted] were not completed, other security controls were completed prior to the affected devices being added to the Electronic Security Perimeter, including conducting baselines for installed software and ports and services and updating the devices to ensure compliance. [redacted] for these devices were completed as part of the annual [redacted] requirement in CIP-010-2 R3.1. For the second instance, indirect references to thorough completion of [redacted] exist for the majority of daily tasks executed by SMEs, which makes it likely that the [redacted] were actually performed, but not documented. No harm is known to have occurred.

The entity has no prior violations.

Mitigation

To mitigate this noncompliance, the entity:

1) performed the [redacted] related to the identified server;
2) reviewed the server build requirements for the identified server;
3) defined the remediation plan for the identified server as determined by the assessment and implemented the patch;
4) executed the needed patch and completed the [redacted] for the identified server; and
5) initiated the following preventive measures to reduce/eliminate reoccurrence of issues:
    a. (1.1.) Commencing immediately, for all new [redacted], the [redacted] will manually add appropriate tasks to the [redacted] through [redacted] for all NERC CIP servers. Such activity will take into consideration all [redacted] related to [redacted] based [redacted] such as but not limited to [redacted]
    b. (1.2.) When it is determined by the [redacted] that a [redacted] will require the requested server to be located within an [redacted] the needed tasks for that build will be added from the recipe of tasks enumerated in the [redacted].
    c. (1.3.) Security vulnerability scans for the [redacted] will be executed before and after the [redacted] goes into the ESP and the results therefrom attached to each task, similar to the way it is done for the servers so the evidence could be retrieved for an [redacted] will automatically capture that a manager has reviewed the build tasks.

To mitigate the noncompliance, the entity also:

1) performed [redacted] for the affected Cyber Assets;
2) performed an extent of condition review of all Cyber Assets that went into production after July 1, 2016, to ensure that pre-production [redacted] were performed. The extent of condition discovered five

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
RFC2017018649	CIP-010-2	R3	[redacted]	[redacted]	7/1/2016	11/24/2017	Self-Report	Completion

additional devices that were added to a production environment without conducting a [redacted] These five devices had the same root cause in that the entity built devices and authorized change requests using processes built for CIP v3 Standards and the devices went into production shortly after CIP-010-2 R3.3 and the CIP v5 Standards went into effect on July 1, 2016. After discovery, the entity completed active [redacted] for the five devices;

3) conducted a compliance stand down meeting to re-enforce the CIP-010-2 R3.3 CVA requirement and the mandatory use of the [redacted] The [redacted] will also provide instruction to the [redacted] for how to properly complete the [redacted];
4) developed a preventative internal control to ensure the [redacted] is completed prior to devices being placed in a production environment. The preventative control will be the completion of a commissioning checklist to verify that the required [redacted] is completed prior to placing the [redacted] into production. The [redacted] will be associated to the [redacted], which is used to authorize the introduction of the new device. The [redacted] will also include peer review and management level approval before the device is placed into the [redacted] and
5) implemented the preventative control developed in Milestone 4.

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
RFC2017017734	CIP-011-2	R1	[redacted]	[redacted]	7/1/2016	8/3/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On June 6, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [redacted], it was in noncompliance with CIP-011-2 R1. During the course of a [redacted], a spreadsheet containing Bulk Electric System (BES) Cyber System Information (BCSI) was mistakenly sent to all project team members via an email distribution list. The information was provided in the form of a spreadsheet that was required for testing of upload into [redacted] During a team training exercise and discussion of what is protected information and who can access it, an entity employee on the [redacted] realized that they had recently received this type of protected information via email in a spreadsheet. The [redacted] had received this e-mail from a [redacted] as part of the CIP v5 transition project. The spreadsheet was a template with specific fields to be uploaded in to [redacted], including [redacted] The project team member that emailed the spreadsheet made the assumption that all [redacted] had access to the information since [redacted] is the system of record for some protected information. The entity determined, however, that six members of the [redacted] did not have [redacted]. The six team members did not have any other privileges or NERC CIP training. The six team members did, however, have valid personnel risk assessments (PRAs). In addition, the spreadsheet was not labeled [redacted]. This noncompliance involves the management practices of workforce management and verification. The root cause is ineffective training as the project team member that emailed the spreadsheet with BCSI incorrectly assumed that all [redacted] had access to and were authorized to view BCSI. Verification is involved because the employee did not verify that his assumption was correct before sending the email out to other [redacted]. The noncompliance started on July 1, 2016, the date the entity was required to comply with CIP-011-2 R1 and ended on August 3, 2017, the date the entity employees permanently deleted the email with the BCSI.
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 this noncompliance arises from allowing unauthorized individuals to view BCSI and that could lead to misuse of the BCSI. The risk is not minimal because of the long, more than one year duration. The risk is minimized because the data at issue was shared with trusted internal entity contractors and employees and was not shared externally. Only six individuals were not authorized to view the information and those six individuals all had valid PRAs. The information, itself, could not have resulted in the loss of BES assets directly. The email was contained completely within the entity network. No harm is known to have occurred. The entity has prior violations. ReliabilityFirst did not consider certain prior violations repeat infractions, in part, because of the amount of time that has passed since mitigation was completed for said violations, which supports the conclusion that processes and systems have evolved such that the current issues are not a result of a failure to mitigate the prior issues. ReliabilityFirst notes that some of the prior violations involved different facts, circumstances, and/or causes. Other violations resolved within this FFT arguably involve similar conduct as some of the prior violations. However, the current violation poses a lesser risk and demonstrates the entity's ability to identify and correct noncompliances, ReliabilityFirst will not consider the prior violations as an aggravating factor.
Mitigation	To mitigate this noncompliance, the entity: 1) received a written attestation regarding request for deletion of email and subject document for [redacted]; and 2) released updated training course requirements for all employees and contractors. Training included identification and classification of BCSI and protection of BSCI in use, transit and storage. 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
RFC2018019775	CIP-011-2	R1	[redacted]	[redacted]	7/20/2017	3/9/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On May 22, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [redacted], it was in noncompliance with CIP-011-2 R1. This noncompliance contains two instances. First, on July 20, 2017, an entity employee sent an [redacted] an unencrypted email that contained confidential Bulk Electric System (BES) Cyber System Information (BSCI) while working with the [redacted] on a project involving a [redacted]. The entity employee sent the [redacted] the [redacted] so they could discuss the design plan of the project work while both viewing the [redacted]. The diagram contained [redacted]. The vendor recipient had a "need to know" as well as a completed personnel risk assessment (PRA) which is required to obtain access to BCSI. The [redacted] also completed the entity's NERC CIP training. The [redacted] was working with the employee on a [redacted] for construction work involving the [redacted]. The entity's detection software, [redacted], triggered a flag based upon predetermined words and or phrases when the email was sent. The email was logged, a copy made and quarantined, then sent on to the recipient in an unencrypted state. The entity discovered this mistake during the standard process of reviewing log files conducted by the [redacted] That discovery and review occurred on August 1, 2017. Second, on March 9, 2018, an entity employee was gathering baseline information for the [redacted]. While doing this task, he inadvertently sent an email externally without encryption when he failed to manually add the required [redacted] in order to encrypt the email. The email he sent should have been encrypted. The employee emailed himself a document containing [redacted] so that he could continue working on gathering the baseline information while working on his corporate laptop after he disconnected from the network. The employee sent the email from his corporate account to his private email account in violation of the entity's policy and procedure. The email contained 52 assets names [redacted]) with their [redacted] The entity discovered this violation while using its [redacted]. The entity [redacted] discovered the email during their periodic verification of flagged emails. This email contained [redacted] deemed [redacted] This noncompliance involves the management practices of workforce management and work management. The root cause was entity personnel's lack of awareness of the entity's [redacted] Specifically, entity personnel did not understand that encryption is a manual process that the user needs to invoke when emails are used for sharing and transporting BCSI. Although the employee at issue was aware of the [redacted] and had taken the required annual [redacted] the employees had inadequate awareness of the encryption process. The noncompliance started on July 20, 2017, the date the entity employee sent the [redacted] to the vendor's email. The noncompliance ended on March 9, 2018, the date the entity employee in the second instance deleted the email and attachment from all his email account folders after sending the email to himself.
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 is allowing a potential bad actor access to BCSI thereby compromising BPS security. The risk is somewhat mitigated for the first instance because of the short, 12 day duration and the information was sent to a vendor with a right to view the information who had a valid PRA and up to date NERC CIP Training. For the second instance, the risk is somewhat mitigated because of the short, one day duration. Additionally, the sender was both the sender and recipient and immediately deleted the email after discovering the mistake. Lastly, the sender had a valid PRA and up-to-date NERC CIP training. No harm is known to have occurred. The entity has prior violations. ReliabilityFirst did not consider certain prior violations repeat infractions, in part, because of the amount of time that has passed since mitigation was completed for said violations, which supports the conclusion that processes and systems have evolved such that the current issues are not a result of a failure to mitigate the prior issues. ReliabilityFirst notes that some of the prior violations involved different facts, circumstances, and/or causes. Other violations resolved within this FFT arguably involve similar conduct as some of the prior violations. However, the current violation poses a lesser risk and demonstrates the entity's ability to identify and correct noncompliances, ReliabilityFirst will not consider the prior violations as an aggravating factor.
Mitigation	To mitigate this noncompliance, the entity: 1) confirmed that the recipient deleted the email and attachment (Incident 1). The entity also deleted the email from the subject matter expert's personal, external email account and checked all email folders to ensure no remnants of the email existed (Incident 2); 2) added a [redacted] Each [redacted] will contain information about a NERC CIP requirement and what the reader should do to ensure compliance with the requirement. Each month a new article will be submitted and included in the [redacted] that is sent via email to all employees as well as be available via internal website. This can be validated for any direct email sent using [redacted] This will allow us to find out how many people an email was sent to, how long they interacted with it and what device they used to access it;

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
RFC2018019775	CIP-011-2	R1	[redacted]	[redacted]	7/20/2017	3/9/2018	Self-Report	Completed

3) designed and implemented a rule set within the [redacted] to identify and block attempts to send outbound, unencrypted email(s) that are themselves, or include attachments that are, classified as [redacted]", including variants of such phrase. Blocked attempts will include an auto-response notification to the sender alerting to the proper method of encrypting outbound email transmissions and auto-encryption of the email. Repeated attempts to send outbound, email transmissions classified as " [redacted] will be reviewed and, if appropriate, result in escalation to management;
4) developed an endpoint data classification tool to assist in the classification of company documents, including BCSI, and reinforcing guidelines on the proper labeling of documents actively managed in [redacted].
5) [redacted]; and
6) deployed the data classification tool to all company-issued workstations and laptops that have authenticated access to the entity network.

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
RFC2019022594	CIP-004-6	R4	[redacted]	[redacted]	10/5/2019	10/7/2019	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)			On November 26, 2019, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-004-6 R4. During an unplanned IT system outage on Saturday, October 5, 2019, an [redacted] added himself (and another [redacted]) into the [redacted] in order to address the outage. The entity is structured so that [redacted] access gives a [redacted] access to the [redacted] system, as well as [redacted] access to [redacted] for [redacted]). The entity had recently implemented a change to reduce the number of [redacted]. The entity reduced the number of [redacted] from [redacted] individuals and created new groups that were more closely tied to job responsibilities. As part of the project, the entity removed the [redacted] in this case from the [redacted] on September 27, 2019, and added them to the newly-created [redacted]" based upon their ongoing job responsibilities. Due to a configuration error, the [redacted] had the ability to add itself and its members to the [redacted]. And, the [redacted] were given inadequate access rights to address the ongoing system outage on Saturday, October 5, 2019 (i.e., they needed [redacted] to troubleshoot the system outage). This issue (i.e., the ability to add users/groups to the [redacted]) was limited to the [redacted] and the [redacted] referenced herein. Early on Monday, October 7, 2019, the [redacted] notified [redacted] that he had added himself and another [redacted] to the [redacted] over the weekend to resolve the outage. The root cause of this noncompliance was the failure to lock down the [redacted] and the privileges and permissions of the [redacted] so that the [redacted] could not add themselves to the [redacted] This noncompliance involves the management practice of workforce management. Workforce management includes, in part, effectively managing and controlling access rights and privileges. This noncompliance started on October 5, 2019, when the individuals obtained unauthorized access and ended on October 7, 2019, when the entity removed the 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). In this case, unauthorized electronic access increased the risk of misuse of the [redacted] to the detriment of the entity and BPS. The ability of the unauthorized individuals to gain access to the [redacted] demonstrated inadequate protections and controls surrounding access management. However, the risk was somewhat reduced in this case based on the following facts. Both individuals had previously held [redacted], which had only been removed eight (8) days prior to this violation as part of an overall IT security policy change. Additionally, both individuals had personnel risk assessments and up-to-date training and retained other active CIP-scoped access. Lastly, the [redacted] was limited to a [redacted] ([redacted] to [redacted]) and [redacted]; it did not include access to any BES Cyber Assets, Protected Cyber Assets, or Electronic Access Control or Monitoring Systems. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes and involved separate and distinct issues.				
Mitigation			To mitigate this noncompliance, the entity: 1) removed the [redacted] from the [redacted], and the permissions of the [redacted] were changed so that they no longer had the ability to add themselves or others to the [redacted] 2) removed the [redacted] within one (1) hour of the notification to [redacted]; and 3) locked down the [redacted] so that only individuals inside of that group can add additional users or groups to the [redacted].				

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022103	CIP-009-6	R1	[redacted]	[redacted]	7/01/2016	2/28/2020	Self-Report	December 28, 2020

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On August 20, 2019, the entity submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-009-6 R1. On April 1, 2019, an [redacted] reviewed the entity's [redacted] in preparation for a planned [redacted]. During the review, the [redacted] discovered that certain [redacted] were not included in the documented recovery plan. As part of its Mitigation Plan, the entity conducted an extent of condition review and identified additional instances of noncompliance. More specifically, the entity did not have properly documented recovery plans for four [redacted] The four [redacted] types were: (1) [redacted] (2) [redacted]; (3) [redacted] and (4) [redacted]. The root cause of this noncompliance was inadequate controls. From a recovery plan perspective, some of the assets were missed during the entity's [redacted], and some of the assets were missed during commissioning or later upgrades [redacted] The issues persisted due to a lack of adequate detective controls. This noncompliance implicates the management practice of risk management. Entities should plan and invoke risk mitigating activities to reduce potential adverse impacts on the reliability and resilience of the BES. This initial instance identified in the Self-Report started on October 1, 2018, when the entity failed to properly document recovery plans for certain [redacted] and ended on October 18, 2019, after the entity corrected the issue. The instances involving the [redacted] started on July 1, 2016, which was the effective date of CIP-009-6 R1 and ended on February 28, 2020, after the entity completed corrective actions associated with the extent of condition review. The instance involving the [redacted] started on July 1, 2019, when the entity failed to properly document recovery plans for the newly commissioned [redacted] and ended on February 28, 2020, after the entity completed corrective actions associated with the extent of condition review.
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). If an entity does not have preplanned recovery capabilities, then it may be more difficult for the entity to rapidly recover from incidents, minimize loss and destruction, mitigate weaknesses that may have been exploited, and restore computing services and BES Cyber System functionality. Here, the risk was not minimal because of the number of instances, the types of assets that were affected, and the durations of the instances. However, the risk was not serious or substantial based upon the following facts. First, this was, in part, a documentation issue because for each affected asset, the entity had a copy of the vendor recovery steps. The entity simply failed to incorporate the vendor recovery steps into an entity-approved format and plan. Second, experienced entity personnel (i.e., subject matter experts and administrators) were assigned to, and responsible for managing, the affected assets, and their familiarity with the assets reduced the risks associated with this noncompliance. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because it posed only a moderate risk to the BPS, the issues were self-reported, and the extent of condition review and mitigation solutions were comprehensive and should prevent recurrence.
Mitigation	To mitigate this noncompliance, the entity: 1) updated the existing [redacted] to include steps to restore all component assets of [redacted]; 2) decommissioned certain assets that are not required for full operational functionality of [redacted] based on the current architectural design; 3) updated its [redacted] to include a step to compare and validate the architecture design or [redacted] with components before the annual recovery exercise, and e-mailed business units a notification of the change; 4) conducted an extent of condition review and updated recovery procedures to ensure that all applicable assets are covered; and 5) conducted CIP-009 testing for [redacted](s). To further mitigate this noncompliance, the entity will complete the following activities by December 28, 2020: 6) conduct CIP-009 testing for [redacted]; 7) conduct CIP-009 testing for [redacted]; and 8) conduct CIP-009 testing for [redacted]. Mitigation is ongoing based on the scope of the associated activities and the time necessary to complete those 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
FRCC2019021605	CIP-007-6	R1, P1.1	[redacted]	[redacted]	07/01/2016	12/18/2019	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 Compliance Audit conducted from [redacted], SERC determined that the Entity, as [redacted] was in noncompliance with CIP-007-6 R1, P 1.1. The Entity failed to document its determination that [redacted] enabled logical network accessible ports were needed. During the Audit, the Entity was unable to provide documentation that supported the business need of the open ports for [redacted] Electronic Access Control and Monitoring (EACMS) Cyber Assets located within the Entity's [redacted]. On August 25, 2019, the Entity completed an extent-of-condition review by scanning the in-scope Cyber Assets and identified [redacted] additional instances where the Entity could not provide documentation that supported the business need of the open ports. All open ports were needed, but the Entity failed to document the business need. This noncompliance started on July 1, 2016, when the Entity failed to document the justification of the need for the logical network accessible ports, and ended on December 18, 2019, when the Entity documented evidence of its determination that the logical network accessible ports were needed. The causes involved management oversight, specifically, a deficient process and a lack of internal controls. The Entity had a process in place that permitted each business unit to implement internal processes for documentation handling, i.e., the naming and formatting conventions and file folders locations, which made identifying, collecting, and reconciling evidence difficult. For example, one business unit identified the [redacted] logical accessible networks by using the vendor supplied documentation, which was not supplied to the Audit Team. The business unit also had identified and documented the necessary logical network accessible ports by the vendor documentation, but did not transition the evidence to the tracking spreadsheet, therefore, it was not submitted as evidence. Management also failed to have adequate internal controls, e.g., checklists, to include all necessary steps the Entity should have taken to properly on-board, off-board or transition an in-scope Cyber Asset, which led to insufficient documentation of the need for enabled network accessible logical ports. Lastly, the Entity failed to ensure that its port identification tool covered all in-scope Cyber Assets and that the reports that it generated did not enable simple identification of issues with enabled network accessible logical 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 (BPS). 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 Bulk Electric System Cyber System and a negative impact on the BPS. The risk was reduced as all of the identified Cyber Assets were within a defined Electronic Security Perimeter (ESP), which would limit the exposure of the potential unneeded open ports and services with limited access through the [redacted]. The ESP is an added layer to protect any potential misuse of those ports not properly documented and the Entity found no ports and services and were not needed, so this resulted in a documentation issue. Notwithstanding, this noncompliance was deemed a moderate risk because the Entity did not have effective detective controls to identify the noncompliance, which lasted approximately 3.5 years. Thus, although the actual risk was minimal due to the potential for an increased risk was significantly increased. No harm is known to have occurred. SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.					
Mitigation			To mitigate this noncompliance, the Entity: 1) documented the need or disabled the port for those for enabled logical network accessible ports identified during the audit as not having an identified need; 2) performed an extent of condition review by scanning in-scope Cyber Assets to identify enabled logical network accessible ports; 3) performed root-cause analysis in conjunction with extent of condition review; 4) documented the need or disabled the port for those enabled logical network accessible ports identified during the extent of condition reconciliation; 5) consolidated the determination of need information for enabled logical network accessible ports; 6) improved the automated reporting of tool to better communicate enabled logical network accessible ports information and issues; 7) implemented an onboarding checklist for Bulk Electric System (BES) Cyber System and their associated BES Cyber Asset (BCA), Protected Cyber Asset (PCA), EACMS, and Physical Access Control Systems (PACS), which helps to eliminate human-performance issues experienced when implementing a diverse set of security controls; 8) created a [redacted] whose scope includes the review of change control ticket actions (including configuration change management) and supporting documentation, planned for once every three weeks, which will eliminate human-performance issues associated with business unit silos; 9) implemented and communicated an off-boarding checklist for BES Cyber Systems and their associated BCA, PCA, EACMS, and PACS, which helps to eliminate human-performance issues experienced when implementing a diverse set of security controls; 10) augmented the enabled port identification capability tool by adding an additional scanning tool for [redacted] Cyber Assets; and 11) conducted training on CIP-007.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020009	CIP-007-6	R4: P4.1	[redacted]	[redacted]	7/1/2016	10/11/2019	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 noncompliance.)	During a Compliance Audit [redacted] WECC determined the entity, [redacted] was in potential noncompliance with CIP-007-6 R2 R4 Part 4.1. Specifically, the entity did not log events for successful login attempts or detected malicious code for [redacted] BES Cyber Assets (BCA) that were capable of performing some of Part 4.1 logging but were not configured to do so; specifically subparts 4.1.1 and 4.1.2. The entity did however provide evidence that gave the auditors reasonable assurance it had implemented methods to log detected malicious code as required by subpart 4.1.3. The extent of condition included [redacted] BCAs associated with Medium Impact BES Cyber Systems (MIBCS) without External Routable Connectivity (ERC) located at [redacted] substations and [redacted] BCAs associated with MIBCS with ERC located at the same [redacted] substations, for a total of [redacted] BCAs [redacted] After reviewing all relevant information, WECC Enforcement concurred with the audit findings as stated herein. The root cause of the noncompliance was attributed to change-related documents not developed or revised. Specifically, the BCAs were installed before the enforcement date of CIP 007-6 and although the entity developed processes for new BES Cyber System acquisition and installation, it did not consider that those processes would need to be developed and documented to establish the condition of existing BCAs. This violation began on July 1, 2016, when the Standard and Requirements became mandatory and enforceable and ended on October 11, 2019 when the BCAs in scope were configured to log events.
Risk Assessment	This issue 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 log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts as required by CIP-007-6 R4 Part 4.1 for [redacted] BCAs at [redacted] substations The failure to log detected successful login attempts or detected failed access attempts and failed login attempts reduced the entity's ability to detect and investigate malicious behavior. Failed login attempts could be indicative of intruder attempts to further compromise BES Cyber Systems to affect the reliability and security of the BPS. [redacted] The extensive length of this violation also contributed to the overall risk determination. However, the entity had implemented good compensating controls. Specifically, the entity implemented multiple technical and procedural controls based on defense-in-depth principles. The entity deployed network segmentation, multiple firewalls, and network level intrusion detection systems (IDS), anti-virus (AV) and threat emulation. Internet access to BCAs with ERC was limited to communications with only the backup control system. The entity also employed network access controls with system level logging providing the capability to shut down network ports should malicious network traffic be detected, and BCAs associated with the HIBCS were authenticated [redacted] No harm is known to have occurred. WECC determined the entity's compliance history with CIP-007-4 R4 should not serve as a basis for escalating the disposition track or applying a penalty. The fact pattern, underlying conduct, and root cause of the prior noncompliance was distinct and separate from the instant noncompliance and the mitigation of the prior noncompliance would not have prevented the instant noncompliance.
Mitigation	To remediate and mitigate this violation, the entity has: 1) updated its [redacted] for asset classifications and asset life cycle management to include tasks to validate compliance with CIP-007-6 during its vulnerability assessment process; 2) updated CIP program processes and procedures to include steps for validating compliance; 3) defined mitigation options for in scope Cyber Assets (replacing or upgrading technology); 4) removed some in scope Cyber Assets from the Electronic Security Perimeter and reclassified them as non-CIP; 5) removed some in scope Cyber Assets from service as part of its Energy Management System upgrade; 6) trained asset administrators [redacted] to include procedures for the asset lifecycle, baseline configurations, and vulnerability assessments to ensure compliance with applicable CIP Standards and Requirements; and 7) upgraded BCAs in scope that couldn't support logging requirements and configuration to log events to the entity's SIEM.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2018020010	CIP-007-6	R4: P4.3	[redacted]	[redacted]	7/1/2016	8/7/2019	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 noncompliance.)

During a Compliance Audit [redacted] WECC determined the entity, [redacted] was in potential noncompliance with CIP-007-6 R4 Part 4.3. Specifically, the entity did not, where technically feasible, retain applicable event logs for at least the last 90 consecutive calendar days as required by CIP-007-6 R4 Part 4.3. The scope included [redacted] BES Cyber Assets (BCAs) and [redacted] Electronic Access Control or Monitoring Systems (EACMS) associated with the High Impact BES Cyber System (HIBCS) located at the primary Control Center where the entity had not correctly configured the Cyber Assets to retain applicable event logs and [redacted] BCAs associated with a MIBCS where the entity did not submit a Technical Feasibility Exception (TFE) for the [redacted] BCAs that could not be configured to retain applicable event logs. This noncompliance began on July 1, 2016, when the Standard and Requirements became mandatory and enforceable and ended on August 7, 2019 when the storage system was configured to retain logs.

The root cause of the noncompliance was attributed to less than adequate procedures and work review checklist. Specifically, the procedures lacked clarity on when to configure logging retention, and there were no reviews of log configuration on the checklist that could have prevented this issue before the entity became noncompliant.

Risk Assessment

This issue 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, where technically feasible, retain applicable event logs for at least the last 90 consecutive calendar days as required by CIP-007-6 R4 Part 4.3 for [redacted] BCAs and [redacted] EACMS associated with the HIBCS.

The failure to submit TFEs could have let to the entity failing to implement mitigating measures for the log retention limitations present on the BCAs and the failure to retain logs of successful, failed, and attempted logins reduces the entity's ability to detect and investigate after-the-fact malicious behavior. Failed login attempts could be indicative of intruder attempts to further compromise BES Cyber Systems, and successful, unexpected logins could have allowed an attacker to establish themselves and gather intelligence, spread electronic infections or interfere with the operation or indication of affected assets. [redacted]. The extensive length of this violation also contributed to the overall risk determination.

However, the entity had implemented good compensating controls. Specifically, the entity implemented multiple technical and procedural controls based on defense-in-depth principles. The entity deployed network segmentation, multiple firewalls, and network level intrusion detection systems (IDS), anti-virus (AV) and threat emulation. Internet access to BCAs with ERC was limited to communications with only the backup control system. The entity also employed Network Access Controls (NAC) with system level logging providing the capability to shut down network ports should malicious network traffic be detected, and BCAs associated with the HIBCS were authenticated via a segregated domain. No harm is known to have occurred.

WECC determined the entity's compliance history with CIP-0007-6 R4 should not serve as a basis for escalating the disposition track or applying a penalty. The fact pattern, underlying conduct, and root cause of the prior noncompliance was distinct and separate from the instant noncompliance and the mitigation of the prior noncompliance would not have prevented the instant noncompliance.

Mitigation

To remediate and mitigate this violation, the entity has:

1) configured applicable Cyber Assets to retain logs for at least 90 days;
2) submitted TFEs for the BCAs that were not capable of retaining event logs;
3) update its vulnerability assessment process to reference the checklist for confirming configuration steps;
4) update the checklist to include explicit steps related to logging; and
5) submit Technical Feasibility Exceptions for applicable Cyber Assets until those Cyber Assets are replaced with assets that are capable of being compliant with CIP Standards.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018181	CIP-006-3c	R6	[redacted]	[redacted]	7/2/2011	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.)	During a Compliance Audit [redacted] WECC determined that the entity, [redacted] was in potential noncompliance with CIP-006-3c R6. Specifically, the entity did not implement a method to log enough information to uniquely identify individuals and their time of access twenty-four hours a day, seven days a week at [redacted] Physical Security Perimeter (PSP) access points controlling access [redacted] when the entity left the PSP access point doors open during business hours. The entity believed that having staff [redacted] monitoring access to the PSP was sufficient for compliance. This issue began on July 2, 2011, when the entity should have been appropriately logging access to the PSP and ended on October 31, 2018, when the entity changed the "Disable Open Too Long" field to "Never" for the [redacted] PSPs in scope. The root cause of the issue was attributed to personnel involved with monitoring the PSP access points misunderstanding the Requirement. Specifically, personnel believed that since the non-PSP door was logging access of authorized personnel, compliance with the Requirement was met.
Risk Assessment	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 adequately implement technical or procedure controls for monitoring physical access at [redacted] access points to the PSP twenty-four hours a day, seven days a week as required by CIP-006-3c R6. Such failure could have resulted in a lack of knowledge of who was inside the PSP at any given time, which could hinder investigations of past events. Additionally, unauthorized access by personnel could potentially result in intentional or unintentional compromise of the Cyber Assets within the PSP [redacted] As compensation, during business hours the system administrator was located directly next to the opened PSP access point to perform controlling, monitoring, and logging; however, the entity could not confirm that those duties were performed 100 percent of the time. Additionally, the access points had posted signage stating all unauthorized personnel must sign the PSP access log when entering. The access points were closed when physical monitoring could not occur. No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To remediate and mitigate this issue, the entity has: 1) discontinued the practice of leaving the PSP access point doors open during business hours; and 2) changed the Physical Access Control System door alarm setting from "Disable Open Too Long" field to "Never" for the [redacted] PSPs access point doors in scope, so that all door held open alarms would be sent to the security operations center for investigation within 15 minutes of receiving the alarm. A "Door Open too long" alarm is triggered when a PSP door is opened and not shut within 30 seconds.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
WECC2017018850	CIP-007-1	R5: R5.2.1	[redacted]	[redacted]	7/7/2008	12/13/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On December 14, 2017, the entity submitted a Self-Report stating that, [redacted] it was in potential noncompliance with CIP-007-1 R5. Specifically, in April of 2017, in preparation for a vulnerability assessment, the entity discovered a hidden supervisor account [redacted] where the password had not been changed prior to putting [redacted] into service on July 7, 2008, as required by CIP-007-1 R5.2.1. At the time of installation, [redacted] were classified as Critical Cyber Assets (CCAs). At the time of discovery, the CCAs had been reclassified under version 6 of the CIP Standards as BES Cyber Assets (BCAs) associated with medium impact BES Cyber Systems (MIBCS) [redacted] The duration of this issue spanned two versions of the CIP Standards. As such, the entity also did not identify and inventory all known enabled default account types as required by CIP-007-6 R5 Part 5.2 and did not submit a Technical Feasibility Exception (TFE) for the BCAs since the entity was not able to technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months. The root cause of this issue was attributed to the vendor not notifying the entity of the hidden supervisor accounts. The entity used two vendor configuration guides for installation, neither of which mentioned the hidden accounts. After further investigation, the entity determined the hidden supervisor account could not be changed due to limitations with the current firmware versions on the BCAs. This issue ended on December 13, 2017 when the entity submitted a TFE for the BCAs in scope of this issue.
Risk Assessment	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, [redacted] associated with MIBCS, the entity failed to 1) change passwords prior to putting any systems into service for accounts that must remain enabled, as required by CIP-007-1 R5.2.1; 2) identify and inventory all known enabled default account types, as required by CIP-007-6 R5 Part 5.2; and 3) submit a TFE for accounts that it could not technically or procedurally enforce password changes or an obligation to change the password at least once very 15 calendar days as required by CIP-007-6 R5 Part 5.6 . The failure of not identifying, taking inventory of, or changing default passwords could have resulted in an individual with malicious intent gaining access to the BCAs at issue to view or monitor substation line status and information or issue any commands to the BCAs with the intent to cause harm and affect the reliability of the BPS. However, as compensation, the hidden supervisor account did not allow any control capabilities of the BCAs in scope, there was no direct access to the Internet from the BCAs, and the BCAs were segregated from the corporate network and resided in an identified Electronic Security Perimeter (ESP). Additionally, authorization to access the BCAs was controlled using a security identity management system which was reviewed quarterly and interactive user access was controlled through layers [redacted] No harm is known to have occurred. WECC determined that the entity's compliance history should not serve as a basis for aggravating the disposition treatment. The entity had one relevant prior noncompliance of minimal risk associated with changing known default passwords which had a distinct fact pattern and root cause, of which the mitigation activities would not have prevented this issue and is not indicative of a systemic or programmatic issue.
Mitigation	To remediate and mitigate this issue, the entity has: 1) submitted a TFE for the BCAs in scope of this issue which WECC subsequently approved; 2) incorporated language into its Request for Proposal (RFP) to address hidden or default vendor accounts; and 3) created a quarterly task to reach out to vendors for any notifications related to CIP compliance and applicable Cyber Assets. Part of this task would be to review any notifications provided and follow through on any necessary actions based on the notifications.

COVER PAGE

This filing/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 filing/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	RFC2019021479	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
2	RFC2019021478	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
3	RFC2019022559	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
4	RFC2019022560	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years Category 2 – 12: 2 years
5	SERC2018020015		Yes	Yes	Yes					Yes				Category 2 – 12: 2 year
6	FRCC2019021675	Yes		Yes	Yes					Yes			Yes	Category 2 – 12: 2 year
7	TRE2020023314	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
8	TRE2019021360			Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
9	TRE2017018670	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
10	TRE2018020245			Yes	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
RFC2019021479	CIP-007-6	R4	[redacted]	[redacted]	9/15/2018	4/8/2019	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On May 2, 2019 and June 18, 2019, the entity submitted Self-Reports stating that, as a [redacted], it was in noncompliance with CIP-007-6 R4. There are two instances in this noncompliance. First, on February 4, 2019, as a result of a quarterly internal control, the entity's [redacted] discovered that the entity's SIEM Security Information and Entity Management (SIEM) system stopped receiving logs from two devices. The first device is an Electronic Access Control or Monitoring System (EACMS) [redacted] This incident had been occurring since September 15, 2018 and the entity restored logging to the SIEM system on January 7, 2019. Both assets were sending logs, but the logs were not received by the SIEM system for alerting or for 90 day retention due to an incorrect translation setting on the firewall. Specifically, the logging destination on these two devices was not updated when the SIEM system received a major upgrade that required new settings on the firewall. All other devices in this network segment did have the correct setting and logging functioned as intended. The first device overran its buffer so it did not retain logs locally for the time period of September 15, 2018 to January 7, 2019. The second device did retain all logs locally and a review of those logs showed that no alerts would have been generated. [redacted] stopped working for the second device at the same time as the firewall change. The entity's [redacted] evaluates all NERC CIP assets; therefore an extent of condition is completed each time there is an execution of this control. Second, one device's [redacted] stopped working, resulting in no logs to SIEM system for alerting or for 90-day retention. The entity discovered this second instance on April 23, 2019, through the same internal control. The entity was unable to determine why the [redacted] stopped working. The entity believes that the [redacted] stopped working at the same time as the firewall change described in the first instance. This resulted in no logs getting sent to SIEM system for alerting or 90 day retention. The second instance began on November 19, 2018, and ended on April 8, 2019, when the entity restored logging to the device. The root cause of both instances of noncompliance was that there was no documented step in the process to communicate changes that impact other assets in the same [redacted] This noncompliance involves the management practices of asset and configuration management, work management, planning, and verification due to the ineffective work process that lacked a step to communicate changes that impact other assets in the same [redacted] This noncompliance started on September 15, 2018, when the first device did not retain logs locally, and ended on April 8, 2019, when the entity restored logging for all impacted 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 posed by not logging is that SIEM system would not generate applicable alerts for the two devices in the first instance. If these devices were to go down, it would turn off authentication, impacting the entity's ability to access the environment. [redacted] The risk is not serious because intrusion detection and prevention systems did remain in place to monitor for malicious code in both instances. Also reducing the risk, the devices in both instances reside behind a firewall with specific and limited [redacted] rules in a Physical Security Perimeter (PSP) with access limited to NERC-CIP qualified personnel. Furthermore, the entity experienced no loss of authentication to the first device in the first instance. The second device in the first instance was logging locally, and retained logs for 90 days. The local logs were reviewed and no issues were found. For the device in the second instance, the entity had no issue obtaining backups for the other networking devices, which reduces the risk of not having logs for that device. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.
Mitigation	To mitigate this noncompliance, the entity: 1) restored Logging reception from the asset to SIEM system; 2) performed an extent of condition to determine if other assets that send logs to SIEM system were not received by SIEM system for the period of Q4 2018 and Q1 2019. The extent of condition determined that no other assets had this logging issue. The entity performed a comparison between CIP assets listed in the entity's asset management system and those logging to its central logging system. This review identified any system not properly listed in each system and prompted investigation of these items: previous CIP assets that may have been removed from CIP Status or retired and not removed from alerting groups; new or existing CIP assets that may not be sending logs or be accurately assigned an alerting group; and any assets recorded in one system and not the other; 3) created a Control Procedure to identify and resolve potential logging issues. SIEM system weekly sends a [redacted] report to the [redacted]. [redacted] used the report to identify assets that SIEM system has not received a log for in 5 or more days. Asset owners are alerted to potential logging issues, which reminds them they are responsible to ensure their

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
RFC2019021479	CIP-007-6	R4	[redacted]	[redacted]	9/15/2018	4/8/2019	Self-Report	Completed

devices are sending logs to SIEM system and those logs are received. They are also told they are expected to resolve any issues identified by the control before the control is executed again one week later;

4) updated their [redacted] to add a step to consider the potential impact to other NERC CIP assets as a result of a global change to a network device. This impact could involve logging, remote access, [redacted], system to system communication, baseline and [redacted]. This step will inform asset owners that [redacted] is making a change that could impact their assets and they should verify their assets are functioning as needed; and

5) [redacted]

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
RFC2019021478	CIP-007-6	R4	[redacted]	[redacted]	9/15/2018	4/8/2019	Self-Report	Completed

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

On May 2, 2019 and June 18, 2019, the entity submitted Self-Reports stating that, as a [redacted], it was in noncompliance with CIP-007-6 R4.

There are two instances in this noncompliance.

First, on February 4, 2019, as a result of a quarterly internal control, the entity's [redacted] discovered that the entity's SIEM Security Information and Entity Management (SIEM) system stopped receiving logs from two devices. The first device is an Electronic Access Control or Monitoring System (EACMS) [redacted]

This incident had been occurring since September 15, 2018 and the entity restored logging to the SIEM system on January 7, 2019. Both assets were sending logs, but the logs were not received by the SIEM system for alerting or for 90 day retention due to an incorrect translation setting on the firewall. Specifically, the logging destination on these two devices was not updated when the SIEM system received a major upgrade that required new settings on the firewall. All other devices in this network segment did have the correct setting and logging functioned as intended. The first device overran its buffer so it did not retain logs locally for the time period of September 15, 2018 to January 7, 2019. The second device did retain all logs locally and a review of those logs showed that no alerts would have been generated. [redacted] stopped working for the second device at the same time as the firewall change. The entity's [redacted] evaluates all NERC CIP assets; therefore an extent of condition is completed each time there is an execution of this control.

Second, one device's [redacted] stopped working, resulting in no logs to the SIEM system for alerting or for 90-day retention. The entity discovered this second instance on April 23, 2019, through the same internal control. The entity was unable to determine why the [redacted] stopped working. The entity believes that the [redacted] stopped working at the same time as the firewall change described in the first instance. This resulted in no logs getting sent to SIEM system for alerting or 90 day retention. The second instance began on November 19, 2018, and ended on April 8, 2019, when the entity restored logging to the device.

The root cause of both instances of noncompliance was that there was no documented step in the process to communicate changes that impact other assets in the same [redacted]. This noncompliance involves the management practices of asset and configuration management, work management, planning, and verification due to the ineffective work process that lacked a step to communicate changes that impact other assets in the same [redacted]

This noncompliance started on September 15, 2018, when the first device did not retain logs locally, and ended on April 8, 2019, when the entity restored logging for all impacted 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 posed by not logging is that the SIEM system would not generate applicable alerts for the two devices in the first instance. If these devices were to go down, it would turn off authentication, impacting the entity's ability to access the environment. [redacted] The risk is not serious because intrusion detection and prevention systems did remain in place to monitor for malicious code in both instances. Also reducing the risk, the devices in both instances reside behind a firewall with specific and limited [redacted] rules in a Physical Security Perimeter (PSP) with access limited to NERC-CIP qualified personnel. Furthermore, the entity experienced no loss of authentication to the first device in the first instance. The second device in the first instance was logging locally, and retained logs for 90 days. The local logs were reviewed and no issues were found. For the device in the second instance, the entity had no issue obtaining backups for the other networking devices, which reduces the risk of not having logs for that device. 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 while the result of some of the prior noncompliances were arguably similar, the prior noncompliances arose from different causes.

Mitigation

To mitigate this noncompliance, the entity:

1) restored Logging reception from the asset to the SIEM system;
2) performed an extent of condition to determine if other assets that send logs to the SIEM system were not received by the SIEM system for the period of Q4 2018 and Q1 2019. The extent of condition determined that no other assets had this logging issue. The entity performed a comparison between CIP assets listed in the entity's asset management system and those logging to its central logging system. This review identified any system not properly listed in each system and prompted investigation of these items: previous CIP assets that may have been removed from CIP Status or retired and not removed from alerting groups; new or existing CIP assets that may not be sending logs or be accurately assigned an alerting group; and any assets recorded in one system and not the other;

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
RFC2019021478	CIP-007-6	R4	[redacted]	[redacted]	9/15/2018	4/8/2019	Self-Report	Completed
			3) created a Control Procedure to identify and resolve potential logging issues. SIEM system weekly sends a [redacted] report to the [redacted] used the report to identify assets that SIEM system has not received a log for in 5 or more days. Asset owners are alerted to potential logging issues, which reminds them they are responsible to ensure their devices are sending logs to SIEM system and those logs are received. They are also told they are expected to resolve any issues identified by the control before the control is executed again one week later; 4) updated their [redacted] to add a step to consider the potential impact to other NERC CIP assets as a result of a global change to a network device. This impact could involve logging, remote access, [redacted], system to system communication, baseline and [redacted] This step will inform asset owners that [redacted] is making a change that could impact their assets and they should verify their assets are functioning as needed; and 5) [redacted] 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
RFC2019022559	CIP-004-6	R4	[redacted]	[redacted]	7/18/2016	10/29/2019	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On November 19, 2019, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-004-6 R4. The entity discovered that keys associated with server cabinets not related to NERC applicable cyber systems (non-NERC cabinets) were capable of unlocking six NERC Physical Security Perimeter (PSP) cabinet doors and six Physical Access Control System (PACS) protection cabinet doors (a total of 12 doors) (NERC cabinets). The keys associated with non-NERC cabinets were not managed following the documented [redacted] and some individuals who had access to the keys had not been approved, trained or background checked appropriately for access to the NERC cabinets. Specifically, on Friday October 11, 2019, a Senior Security Consultant working in a [redacted] noticed keys in the latch mechanisms of several non-NERC cabinets. The keys appeared very similar to keys that [redacted] holds for NERC cabinets, which prompted the security consultant to test them. He determined that turning the key in the NERC cabinets' latches allowed the cabinets' doors to be opened without using the card reader and PIN keypad mounted on the cabinets. Opening the doors this way initiated a "forced door" alarm associated with the cabinet door being opened without an authorizing card swipe and PIN entry. The security consultant then immediately informed the [redacted] of this issue. The entity purchased and installed the NERC cabinets in preparation for CIP v5. The entity commissioned the NERC cabinets into production on April 6, 2016. The entity installed the non-NERC cabinets and their keys for an Information Technology (IT) project on July 18, 2016. Personnel involved with the initial installation of the NERC cabinets are no longer employed by the entity and entity [redacted] have secured the keys from the NERC cabinets since installation. The entity has only used the installed [redacted] to manage access to the NERC cabinets. After discovering this noncompliance, the entity contacted the lock manufacturer to determine whether other customers hold keys that are capable of opening NERC cabinets. The lock manufacturer has been unable to disclose whether other customers hold keys that are capable of opening the NERC cabinets. Upon determining that the lock cylinders in the NERC cabinets cannot be re-keyed, the entity made physical modifications to the latch handles, making it impossible to open the NERC cabinets with the non-NERC cabinet keys. The entity performed an extent of condition and determined that no one ever used the non-NERC cabinet keys to open up any of the NERC cabinets because using the key would have caused a "forced door" alarm and no such alarms have ever been triggered (other than the test performed by the Senior Security Consultant in investigating this issue discussed above). This noncompliance involves the management practices of asset and configuration management and verification because the entity did not purchase NERC cabinets that required unique keys. The root cause of this noncompliance was a failure to buy NERC cabinets that required unique keys. A contributing cause is that entity personnel did not fully understand the controls implemented to secure the NERC PSP cabinets. This noncompliance started on July 18, 2016, the first date that the keys for the non-NERC cabinets could open the NERC cabinets and ended on October 29, 2019, when the entity made physical modifications to the latch handles, making it impossible to open the NERC cabinets with the non-NERC cabinet keys.
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 this noncompliance is allowing two-factor authentication to be bypassed by using the non-NERC cabinet keys in order to access NERC cabinets and allowing individuals access to NERC cabinets (PSPs) containing Bulk Electric System Cyber Assets and PACS without proper approval, training, and background checks. These risks could lead to the compromise of the cyber assets inside the NERC cabinets. The risk is not minimal because of the long, more than three year duration. The risk is lessened because any use of the non-NERC cabinet keys to open the NERC cabinet doors and access the PSP would have resulted in a forced door alarm with immediate investigation by security personnel exposing the use of the key. The entity confirmed that this never occurred since the installation of the cabinets in 2016. Additionally, the entity restricted access to the [redacted] holding the NERC cabinets to authorized entity personnel for the duration of the noncompliance. The entity logged and escorted any non-authorized entity personnel who accessed the [redacted] Lastly, entity personnel were not aware that the keys to the NERC cabinets were not unique to the NERC cabinets and all NERC cabinets are clearly marked as NERC PSP Access Points and have card readers with PIN pads requiring two-factor authentication. 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 involved separate and distinct issues and conduct.
Mitigation	To mitigate this noncompliance, the entity: 1) collected all known keys for the non-NERC cabinets with this type of door latch at all corporate [redacted] locations; and 2) contacted a locksmith who determined that the cabinets could not be re-keyed, and the entity made physical modifications to the latch handles, making it impossible to open the NERC cabinets with the non-NERC cabinet keys.

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
RFC2019022559	CIP-004-6	R4	[redacted]	[redacted]	7/18/2016	10/29/2019	Self-Report	Completed
			ReliabilityFirst has verified the completion of all mitigation activity.					

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019022560	CIP-004-6	R4	[redacted]	[redacted]	7/18/2016	10/29/2019	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On November 19, 2019, the entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-004-6 R4. The entity discovered that keys associated with server cabinets not related to NERC applicable cyber systems (non-NERC cabinets) were capable of unlocking six NERC Physical Security Perimeter (PSP) cabinet doors and six Physical Access Control System (PACS) protection cabinet doors (a total of 12 doors) (NERC cabinets). The keys associated with non-NERC cabinets were not managed following the documented [redacted] and some individuals who had access to the keys had not been approved, trained or background checked appropriately for access to the NERC cabinets. Specifically, on Friday October 11, 2019, a Senior Security Consultant working in a [redacted] noticed keys in the latch mechanisms of several non-NERC cabinets. The keys appeared very similar to keys that [redacted] holds for NERC cabinets, which prompted the security consultant to test them. He determined that turning the key in the NERC cabinets' latches allowed the cabinets' doors to be opened without using the card reader and PIN keypad mounted on the cabinets. Opening the doors this way initiated a "forced door" alarm associated with the cabinet door being opened without an authorizing card swipe and PIN entry. The security consultant then immediately informed the [redacted] of this issue. The entity purchased and installed the NERC cabinets in preparation for CIP v5. The entity commissioned the NERC cabinets into production on April 6, 2016. The entity installed the non-NERC cabinets and their keys for an Information Technology (IT) project on July 18, 2016. Personnel involved with the initial installation of the NERC cabinets are no longer employed by the entity and entity [redacted] have secured the keys from the NERC cabinets since installation. The entity has only used the installed [redacted] to manage access to the NERC cabinets. After discovering this noncompliance, the entity contacted the lock manufacturer to determine whether other customers hold keys that are capable of opening NERC cabinets. The lock manufacturer has been unable to disclose whether other customers hold keys that are capable of opening the NERC cabinets. Upon determining that the lock cylinders in the NERC cabinets cannot be re-keyed, the entity made physical modifications to the latch handles, making it impossible to open the NERC cabinets with the non-NERC cabinet keys. The entity performed an extent of condition and determined that no one ever used the non-NERC cabinet keys to open up any of the NERC cabinets because using the key would have caused a "forced door" alarm and no such alarms have ever been triggered (other than the test performed by the Senior Security Consultant in investigating this issue discussed above). This noncompliance involves the management practices of asset and configuration management and verification because the entity did not purchase NERC cabinets that required unique keys. The root cause of this noncompliance was a failure to buy NERC cabinets that required unique keys. A contributing cause is that entity personnel did not fully understand the controls implemented to secure the NERC PSP cabinets. This noncompliance started on July 18, 2016, the first date that the keys for the non-NERC cabinets could open the NERC cabinets and ended on October 29, 2019, when the entity made physical modifications to the latch handles, making it impossible to open the NERC cabinets with the non-NERC cabinet keys.
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 this noncompliance is allowing two-factor authentication to be bypassed by using the non-NERC cabinet keys in order to access NERC cabinets and allowing individuals access to NERC cabinets (PSPs) containing Bulk Electric System Cyber Assets and PACS without proper approval, training, and background checks. These risks could lead to the compromise of the cyber assets inside the NERC cabinets. The risk is not minimal because of the long, more than three year duration. The risk is lessened because any use of the non-NERC cabinet keys to open the NERC cabinet doors and access the PSP would have resulted in a forced door alarm with immediate investigation by security personnel exposing the use of the key. The entity confirmed that this never occurred since the installation of the cabinets in 2016. Additionally, the entity restricted access to the [redacted] holding the NERC cabinets to authorized entity personnel for the duration of the noncompliance. The entity logged and escorted any non-authorized entity personnel who accessed the [redacted]. Lastly, entity personnel were not aware that the keys to the NERC cabinets were not unique to the NERC cabinets and all NERC cabinets are clearly marked as NERC PSP Access Points and have card readers with PIN pads requiring two-factor authentication. 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 involved separate and distinct issues and conduct.
Mitigation	To mitigate this noncompliance, the entity: 1) collected all known keys for the non-NERC cabinets with this type of door latch at all corporate [redacted] locations; and 2) contacted a locksmith who determined that the cabinets could not be re-keyed, and the entity made physical modifications to the latch handles, making it impossible to open the NERC cabinets with the non-NERC cabinet keys.

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
RFC2019022560	CIP-004-6	R4	[redacted]	[redacted]	7/18/2016	10/29/2019	Self-Report	Completed
			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	Mitigation Completion Date
SERC2018020015	CIP-007-6	R5, R5.1	[redacted]	[redacted]	7/1/2016	4/10/2019	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, alleged, or confirmed violation.)

On July 12, 2018, the Entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-007-6 R5, P5.1. The Entity did not enforce authentication of interactive user access to multiple relays.

On May 15, 2018, an Entity transmission settings engineer attended a [redacted] conference where a paper was presented on a security vulnerability with certain relays. Specifically, the paper was on default communication port timeout settings set to "0" or "OFF" for locally accessible ports. If deployed using this setting, authentication to the relay would not require a password. On May 16, 2018, the transmission settings engineer returned to the office and discovered that two relays had default communication port timeout settings set to "0" or "OFF" for locally accessible ports. As deployed, authentication to the relay did not require a password. Because a password was not required, a method to enforce interactive user access was not in place, and a noncompliance with CIP-007-6 R5, P5.1 resulted. On May 17, 2018, the Entity entered a report to review this issue internally, and on July 5, 2018, the Entity updated the port timeout settings of the relays discovered on May 16, 2018.

To determine the scope and extent-of-condition (EOC), the Entity reviewed all relays in CIP substations, including affiliates' substations. The Entity concluded that of [redacted] relays made by the same vendor, [redacted] required an update. Thus, the issue impacted [redacted] Bulk Electric System (BES) Cyber Assets associated with [redacted] BES Cyber Systems.

This noncompliance started on July 1, 2016, when the standard became mandatory and enforceable, and ended on July 5, 2018, when the Entity updated the port timeout settings of the relays.

The cause of this violation was a manufacturing issue. Specifically, relay firmware contained a hidden vulnerability where default communication port timeout settings set to "0" or "OFF" for locally accessible ports resulted in a situation where authentication to the relay did not require a password. The Entity's testing was based on the vendor's documentation on the devices which did not document this specific issue because the vendor was unaware of the issue at the time; therefore, the Entity would not have known to test for the issue.

On June 13, 2019, the Entity submitted a Scope Expansion of CIP-007-6 R5, P5.1. On August 30, 2018, the Entity transmission engineering transmitted a port timeout setting for a specific relay type to field personnel. An employee verified that the relay had the correct port timeout setting. Sometime between August 30, 2018 and March 11, 2019, while working on a capital project requiring relay reconfiguration, field contract personnel inadvertently changed relay settings so that authentication was not required. On March 11, 2019, document management personnel discovered the issue when they compared relay settings files uploaded by field personnel with intended settings and discovered that the previously correct port timeout setting was now incorrect. Field personnel sent an email to a settings engineer to notify them of the discrepancy. The settings engineer contacted project management & construction personnel. On April 10, 2019 field personnel corrected the setting.

The scope of the noncompliance affected [redacted] substations, [redacted] BES Cyber Systems and [redacted] BCAs.

This noncompliance started on August 31, 2018, the earliest date that a relay setting could have been changed, until April 10, 2019, when the Entity applied the correct port timeout settings.

The cause of the noncompliance was an inadequate procedure. The Entity's procedure failed to include an additional step for field personnel to verify that relay settings matched the desired settings.

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 enforcing authentication, there was a potential for malicious actors to log into relays, run malicious code, make settings changes, trip breakers or cause misoperations compromising grid security. However, malicious exploitation of the vulnerability would be difficult because the Entity had several controls in place. The Entity disabled remote access to the relays; therefore, only individuals with authorized physical access would be able to make modifications. The Entity also outfitted all PSPs with active monitoring including recorded security cameras monitored at all times by its security operations center. Finally, the Entity's protective relaying schemes employed backup protection in the event of unwanted trips, and the Entity operates its system with contingency plans in place at all times. No harm is known to have occurred.

SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.

Mitigation

For the original Self-Report, to mitigate this noncompliance, the Entity:

1) performed an EOC for all relays from the vendor (Instance 1 and 2);
2) changed all the incorrect relay port settings (Instance 1 and 2);
3) revised all transmission standard relay setting templates to ensure no port timeout settings are set to "0" or" OFF." The Entity changed port timeout setting to the maximum time delay value (Instance 1);
4) created and transmitted a bulletin to stakeholders, including field relay employees, field relay contractors, and relay settings personnel, to remind them to avoid any port timeout settings with a value of "0" or "OFF" in the future (Instance 1);

SERC Reliability Corporation (SERC) FFT CIP

	5) created and communicated a bulletin to affected stakeholders, including field relay employees and field relay contractors, directing them to perform a documented peer check that they have successfully logged out of communications ports following any log-ins to communications ports on relay devices in CIP [redacted] substations (Instance 1); 6) performed training applying the correct port timeout settings, emphasizing the use of tools including procedure usage (Instance 2); 7) communicated a notification to all field relay employees and field relay contractors to implement all settings in relays exactly as transmitted (Instance 2); 8) updated its protection system commissioning and testing procedure to ensures field personnel, including contractors, verify that the settings match the designed settings (Instance 2); 9) benchmarked other utility companies to understand how they are addressing this issue (Instance 2); 10) developed and delivered one-time refresher training as change management on the updated procedure and bulletins related to relay commissioning with all personnel involved in relay changes (Instance 1 and 2); 11) developed and deployed annual computer-based training module for field relay employees and contractors on the updated procedure (Instance 1 and 2); and 12) conducted an effectiveness review to verify that relay local port timeout settings are not set to “null” or “zero” (Instance 1).

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
FRCC2019021675	CIP-007-6	R4, P4.2, P4.3	[redacted]	[redacted]	11/17/2018	03/11/2019	Self Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On June 12, 2019, the Entity submitted a Self-Report stating that, as a [redacted], [redacted], [redacted], [redacted], [redacted], and [redacted], it was in noncompliance with CIP-007-6 R4, P4.2, and P4.3. The Entity failed generate the appropriate alerts for log files (P4.2), and retain log files for 90 days (P4.3). On March 7, 2019, during the 15-day log reviews, the Entity's [redacted] discovered that events were being logged on [redacted] servers, but logs were not being retrieved and retained on the servers for a number of Cyber Assets due to a configuration error on the servers (P4.3). The [redacted] servers receive [redacted] files for [redacted] Cyber Assets at the Entity's [redacted]. Additionally, because logs were not being retrieved by the [redacted] servers, the alerting system was incapable of generating alerts (P4.2). The Entity did not discover the missing logs during earlier log reviews because the of a configuration error in the alerting system. The Entity conducted an extent-of-condition which revealed that logs had not been retrieved and retained for multiple dates, during a period of 104 days, for [redacted] BES Cyber Assets (BCAs) and [redacted] Physical Access Control Systems (PACS) on the [redacted] Server (P4.3). Additionally, logs had not been retrieved and retained for multiple dates, during a period of 111 days, for [redacted] BCAs and [redacted] PACS on the [redacted] Server (P4.3). Because the logs were not received on the [redacted] servers, the alerting system was incapable of generating appropriate alerts (P4.2). In addition, the logs were not stored for 90 days (P4.3) because the Cyber Assets do not always have the capability to retain local logs for 90 consecutive days and the logs could not be retrieved by the [redacted] servers. This noncompliance started on November 17, 2018, when the Entity first failed to generate alerts for the [redacted] Cyber Assets, and ended on March 11, 2019, when a temporary solution was implemented to correct the log collection issues. The cause for this noncompliance was a lack of internal control, such as an [redacted] for the affected servers, which would have detected the misconfiguration on the servers and discovered that log files were generated every day.
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 properly collect log files, generate appropriate alerts, and retain the log files for 90 days from the BCAs and EACMS could have allowed unknown Cyber Security activity to go unnoticed and allow unauthorized actions to take place on the Cyber Assets impacting the reliability of the bulk power system. This risk was reduced because, according to the Entity, all of the affected Cyber Assets were afforded the other protections required by the Standards, and the Entity's response to resolving the technical causes were done promptly after discovery. No harm is known to have occurred. SERC considered the Entity's relevant compliance history in determining the disposition track. The Entity's relevant noncompliance with CIP-007-6 includes: [redacted] occurred [redacted] and [redacted] occurred [redacted]. Additionally, [redacted] involved [redacted] BCAs that were not properly configured for logging, and the root cause of the prior instant noncompliance was different, such that the prior mitigation would not have prevented the instant noncompliance. These prior instances should not serve as a basis for applying a penalty.
Mitigation	To mitigate this noncompliance, the Entity: 1) implemented an [redacted] to run daily, at midnight, to restart the [redacted] service for stability; 2) fixed queuing issue within the [redacted] configurations identified by [redacted] during the root cause analysis; 3) fixed the misconfigured alert to properly show assets that the SIEM has not received a log for 24 hours or more; and 4) created a new [redacted], which [redacted] confirmed that folders are being generated every day with the history of the daily results.

Texas Reliability Entity, Inc. (Texas RE) 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
TRE2020023314	CIP-002-5.1a	R2	[redacted] (the "Entity")	[redacted]	03/01/2019	02/27/2020	Self-Report	12/18/2020

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On May 1, 2020, the Entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-002-5.1a R2. The Entity submitted the Self-Report to Texas RE under an existing multi-region registered entity agreement. Specifically, the Entity reported that it failed to acquire CIP Senior Manager approval of its list of high and medium impact BES Cyber Systems (BCS) in 2018 and 2019. The Entity reported that although it had documented CIP Senior Manager approval of a list of high and medium impact BES Cyber Assets (BCA), it failed to have the documented approval of a list of medium and high impact BCS required by CIP-002-5.1a R2. Texas RE reviewed the approved lists of medium and high impact BCAs that were created and approved in 2018 and 2019. Texas RE determined that the 2018 list included identifications of the applicable medium and high impact BCS, however it did not include a list of assets that contain low impact BCS, as required by the standard. Texas RE determined that the 2019 list included identifications for [redacted] applicable medium and high impact BCS and included identifications of all of the BES assets that contain low impact BCS. The root cause of this noncompliance was insufficient procedures. The Entity determined that an insufficient knowledge transfer occurred between an outgoing employee that had been responsible for ensuring these activities were completed successfully and the new employee that took over the process. Additionally, the Entity determined that the personnel performing the review of the CIP-002-5.1a R2 evidence followed the Entity's documented procedures as they were written. As such, the Entity subsequently determined that the procedures lacked the level of detail necessary to ensure that the noncompliance would not occur. Specifically, the Entity determined that the procedure document did not specify the information that is required to be validated to ensure the evidence is in compliance with CIP-002-5.1a R2. This noncompliance started on March 1, 2019, which is the first day that is more than 15 calendar months from when the CIP Senior Manager (or delegate) approved the identifications required in CIP-002-5.1a R1 and ended on February 27, 2020, when the Entity documented CIP Senior Manager (or delegate) approval of the identifications required in CIP-002-5.1a R1.
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. Increasing the risk as it relates to the Entity: • the Entity is [redacted]; • the Entity is [redacted]; • the Entity owns or operates equipment for [redacted]; • the Entity is party to [redacted]; • the Entity is responsible for monitoring and operating BES assets or systems [redacted]; • the Entity uses [redacted]; • the Entity owns or operates [redacted]; and • the Entity owns or operates [redacted]. Lessening the risk as it relates to the Entity: • the Entity has not reported any cyber security events using EOP-004. Increasing the risk as it relates to the noncompliance: • the duration of the noncompliance was long, approximately one year; and • during the period of noncompliance the Entity was noncompliant with CIP-002-5.1 R1. Lessening the risk as it relates to the noncompliance: • the Entity created, reviewed, and approved an itemized list of BCAs, in excess of the minimum required by the standard; and • no harm is known to have occurred. Texas RE determined that the Entity's compliance history should serve as a basis for determining the disposition type. The Entity does not have relevant compliance history related to CIP-002-5.1a R2, however the Entity has had multiple violations for CIP-002-5.1a R1, a closely related requirement.

Texas Reliability Entity, Inc. (Texas RE) FFT CIP

Mitigation	To mitigate this noncompliance, the Entity took the following actions: • to end the noncompliance the Entity acquired CIP Senior Manager (or delegate) approval of its identifications required in CIP-002-5.1a R1; and • to determine the scope of the noncompliance the Entity performed an extent of condition review. This review subsequently led to the Entity submitting this self-report to Texas RE. To mitigate this noncompliance the Entity will take the following actions: • to prevent reoccurrence of this noncompliance the Entity will, by June 30, 2020, update its processes to standardize the review, validation, and approval process of evidence for CIP-002-5.1a R2; • to prevent reoccurrence of this noncompliance the Entity will, by June 30, 2020, review its CIP-002 Training module, determine if updates are needed, and if applicable implement said updates; • to prevent reoccurrence of this noncompliance the Entity will, by June 30, 2020, if applicable, identify the individuals that need to receive the updated training module; • to prevent reoccurrence of this noncompliance the Entity will, by September 30, 2020, communicate process and procedure changes to applicable personnel; • to prevent reoccurrence of this noncompliance the Entity will, by September 30, 2020, train process and procedure changes to applicable personnel; and • to prevent reoccurrence of this noncompliance the Entity will, by December 18, 2020, create a knowledge transfer process related to work management within the CIP Program Management department.

Texas Reliability Entity, Inc. (Texas RE) 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
TRE2019021360	CIP-002-5.1a	R1	[redacted] (the "Entity")	[redacted]	11/13/2018	01/14/2019	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On April 11, 2019, the Entity submitted a Self-Report stating that, as a [redacted] it was in noncompliance with CIP-002-5.1a R1. In particular, the Entity reported that it had failed to identify each medium impact BES Cyber System (BCS) in accordance with CIP-002-5.1a R1.2. Specifically the Entity implemented a planned change at [redacted] which resulted in the creation of new BCS. The BCS meet the 2.5 impact criteria as defined in CIP-002-5.1a Attachment 2 Section 1, and as such the BCS were required to be identified as medium impact and provided the applicable cyber security protections described in CIP-004 through CIP-011. The root causes of this noncompliance were a weak preventative control and a lack of existing detective controls. The affected [redacted], and as such not all [redacted]. Entity staff correctly documented that they were adding a [redacted]. However [redacted] could have a CIP impact. This noncompliance started on November 13, 2018, when the Entity [redacted] and associated devices into service, and ended on January 14, 2019, which is the earliest dated documentation showing the list of applicable BCS and referencing them as meeting the medium impact criteria.
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. Entity specific factors that increase the risk posed by this noncompliance: • the Entity [redacted]; • the Entity has medium impact BCS and ICCP [redacted]; • the Entity is planning on or currently [redacted]; • the Entity [redacted] • the Entity [redacted]; and • the Entity [redacted]. Entity specific factors that reduce the risk posed by this noncompliance: • the Entity [redacted]. Factors specific to this noncompliance that increase risk: • the affected BCS are capable of impacting the BCS owned by a separate entity; and • due to the noncompliance, the Entity failed to implement numerous required physical and cyber security controls, including: o the Entity did not have a Physical Security Perimeter protecting applicable Cyber Assets; o the Entity did not have a defined Electronic Security Perimeter; o the Entity did not implement remote access through an Intermediate System; o the Entity did not implement security event monitoring; and o the Entity did not record baseline documentation for applicable Cyber Assets. Factors specific to this noncompliance that reduce risk: • the noncompliance was short, lasting 76 days; • the affected BCS represent less than 3% of the Entity's medium impact BCS; and • 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 took the following actions: 1) to end the noncompliance, the Entity identified the BCS [redacted];

	2) to prevent reoccurrence of this noncompliance, the Entity created a new detective control. Specifically, the Entity's [redacted] team reviews approved projects on a monthly basis and determines if the projects have any potential CIP impact; 3) to prevent reoccurrence of this noncompliance, the Entity modified an existing preventative control. Specifically, the Entity has clarified that it is mandatory to consult a CIP SME when making design changes that may have a CIP impact; 4) to ensure no other instances of noncompliance were occurring, the Entity performed an Extent of Condition review; and 5) the Entity has implemented applicable CIP protections to the affected BCS. Texas RE has verified the completion of all mitigation activity.

Texas Reliability Entity, Inc. (Texas RE) 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
TRE2017018670	CIP-010-2	R1; R1.1, R1.2, R1.4, R1.5	[redacted] (the "Entity")	[redacted]	7/1/2016	5/11/2020	Compliance Audit	Completed

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

During a Compliance Audit conducted from [redacted] Texas RE determined that the Entity, as a [redacted] was in noncompliance with CIP-010-2 R1. The Compliance Audit identified three separate instances of noncompliance. Additionally, the Entity identified a fourth instance of noncompliance while performing mitigating activities related to the Compliance Audit's findings.

Regarding the first instance, prior to applying changes that deviated from the existing baseline configuration for [redacted] Cyber Assets, comprising [redacted] BES Cyber Assets (BCAs) and [redacted] Protected Cyber Assets (PCAs), the Entity did not approve changes and did not test the changes in a test or production environment, in noncompliance with Parts 1.2 and 1.5 respectively. Specifically, on July 13, 2017, [redacted] Cyber Assets downloaded an unapproved update for the Entity's antivirus software when the installed version expired in noncompliance with Part 1.2. Because of the unplanned nature of the update, the Entity also did not perform the verifications required by Part 1.5 prior to this change. Shortly after becoming aware of the issue, the Entity disabled the setting so that antivirus clients would only download approved software updates from the Entity's internal update management server. To end the noncompliance, the Entity documented updated baselines and the review of the required cyber security controls for [redacted] Cyber Assets at issue between July 26, 2017 and August 2, 2017.

Regarding the second instance, the Entity did not timely document a compliant initial baseline configuration for [redacted] devices, in noncompliance with Part 1.1. In particular, for [redacted] Intrusion Prevention System (IPS) devices, the Entity's initial baselines did not include the operating system version. In addition, the Entity failed to document the initial baselines for [redacted] Cyber Assets by July 1, 2016 as required. To end the noncompliance, the Entity documented the applicable initial baselines for these [redacted] Cyber Assets between August and October 2016. In addition, the Entity revised the baselines for the [redacted] IPS devices at issue on November 20, 2017. Finally, the Entity performed an extent of condition review of all of the devices with baselines managed by the Entity's baseline management software.

Regarding the third instance, for changes during July 1, 2016 to May 7, 2018 that deviated from the existing baseline configuration, the Entity did not document the determination of the required cyber security controls in CIP-005 that could be impacted prior to the change, as required by CIP-010-2 R1, Part 1.4. In particular, the Entity's process documentation included a list of cyber security controls in CIP-005 and CIP-007, but the documentation stated that the cyber security controls in CIP-005 were only applicable to Electronic Access Control and Monitoring System (EACMS) devices. On May 7, 2018, the Entity documented the required cyber security controls by revising its process documentation to state that the listed controls relating to CIP-005 are applicable to High Impact and Medium Impact BES Cyber Systems and associated PCA, EACMS, and Physical Access Control System (PACS) devices, consistent with Part 1.4's list of applicable systems.

Regarding the fourth instance, while performing mitigating activities for the Compliance Audit findings, the Entity identified [redacted] additional devices with incomplete baselines in noncompliance with CIP-010-2 R1, Part 1.1. Specifically, on May 20, 2020, the Entity reported that the custom script used to update baselines for certain devices was not correctly programmed to retrieve the version number for the installed antivirus software. This issue affected [redacted] BCAs and [redacted] PCAs from July 1, 2016 until May 11, 2020, when the baselines were revised using a corrected script.

The root cause of this issue is that the Entity did not have a sufficient process for compliance with CIP-010-2 R1. Regarding the unplanned update to antivirus clients, the Cyber Assets were configured to automatically update when the installed version expired. Regarding the Cyber Assets with untimely or incomplete initial baselines, the Entity relied on an inaccurate script to create baselines for IPS devices and did not have a procedure that included a sufficient review of baselines for new Cyber Assets. Regarding the insufficient documentation of CIP-005 and CIP-007 controls, the Entity's process did not identify that changes to PCAs, EACMS, BCAs or PACs could also affect related CIP-005 controls. Finally, regarding the devices affected by the missing antivirus version information, the Entity had inadequate controls to ensure its configuration tool accurately documented the applicable information.

This noncompliance started on July 1, 2016, when CIP-010-2 R1 became enforceable and the Entity did not have complete baselines for all applicable Cyber Assets, and ended on May 11, 2020, when the Entity revised the final applicable baseline using a corrected script.

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 posed by implementing changes without completing the requisite change management activities, including testing security controls, is that the change could introduce vulnerabilities in the system. In addition, the Entity's out-of-scope corporate devices, which were configured to use the software vendor's server as a secondary source for updates when the installed software version expired, caused a significant increase in network traffic, resulting in temporary performance issues for the Entity's internal network. Although the network congestion did not affect the Entity's in-scope devices, this issue could have prevented the Entity's personnel from logging in to and operating the Entity's BCAs, which are part of a control center associated with a High Impact BES Cyber System. Similarly, failing to document controls to be tested prior to applying a change could result in the Entity's devices or controls failing to operate as intended. However, the risk posed by this issue is reduced by the following factors. First, the Entity's [redacted] has a [redacted], comprising [redacted] and approximately [redacted]. The Entity's [redacted]

	[redacted] The Entity also [redacted] Second, although the Entity did not test its cyber security controls before the unplanned update to the Entity's antivirus software clients, the Entity subsequently documented a review of its controls and did not identify any controls that were adversely affected. Third, regarding the devices with incomplete or untimely created initial baselines, the Compliance Audit did not identify any missed security patches or unauthorized changes applied to these devices. Fourth, regarding the devices affected by the missing antivirus version information, the issue had a limited scope, affecting only the documentation of the software version number for a single software and for a limited number of vendor systems. The Entity noted that anti-malware software was installed and working on the Cyber Assets. No harm is known to have occurred. Texas RE determined the Entity's and its affiliates' compliance history should not serve as a basis for aggravating the risk posed by this issue. The Entity's and its affiliates' relevant compliance history comprises one prior instance, [redacted], in which an affiliate experienced a similar fact pattern as the instant noncompliance. However, this prior instance is not considered to be aggravating because the Entity and its affiliates discovered and mitigated the prior instance when they were reviewing their compliance processes as part of their activities to address the instant noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) documented updated baselines for the Cyber Assets that had received the unplanned baseline change and documented the review of the required cyber security controls; 2) documented compliant baselines for the Cyber Assets that had late or incomplete baselines and completed an extent of condition review of Cyber Assets managed by the Entity's baselining software; 3) documented updated baselines for the devices affected by the missing antivirus version information; 4) documented the required cyber security controls by revising its process documentation to state the listed controls relating to CIP-005 are applicable to High Impact and Medium Impact BES Cyber Systems and associated PCA, EACMS, and PACS devices; 5) revised its baselining and configuration change management procedure; 6) communicated the revised procedure to the Entity's personnel and conducted training; 7) revised the script used to generate baselines for IPS devices and the script used to create baselines for the devices affected by the missing antivirus version information; 8) developed a work instruction, including an appendix instructing to disable secondary server download setting for antivirus clients; 9) assigned personnel to receive recurring reports regarding software installed on the devices affected by the missing antivirus version information and to confirm the relevant baselines are complete; and 10) created a quarterly process to review the actual installed software on the devices affected by the missing antivirus version information. Texas RE has verified the completion of all mitigation activity.

Texas Reliability Entity, Inc. (Texas RE) 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
TRE2018020245	CIP-007-6	R1; R1.1	[redacted] (the "Entity")	[redacted]	07/01/2016	01/13/2020	Compliance Audit	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	During a Compliance Audit conducted per an existing multi-region registered entity agreement from [redacted], Texas RE determined that the Entity, as a [redacted] was in noncompliance with CIP-007-6 R1. In particular, for 13 Cyber Assets the Entity was unable to demonstrate that only logical network accessible ports that had been determined by the Entity to be needed were enabled. The root cause of this noncompliance was a lack of preventative and detective controls. The Entity's documented process established that only required logical network accessible ports and services would be enabled. The documented process also established that any changes to enabled ports must follow the Entity's change management process. However, the documented process did not specify any means by which the Entity would detect or correct enabled logical network accessible ports that were missing documented justifications. This noncompliance started on July 1, 2016, when CIP-007-6 R1.1 became enforceable, and ended on January 13, 2020, when all enabled logical network accessible ports were documented.
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. Entity specific factors that increase the risk posed by this noncompliance: • the Entity has medium impact BCS with [redacted]; • the Entity [redacted]; and • the Entity [redacted]. Entity specific factors that reduce the risk posed by this noncompliance: • less than 25% of the Entity's System Operators have less than 5 years of System Operator experience; and • the Entity does not have any responsibilities during system restoration. Factors specific to this noncompliance that increase risk: • the duration of the noncompliance was long, lasting 3 years, 6 months, and 12 days; • the time between the Entity becoming aware of the noncompliance and the noncompliance ending was long, lasting 1 year, 5 months, and 5 days; and • the time between the Entity becoming aware of the noncompliance and the Entity implementing a control to prevent reoccurrence of the noncompliance was long, lasting 1 year, 8 months, and 22 days. Factors specific to this noncompliance that reduce risk: • the noncompliance was administrative in nature. The Entity did not identify any ports which needed to be disabled; and • 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 took the following actions: 1) to end the noncompliance the Entity updated its documentation of enabled logical network accessible ports to include the business justification for each port; 2) to end the noncompliance the Entity decommissioned a device that did not have business justifications for each enabled logical network accessible port; and 3) to prevent reoccurrence of this noncompliance the Entity modified its documented process to include an internal review step to ensure the justifications for open ports are documented.

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 Find, Fix, Track, and Reports 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	MRO2018019141	Yes		Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2-12: 2 years
2	RFC2019021654	Yes		Yes	Yes									Category 1: 3 years; Category 2-12: 2 years
3	TRE2019022002	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2-12: 2 years
4	WECC2016015678			Yes	Yes					Yes				Category 1: 3 years; Category 2-12: 2 years
5	WECC2018019396			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
MRO2018019141	CIP-007-3a	R6	[redacted] (the Entity)	[redacted]	05/17/2016	07/21/2017	Self-Log	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On December 13, 2017, the Entity submitted a Self-Log stating that, [redacted], it was in noncompliance with CIP-007-6, R4. The Self-Log included three instances of noncompliance; the noncompliance dates for the third instance falls under CIP-007-3a R6, so the standard these are all being processed under has been adjusted to CIP-007-3a R6. After subsequent review, MRO determined that the noncompliance posed a moderate risk to the reliability of the bulk power system and adjusted the processing method. In the first instance of noncompliance, the Entity determined that it had an issue with CIP-007-6 P4.1 because security event logging was not configured for [redacted] BES Cyber Assets (BCAs) and [redacted] Protected Cyber Assets (PCAs) across [redacted]. The BCAs are [redacted] relays [redacted]. The PCAs are [redacted] relays for 115kV systems (which qualifies them as low impact BCAs) that also [redacted]. The noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on July 21, 2017, when the necessary settings were updated. In the second instance of noncompliance, the Entity determined that it had an issue with CIP-007-6 P4.2 due to detection alerting of the failure of security event logging was not configured for [redacted]. The noncompliance began on July 1, 2016, when the requirement became enforceable, and ended on July 21, 2017, when the necessary settings were updated. In the third instance of noncompliance, the Entity determined that it had an issue with CIP-007-3a R6 P4.3 because it failed to maintain 90 days of stored security event logs for [redacted] PCAs, all of which [redacted] containing additional PCAs. The Entity's design for implementing a reliable 90-day local log retention was not properly configured to store 90 days or more of required logging. The noncompliance began on May 17, 2016, when the PCAs went into service with inadequate log retention settings, and ended on May 11, 2017, when the Entity properly configured the local log retention to perform required logging. The start date of this instance of noncompliance makes this issue a CIP-007-3a R6 R4.3 issue. The cause of the noncompliance for all instances was the Entity's Cyber Asset deployment process documentation lacked the level of detail necessary to guide the Entity's staff responsible for configuring the logs to perform the steps necessary to configure security event logging, security event alerting, and security event log retention. The aggregate of noncompliance began on May 17, 2016, when the third instance of noncompliance began, and ended on July 21, 2017, when all necessary settings 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. The first instance was moderate because the noncompliance lasted longer than a year, impacted a significant number [redacted] of BCAs and all of the Entity's substations that contain [redacted]. However, MRO determined that this instance posed a risk less than serious or substantial because the impact of this noncompliance is limited to being the absence of an informational, log-based detective control and the issue affected fewer than [redacted] of the Entity's protective relays. The second and third instances were minimal because of the limited scope of the instances of noncompliance. Additionally, for the third instance, the Entity reported that when the Entity discovered this issue, the logging retention function was operational and retaining logs, but did not retain a full 90 days of logs due to an incorrect assessment of the storage requirements. No harm is known to have occurred. The Entity has no relevant history of noncompliance; however, MRO processed a prior instance of noncompliance associated with CIP-006-6 R2 [redacted] that was concurrent with the current instance.
Mitigation	To mitigate the first instance of noncompliance, the Entity: 1) corrected the settings for the relays, which enabled logging; and 2) updated its device management document, describing how to configure the logging feature for relays. To mitigate the second instance of noncompliance, the Entity: 1) corrected the settings for the relays, which enabled alerting; and 2) updated its device management document, describing how to configure the alerting feature for relays. To mitigate the third instance of noncompliance, the Entity: 1) updated the device's local logging settings to include 90 days of log retention; 2) updated the documented procedures about log retention for applicable devices; and 3) trained applicable personnel on the updated procedures and re-enforce the logging requirements. MRO verified the completion of the mitigation activity associated with the first instance of noncompliance because it was determined to be a moderate risk issue.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021654	CIP-007-6	R2	[redacted]	[redacted]	10/2/2017	3/15/2019	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On June 3, 2019, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-007-6 R2. On December 5, 2018, as part of a separate investigation, the entity discovered one applicable security patch released on October 1, 2018, that it did not evaluate within a 35-calendar-day interval. Since it did not complete an evaluation, the entity also did not (a) apply the patch or (b) create or revise a plan to mitigate the vulnerabilities addressed by the patch. The patch was associated with one of the technologies that the entity uses for cyber security event monitoring. The entity evaluated the patch on December 5, 2018 (i.e., 30 days late), and created a plan to mitigate the vulnerabilities addressed by the patch on January 2, 2019. On January 14, 2019, the entity applied the patch. The entity performed a comprehensive review of patches for cyber security event monitoring technologies that had been released since July 1, 2016, and discovered four additional instances of noncompliance. In each additional instance, the entity did not evaluate a patch and, therefore, did not (a) apply the patch or (b) create or revise a plan to mitigate vulnerabilities addressed by the patch. The additional instances are summarized as follows: (a) a patch was released on August 28, 2017, and was no longer applicable as of November 16, 2017, because the entity installed a new product version, which eliminated the vulnerability associated with the patch; (b) a patch was released on August 30, 2017, and was no longer applicable as of November 16, 2017, because the entity installed a new product version, which eliminated the vulnerability associated with the patch; (c) a patch was released on September 6, 2018, and was no longer applicable as of March 15, 2019, because the entity installed a new product version, which eliminated the vulnerability associated with the patch; and (d) a patch was released on October 16, 2018, and was no longer applicable as of March 15, 2019, because the entity installed a new product version, which eliminated the vulnerability associated with the patch. Collectively, the missed patches were applicable to [redacted] devices. The root causes of this noncompliance were a process failure and insufficient training. Entity personnel were reviewing patches every three weeks in a recurring meeting but failed to identify the patches referenced herein, in part, because they were not filtering the vendor's website correctly. And, the entity failed to identify and correct the instances of noncompliance through existing detective controls (i.e., the issues were identified and corrected by happenstance). The noncompliance involves the management practice of workforce management. Workforce management includes, in part, the development and implementation of clear, thorough, and repeatable processes, procedures, work instructions, and controls. Such efforts can (a) minimize the frequency of the types of issues experienced in this case and (b) assist in identifying and correcting them in a more timely manner. The noncompliance involved five separate instances with the following durations: (a) The first instance started on October 2, 2017, when the entity failed to evaluate a patch and ended on November 16, 2017, when the entity installed a new product version; (b) The second instance started on October 4, 2017, when the entity failed to evaluate a patch and ended on November 16, 2017, when the entity installed a new product version; (c) The third instance started on October 11, 2018, when the entity failed to evaluate a patch and ended on March 15, 2019, when the entity installed a new product version; (d) The fourth instance started on November 5, 2018, when the entity failed to evaluate a patch and ended on December 5, 2018, when the entity evaluated the patch; and (e) The fifth instance started on November 20, 2018, when the entity failed to evaluate a patch and ended on March 15, 2019, when the entity installed a new product version.
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of bulk power system (BPS) based on the following factors. Errors in patch management allow known vulnerabilities to persist in an entity's environment, and a bad actor could leverage those vulnerabilities and cause harm to the BPS. Here, the risk was not serious or substantial because each discrete instance was relatively short in duration, and existing controls in the entity's environment reduced the risks associated with the missed patches (e.g., firewall protections, access controls, and multi-factor authentication). However, the risk was not minimal in this case because it involved several instances of noncompliance that affected [redacted] that perform critical cyber security event monitoring functions. Further, this noncompliance involved process failures and a lack of sufficient detective controls. No harm is known to have occurred. The entity has relevant compliance history. A majority of the entity's prior noncompliances involved separate and distinct issues as well as different root causes. While one of the prior noncompliances involved conduct that is arguably similar to the instant noncompliance, ReliabilityFirst determined that the instant noncompliance does not warrant a penalty because the current issue posed only a moderate risk to the BPS, involves high frequency conduct, and is not indicative of a systemic or programmatic failure.
Mitigation	To mitigate this noncompliance, the entity: 1) evaluated and documented the initial missed patch identified in the self-report; 2) conducted a comprehensive review of all cyber security patches released since July 1, 2016, for cyber security event monitoring technologies (note: the entity discovered the four additional missed patches described herein that had all been superseded by product version upgrades); 3) centralized primary responsibility for coordinating the evaluation of security patches; and 4) provided training on the new process enhancements for personnel who will be responsible for patch evaluations.

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
RFC2019021654	CIP-007-6	R2	[redacted]	[redacted]	10/2/2017	3/15/2019	Self-Report	Completed
			ReliabilityFirst has verified the completion of all mitigation activity.					

Texas Reliability Entity, Inc. (Texas RE) 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
TRE2019022002	CIP-004-6	R5; R5.1; 5.3; 5.5	[redacted] (the "Entity")	[redacted]	O5/29/2017	08/01/2018	Compliance Audit	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	During a Compliance Audit from [redacted], Texas RE determined that the Entity, as a [redacted] was in noncompliance with CIP-004-6 R5. Specifically, the Entity did not remove the unescorted physical access and Interactive Remote Access of three employees within 24 hours of termination actions under CIP-004-6 R5.1. Further, the Entity did not remove access to the designated BES Cyber System Information (BCSI) storage locations for three employees after termination within the next calendar day pursuant to CIP-004-6 R5.3. Finally, for one employee, the Entity did not change the password for a shared account known to one user within 30 calendar days of the termination action, under CIP-004-6 R5.5. The root cause of each instance for the CIP-004-6 R5.1 and CIP-004-6 R5.3 noncompliances was from a supervisor either filing the wrong revocation request date or not timely requesting revocation. The root cause of the CIP-004-6 R5.5 instance was that a manual alerting mechanism failed to send alerts to the appropriate personnel, and the Entity did not collect the evidence of the password changes. This noncompliance started on May 29, 2017, which, for the CIP-004-6 R5.5 noncompliance, is 31 days after an employee left the company without his or her password being changed, and ended on August 1, 2018, when, for the CIP-004-6 R5.1 and 5.3 noncompliances, a terminated employee whose unescorted physical access, Interactive Remote Access, and access to the designated BCSI storage locations was not removed within 24 hours had their access removed.
Risk Assessment	This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Entity's failure to remove users' unauthorized access within the Standard's specific time period and change the password for a shared accounts for terminated employees increases the risk of compromise to the Entity. The Entity's [redacted]. The risk of the noncompliance is lessened by a few factors: (1) the employees' physical access had been revoked within 24 hours of termination. All physical access badges and electronic devices were returned to the Entity; (2) the terminated employees' cyber and physical access to all in-scope devices and BCSI was revoked within 24 hours of termination. Thus, the employees had no access to in-scope assets or data. The assets and data all reside within secure areas providing "defense in depth." Additionally, the Entity's buildings in question are all protected by various levels of security (card key readers, guards, etc.). Further, the durations of inappropriate access under CIP-004-6 R5.1 and CIP-004-6 R5.3 was relatively short for those three employees at one day, 22 days, and 31 days. The duration of the CIP-004-6 R5.5 noncompliance was also relatively short, at 34 days. No harm is known to have occurred. Texas RE considered the Entity's compliance history and determined there was one relevant instances of noncompliance for CIP-004-6 R5.1, with a substantially similar root cause. Therefore, Compliance Exception treatment is not appropriate here.
Mitigation	To end this noncompliance, the Entity: 1) removed the individuals' unescorted physical access to PSPs, Interactive Remote Access, and access to the designated BCSI storage locations for the three employees at issue; and 2) provided evidence that passwords for accounts on the [redacted] were changed. To prevent reoccurrence of this noncompliance: 1) for the R5.1 and 5.3 noncompliances, the Entity implemented a new access management tool as its onboard/offboard/transfer/reassignment tool. With this tool, supervisors cannot initiate the off-boarding process without first submitting a proper access revocation request; and 2) for the R5.5 noncompliance, the Entity implemented a tool that will detect the failures of its alerting mechanism. Texas RE 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
WECC2016015678	CIP-006-3c	R5	[redacted]	[redacted]	2/26/2015	9/28/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On April 19, 2016, the entity submitted a Self-Report stating that, as a [redacted], it was in potential noncompliance with CIP-006-3c R5. Specifically, in April 2016, during a review of physical security logs, the entity discovered that the security company it had contracted with to perform offsite monitoring of the Physical Security Perimeter (PSP) at [redacted] of its [redacted] had not reviewed all of the physical security logs for the [redacted] access point door alarms to the Physical Security Perimeter (PSP) controlling access to a Medium Impact BES Cyber System (MIBCS) located at a [redacted] since February 26, 2015. During discussions of this issue with the security company, the entity learned that the security company was unable to staff qualified personnel with an appropriate head-count to perform the review of logged alarm events. Upon learning of the deficiency, the entity immediately terminated its contract with the security company and contracted with another security company. This issue began on February 26, 2015, when the first physical access attempt was not immediately reviewed and handled per the entity's procedures and ended on September 28, 2017, when the entity completed mitigating activities. The root cause of the issue was attributed to too few workers assigned to the tasks. Specifically, the vendor the entity contracted with did not provide an adequate number of skilled staff to perform the obligations required to monitor, respond to, or escalate events or incidents at the PSPs.
Risk Assessment	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 immediately review and handle unauthorized access attempts in accordance with its procedures specified in CIP-008-3, as required by CIP-006-3c R5, for [redacted] access points to the PSPs controlling access to a MIBCS. Failure to review unauthorized access attempts could have resulted in unauthorized physical access to the PSPs to go unnoticed and unchecked, thereby potentially allowing access to Cyber Assets by someone intent on doing harm. However, as compensation, the entity had implemented internal controls to prevent potential unauthorized physical access occurrences, which included [redacted] personnel, 24 hours, seven days-a week control room staffing, and policies and procedures that restricted access to only authorized personnel. Additionally, the entity did not experience any physical security events or incidents during the duration of noncompliance. No harm is known to have occurred. WECC determined that the entity's compliance history should not serve as a basis for applying a penalty because the previous noncompliance had a different root cause and fact pattern, and the mitigation activities would not have prevented the current issue.
Mitigation	To mitigate this violation, the entity: 1) hired a new security company to monitor the PSP at the generation facility; 2) modified the contract to require that the contractor perform a PSP door alarm review at the end of each shift. The reviewer will look for any missed door alarms during the shift and initiate the appropriate response; 3) established a weekly review of PSP door alarms by its personnel who will investigate any alarms that were missed by the contract security guards; and 4) established a policy to make sure that failed PACS components that cause false door alarms are corrected in a timely fashion, to include maintaining a stock of PACS components that are known to be failure prone to allow for timely repairs. Reducing the false door alarms will allow the guards more time to respond to valid alarms.

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
WECC2018019396	CIP-006-3c	R4	[redacted]	[redacted]	12/29/2015	9/26/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On March 15, 2018, the entity submitted a Self-Report stating that, as a [redacted], it was in potential noncompliance with CIP-006-3c R4. Specifically, as the result of a component failure at [redacted] Physical Security Perimeter (PSP) doors controlling access to a Medium Impact BES Cyber System (MIBCS) located at a [redacted], nuisance alarms filled the Physical Access Control or Monitoring Screens (PACS) screens. To prevent the screens from filling up with these nuisance alarms, entity staff masked the alarms, that is configured the PACS to ignore them. While masked, the alarms did not register at the PACS, and the doors could be forced open without the entity being aware. [redacted], which the entity did not do during the time the masking was in place. There were two separate instances where the entity [redacted] to monitor access; the first instance began on December 29, 2015 and the second instance on September 1, 2017. These instances ended on March 3, 2017 and September 26, 2017, when masking was removed from the PSP door alarms. The root cause of the issue was attributed to inadequate training. Specifically, although the entity had a documented policy which [redacted], the personnel responsible for the masking in this instance were not aware of the policy.
Risk Assessment	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 adequately implement its operational and procedural controls to manage physical access at all access points to the PSP twenty-four hours a day, seven days, a week, for [redacted] PSP access points as required by CIP-006-3c R4. Failing to create alarms for PSP doors controlling access to MIBCS could have resulted in the entity being unaware of unauthorized access into that PSP by someone with malicious intent to cause damage to the MIBCS to affect reliability of the BPS. However, as compensation, some of the Cyber Assets were within view of the Chief Operator's desk, and the [redacted] was protected by [redacted], both of which were manned 24 hours, seven days-a-week. No harm is known to have occurred. WECC determined that the entity's compliance history should not serve as a basis for aggravating the disposition track. The prior one relevant compliance history had a different fact pattern and root cause and is not indicative of a broader issue. The mitigation activities of the previous noncompliance would not have prevented the current issue.
Mitigation	To mitigate this issue, the entity has: 1) removed the masking from the PSP doors of this issue; 2) reduced the number of PSPs by one when it moved the Cyber Assets into another PSP and updated its Physical Security Plan accordingly; and 3) updated personnel on the requirements related to masking PSP doors and alarming.

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 Find, Fix, Track, and Reports 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	MRO2018019130			Yes	Yes					Yes				Category 2 – 12: 2 years
2	RFC2019021832	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
3	SERC2017017559			Yes	Yes					Yes	Yes		Yes	Category 2 – 12: 2 years
4	SERC2017018662			Yes	Yes				Yes	Yes			Yes	Category 2 – 12: 2 years
5	SERC2018019419			Yes	Yes					Yes	Yes			Category 2 – 12: 2 years
6	FRCC2019021601	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
7	FRCC2019021602	Yes		Yes	Yes					Yes	Yes			Category 2 – 12: 2 years
8	TRE2017018208	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
9	TRE2017018673	Yes		Yes	Yes					Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 year
10	WECC2017017464	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 years
11	WECC2017017465	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 years
12	WECC2017017511	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
13	WECC2017018579			Yes	Yes					Yes				Category 2 – 12: 2 years
14	WECC2017017466	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
15	WECC2017017467	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
16	WECC2017017468	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
17	WECC2017017469	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
18	WECC2017017470	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
19	WECC2017017471			Yes	Yes					Yes				Category 2 – 12: 2 years
20	WECC2017017472	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
21	WECC2017017891			Yes	Yes					Yes				Category 2 – 12: 2 years

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
MRO2018019130	CIP-010-2	R3	[redacted] (the Entity)	[redacted]	07/01/2017	06/29/2018	Self-Log	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On December 1, 2017, the Entity submitted a Self-Log stating that, as a [redacted], it was in noncompliance with CIP-010-2 R3.1. After subsequent review, MRO determined that the noncompliance posed a moderate risk to the reliability of the bulk power system and adjusted the processing method. The Entity determined that it failed to complete a paper or active vulnerability assessment within the first 12 months as required in the CIP V5 implementation plan. This issue affected [redacted] of the Entity's high and medium impact BES Cyber Assets (BCAs) and Protected Cyber Assets (PCAs), Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS) associated with high and medium BES Cyber Systems (BCS). The cause of the noncompliance was that the Entity's process lacked the level of detail required by CIP V5 standard and requirement. The noncompliance began on July 1, 2017, when the Entity failed to conduct an active vulnerability assessment within the 12-month initial performance period specified in the CIP V5 Implementation Plan, and ended on June 29, 2018, when all vulnerability assessments were 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. The noncompliance was moderate and not serious or substantial because the delay in performing the vulnerability assessments did not extend longer than one assessment period. Observations made during an entity's vulnerability requirement under this requirement part are checks against the Entity's previous work for conforming to other requirements which reduced the risk because this is a detective control and does not introduce additional security protections. The risk was not minimal because the issue affected [redacted] of the Entity's applicable medium and high BCS. Until the noncompliance was ended, the overall security posture of affected Cyber Assets was not known and the proper implementation of cyber security controls was not ensured. Additionally, the time from discovery and the task of adjusting its vulnerability assessment process for CIP V5 was not addressed for a period in excess of ten months. When the Entity completed the vulnerability assessments, [redacted] potential issues were discovered. The delay in conforming to this requirement therefore caused the discoveries of those potential issues to be made over 11 months later than they would have been had the Entity performed the task within schedule requirements. No harm is known to have occurred. The Entity has no relevant history of noncompliance.
Mitigation	To mitigate the noncompliance, the Entity: 1) performed the required Vulnerability Assessments; 2) updated its CIP Cyber Security Plan for Vulnerability Assessments; and 3) trained its staff on the revised CIP Cyber Security Plan.

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
RFC2019021832	CIP-004-6	R4	[redacted]	[redacted]	3/13/2019	5/24/2019	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On July 11, 2019, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-004-6 R4. An entity administrator did not follow the entity's process for granting a part-time employee access to CIP-scoped systems and information on March 13, 2019, in violation of CIP-004-6 R4.1. As a result, the entity did not complete a personnel risk assessment (PRA) prior to provisioning access (CIP-004-6 R3), and the part-time employee did not complete requisite training prior to obtaining access (CIP-004-6 R2). The administrator granted the part-time employe [redacted] No access was granted to the [redacted] The part-time employee was hired on a temporary basis as an intern and separated from the entity on May 24, 2019, on good terms upon completion of scheduled work. The entity discovered the noncompliance while executing its access revocation procedure upon separation. The root cause of this noncompliance was the administrator's lack of understanding of the entity's process for granting access. This noncompliance implicates the management practice of workforce management. Workforce management includes the need to ensure that staff are adequately trained and capable of carrying out their tasks and responsibilities in a manner that minimizes the risk to the reliability of the bulk power system (BPS). This noncompliance started on March 13, 2019, when the administrator did not follow the entity's process for granting access, and ended on May 24, 2019, when the entity revoked the part-time employee's access.
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS based on the following factors. There is an increased risk of an individual obtaining improper access, misusing access, or failing to adhere to security practices when an entity fails to: (a) follow a process to authorize access; (b) complete a PRA prior to granting access; and (c) require the completion of training prior to granting access. The risk was not minimal in this case because of the lack of requisite qualifications (i.e., no training or PRA) coupled with the type of access that was provisioned (i.e., access to [redacted]). Additionally, the circumstances under which this noncompliance arose were problematic, namely an administrator neglecting to follow (or failing to understand the importance of) the entity's policies and procedures when provisioning heightened access privileges. However, the risk was not serious or substantial based upon the following facts. No access was granted to [redacted]. The part-time employee's access to [redacted] did not include the ability to [redacted]. Further, even though it was not as thorough as a CIP-based PRA, the entity did complete a standard pre-employment background check prior to hiring the part-time employee. The entity reviewed records and could not find evidence that the part-time employee accessed [redacted] during the course of his temporary employment. The potential harm to the overall BPS was also minimized based upon [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 involved separate and distinct issues with different underlying causal factors.
Mitigation	To mitigate this noncompliance, the entity: 1) disabled the part-time employee's administrator account within an hour of the notification of departure from the entity; 2) sent out a reminder e-mail to all corporate domain administrators to reinforce the requirements [redacted] and 3) retrained all corporate domain administrators on [redacted], including the necessity for a personnel risk assessment and training.

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
SERC2017017559	CIP-010-2	R1	[redacted]	[redacted]	7/1/2016	Present	Compliance Audit	8/31/2020 Expected Date

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	During a Compliance Audit conducted from [redacted], the SERC Audit team determined that the Entity, as a [redacted] was in noncompliance with CIP-006-6 R1. The Audit Team Determined that the Entity's hardware/hypervisors that host virtual Physical Access Control System (PACS) workstations were not identified and protected as PACS. However, after reviewing additional evidence, SERC determined that this finding is not a noncompliance with CIP-006-6 R1, but is instead a noncompliance with CIP-010-2 R1, because it did not formally identify the hypervisors as a part of the PACS and did not subsequently establish and require baselines and the applicable CIP-010-2 processes and procedures for the hypervisors that host the PACS workstations. The [redacted] hypervisors host the virtual PACS workstations, and these workstations are used by the Entity to monitor the PACS and to add or remove users for physical access to all existing Entity Physical Security Perimeters (PSPs). For this reason, the hypervisors are components of the PACS, and as such, must be identified and protected as required, including inclusion on the Entity's baseline documentation under CIP-010-2 R1. However, the Entity did not establish and require baselines and the applicable CIP-010-2 processes and procedures for the hypervisors The scope of affected assets included the [redacted] hypervisors and [redacted]. During the same audit, the SERC audit team determined that the Entity was in noncompliance with CIP-005-5 R1. The Audit Team Determined that the Entity's hardware/hypervisors that host virtual Jump Hosts were not identified and protected as Electronic Access Control and Monitoring System (EACMS). However, after reviewing additional evidence, SERC determined that this finding is not a noncompliance with CIP-005-5 R1, but is instead a noncompliance with CIP-010-2 R1 because the Entity did not have established baselines and the applicable CIP-010-2 processes and procedures established for the hypervisors and jump hosts. This noncompliance was assigned violation ID [redacted]. However, because it involved the same Standard and Requirement as the instant issue, SERC Staff is using a single tracking number, [redacted], for both issues and dismissed [redacted]. The [redacted] virtual workstations also served as the Entity's jump host (also known as the intermediate system). The Entity's intermediate system is classified as being part of the EACMS. As such, the Entity should considered the hypervisors and jump hosts when determining the Cyber assets associated with the BCS. The scope of affected assets included the [redacted]s. The extent-of-condition assessment was conducted through the Audit process. The Audit team identified and reported the entire population of PACS hypervisors, PACS virtual workstations, EACMS hypervisors, and jump hosts for the Entity through the Audit team's findings. This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable, and will end on August 31, 2020 when the noncompliance is mitigated. The root causes of this noncompliance were a lack of internal controls and deficient processes and procedures under CIP-010-2 R1. The Entity did not properly consider the hypervisors, virtual PACS workstations, EACMS hypervisors, and jump hosts when determining the Cyber Assets associated with the BCS. This oversight was the result of process and procedures that lacked the internal controls to ensure proper consideration and vetting of all Cyber Assets and the functions these Cyber Assets performed.
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 the hypervisors as PACS and by not including the hypervisors in its baseline documentation, the Entity had the potential risk for the actual running configurations to not be properly maintained within the existing baseline documentation, leading to an opportunity for security controls to be overlooked or not recognized as necessary, permitting unauthorized changes to go unrecognized and untested. However, the Entity encrypted the virtual hard disks for the PACS workstations (the hypervisors). In addition, the Entity physically protected the hypervisors and employed electronic access controls such that outside access was restricted and an unauthorized user could not have gained control of them and operated bulk power system facilities. SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance for the PACS issue, the Entity: 1) replaced the medium EACM servers with physical servers and retired the virtual machines; 2) implemented and enhanced controls necessary to produce the evidence necessary to meet CIP-007 R2 and R5. Corrective activities include: a) including the hypervisor in the security patch management source list; b) updating and verifying password policy and security patch level for the hypervisor; c) updating procedural documentation; and d) identifying evidence and internal controls; and

	3) implemented and enhanced controls necessary to produce the evidence necessary to meet CIP-007 R1 and R4. Corrective activities include: a) installing baseline monitoring software on the hypervisor; b) pulling down initial baseline configuration to document ports and services c) documenting ports and services justifications; d) configuring logging and alerts for the hypervisor e) verifying that logging, alerting, and ports and services monitoring is functioning as intended; f) updating procedural documentation: and g) identify evidence and internal controls; To mitigate this noncompliance for the PACS issue, the Entity will complete the following mitigation activities by August 31, 2020: 1) implement and enhance controls necessary to produce the evidence necessary to meet CIPO-009 R1-R3 and CIP-010 R1 and R3. Corrective activities will include: a) reviewing current plan and modify roles and responsibilities as needed to include the hypervisor; b) updating procedural documentation; c) identifying evidence and internal controls; 2) implement and enhance controls necessary to produce the evidence necessary to meet CIP-010 R1 and R3. Corrective activities will include: a) implementing baseline monitoring for the hypervisor: b) pulling the hypervisor into the existing vulnerability assessment process; c) updating procedural documentation; and d) identifying evidence and internal controls; and 3) verify that the hypervisors met all the applicable CIP requirements, socialize changes, and ensure that the parties responsible for execution understand roles and responsibilities. This includes: a) providing assurance by reviewing and validating that all proposed controls and procedural documents meet the applicable NERC CIP requirements; and b) providing impacted stakeholders (control owners and performers with instruction regarding roles and responsibilities, required activities, and evidence output associated with pulling the hypervisor into the NERC CIP program. To mitigate this noncompliance for the EACM issue, the Entity replaced high EACM intermediary devices and medium EACM servers with physical servers and retired the virtual machines.

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
SERC2017018662	CIP-004-6	R2, P2.3	[redacted]	[redacted]	08/01/2017	02/15/2019	Self-Report	Completed

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

On November 16, 2017, August 23, 2018, and May 6, 2019, the Entity submitted Self-Reports stating that, as a [redacted] it was in noncompliance with CIP-004-6 R2, P2.3. The Entity reported three instances where it failed to maintain annual cyber security training for multiple employees with authorized electronic access and/or physical access to Bulk Electric System Cyber Systems (BCSs).

In Instance 1, on August 2, 2017, the Entity discovered that cyber training had lapsed for seven employees on July 31, 2017, and that its access management system had not initiated automatic revocation of such access. On August 7, 2017, the Entity revoked the access of all seven employees.

The seven employees collectively had electronic and physical access to [redacted]). Affected Cyber Assets included [redacted]

The cause of Instance 1 was a failure to verify that the software was properly functioning. Specifically, during testing of a new software project, an analyst incorporated a new software feature. The CIP access removal logic was an internal portion of the code in the workflow's set of events that gets triggered when an employee or contractor is terminated. When the new feature was introduced, the logic was corrupted and access revocation was automatically applied only to terminated employees.

On August 23, 2018, the Entity submitted an additional Self-Report of CIP-004-6 R2, P2.3 [redacted], which was dismissed and consolidated with the initial November 16, 2017 Self-Report.

In Instance 2, on July 2, 2018, during a quarterly access review, the Entity discovered that on April 27, 2018, the Entity's access management system flagged a contract employee with CIP physical and electronic access whose cyber training had lapsed. The access management system automatically generated an access revocation record to initiate revocation. However, due to a program bug, the software generated a blank summary field, resulting in an invalid input to the next stage in the access revocation process, the change request management system (a work ticketing system) used to manually manage access revocation. The invalid input caused the work ticketing system to not generate a service request for effecting final removal of access by the Entity's [redacted]. As a result, the Entity did not revoke access within 15 calendar months of previous training. The Entity could not determine the cause of the software bug but replaced the software application with a new one on August 13, 2018. The Entity revoked the contractor's access that same day on July 2, 2018.

The scope of affected assets in Instance 2 included [redacted].

The cause of Instance 2 was gaps in procedural controls related to ensuring employees completed training within allotted timeframes. Compensating controls (automatic access revocation via software) were also an issue in that the Entity did not verify that the end-to-end process of automatically detecting and revoking access worked properly at the appropriate time.

On May 6, 2019, the Entity submitted an additional Self-Report of CIP-004-6 R2, P2.3 [redacted], which was dismissed and consolidated with the initial November 16, 2017 Self-Report.

In Instance 3, on February 14, 2019, during a review of a condition report, the Entity identified a CIP user with electronic and physical access past due for CIP training. The user's training was due no later than January 31, 2019.

On February 15, 2019, the Entity conducted an EOC review and determined the issue affected [redacted].

The Entity revoked electronic and physical access for the [redacted] users that same day.

The reason for the large number of affected users was that the Entity was experiencing implementation issues while transitioning to a new software system for managing and revoking access. On August 13, 2018, the Entity replaced its old access management system with a new one. Certain functionality was still pending completion of the upgrade. For approximately two weeks, from August 13, 2018 until September 1, 2018, the new system identified and reported users with lapsed training. However, determinations of access revocation required a manual review. As a result, human errors occurred in reviewing and revoking access due to lapsed training.

	On September 1, 2018, the Entity implemented the automated access revocation feature on the new system. Although it worked properly in a test environment, it did not in the production environment as the Entity did not validate functionality in the production environment once installed. Thereafter, automatic access revocation did not work properly until the instance was discovered on February 14, 2019. The [redacted] CIP users collectively had electronic and physical access to [redacted] The scope of affected Cyber Assets included [redacted] The cause of Instance 3 was a deficient internal control with respect to software development/deployment. The Entity did not test functionality in the production environment prior to releasing the new automated access revocation feature. This noncompliance started on August 1, 2017, the Entity's earliest instance of lapsed training and access not revoked, and ended on February 15, 2019, the Entity's last instance of access revoked due to lapsed training.
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's failure to revoke electronic and physical access to users with lapsed training could allow malicious actors to access and control assets in sensitive networks, install malicious software or backdoors, exfiltrate BCS information, and potentially disrupt, desynchronize or impact data communications necessary for communications and controls. However, the Entity revoked access promptly after discovery. The maximum period of lapsed training was approximately six months, and, valid Personnel Risk Assessments were in place during the violation period for all individuals involved. Additionally, all individuals who were granted access were initially trained and there were no changes in the delivered training. Furthermore, the Entity protected its Cyber Assets with intrusion monitoring and alerting as well as electronic access controls, and operated its system in a manner that accounts for operating contingencies. In all instances, no harm is known to have occurred. SERC considered the Entity's compliance history with CIP-004-6 R2 and determined that there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) removed CIP access from the users until the new training was completed, if applicable (all Instances); 2) corrected the workflow that executes Request Access Change events (Instance 1); 3) implemented and executed a manual daily check/report process (Instance 1); 4) trained users on the manual daily check (Instance 1); 5) reinforced with contractors to renew training within the CIP required timeframes, or to request access revocation if not needed (Instance 2); 6) developed a report which alerts the access management team of any requests which are unresolved beyond three calendar days (Instance 2); 7) implemented automated CIP Access Revocation via Access Review functionality (Instance 3); 8) updated internal on-call designated Work Instructions to perform daily checks to within the system validating the CIP revocation function is performing as expected (Instance 3); 9) developed a Work Instruction for testing after any updates to the application or infrastructure (Instance 3); 10) worked with appropriate teams to implement automated solution to alert Identity Management Systems Support team during failures of critical processes (Instance 3); and 11) updated CIP Training certification expiration timeframe from 15 months to 12 months (Instance 3).

FFT

SERC Reliability Corporation (SERC)

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
SERC2018019419	CIP-010-2	R1 P1.1	[redacted]	[redacted]	07/01/2016	03/15/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			On March 21, 2018, the Entity submitted a Self-Report to SERC stating that, as a [redacted], it was noncompliance with CIP-010-2 R1, P1.1. The Entity did not develop an accurate baseline configuration. On January 23, 2018, while performing its 2018 annual password change process, the Entity discovered [redacted] Protection System relays with incorrect baseline configuration records. Specifically, sometime prior to July 1, 2016, the Entity recorded incorrect firmware versions in the field as indicated in CIP Test Engineer Reports (TER), then transcribed the incorrect versions into the baseline documentation record. On March 15, 2018, the Entity updated baseline configuration documentation for the [redacted] relays. The scope of affected Facilities included [redacted]. Affected Cyber Assets included [redacted]. For the extent-of-condition assessment, during the annual password change conducted in January of 2018, the Entity compared actual firmware versions as pooled in the field on all medium impact BCAs, and compared them with firmware versions indicated in associated TERs. The Entity determined all other TERs reflected the correct versions of firmware. This noncompliance started on July 1, 2016, when the standard became mandatory and enforceable on the Entity, and ended on March 15, 2018, when the Entity updated its baseline configuration documentation. The cause of the noncompliance was inadequate internal controls during the implementation of CIP Version 5. The procedure did not require secondary firmware verification controls to ensure accurate baseline configurations.					
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 reflecting correct versions of firmware in documented baseline configurations of the relays, it could have adversely affected security patch management processes related to checking for new security patches. Hackers could have exploited a security-related vulnerability, impacted a change to relay configurations, and compromised grid security. However, none of the affected Cyber Assets were remotely accessible, and they had no External Routable Connectivity. Tampering required Physical Security Perimeter access, which the Entity had secured. Three of the four relays were not firmware upgradeable, and the Entity employed them in secondary protection schemes. The remaining relay required no updates of firmware because of these oversights and was not a protection relay configured for current interruption. No harm is known to have occurred. SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.					
Mitigation			To mitigate this noncompliance, the Entity: 1) re-ran the CIP TER on the [redacted] relays and recorded the correct firmware values; 2) uploaded the correct firmware versions to the system of record that reflected the approved device baseline; 3) updated the procedures to reinforce the prohibition of manual copying and pasting of data; 4) revised the procedure of baseline retrieval for these device types to include verification controls to ensure accurate, consistent, and efficient collection of baseline data.					

FFT

SERC Reliability Corporation (SERC)

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
FRCC2019021601	CIP-002-5.1	R1, P1.2	[redacted]	[redacted]	07/01/2016	05/08/2019	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 Compliance Audit conducted from [redacted], SERC determined that the Entity, as a [redacted], was in noncompliance with CIP-002-5.1 R1, P 1.2. The Entity failed to identify a workstation as a medium impact BES Cyber Asset (BCA). The Entity implemented a rule in the production firewall permitting a workstation, located outside of the Electronic Security Perimeter (ESP), to access [redacted] servers inside the ESP. The workstation is used as a training workstation for System Operators and is also an additional console because it can be used during a storm and other emergencies to perform production work. The Entity should have declared this workstation as a medium impact BCA because it used for production activities during emergencies. Upon discovery, the Entity confirmed that it improperly assigned the IP address of the workstation's host name, within the firewall ruleset, which allowed it to gain the improper access to the ESP. The Entity immediately corrected the firewall rule and host assignment by removing the improper access of the workstation into the ESP. The Entity conducted an extent-of-condition and found no additional occurrences of improper classification or access into the ESPs. This noncompliance started on July 1, 2016, when the standard became mandatory and enforceable and the Entity failed properly identify the workstation as [redacted] BCA, and ended on May 8, 2019, when the Entity corrected the firewall ruleset to remove the improper access of the workstation into the ESP while the Audit Team was still on-site. The cause of this noncompliance was a lack of internal control. The Entity did not have a checklist to properly identify the rules in the firewalls for the workstations in its CIP-002 categorization and on-boarding processes.
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 properly identify this Cyber Asset as a BCA could have allowed it to not have appropriate security controls applied as required by the CIP Standards. This could leave the BCA vulnerable to compromise or misuse and with its capability of monitoring and controlling the BES could impact the bulk power system. The Entity reduced the risk because workstation resides and is protected within the Physical Security Perimeter and within a dedicated [redacted] Furthermore, the Entity limited access specific to its Staff that had been approved for authorized electronic and authorized, unescorted physical access to BCS at the Control Center. No harm is known to have occurred. SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1. updated firewall rules to ensure the correct security posture at [redacted] and [redacted] ESPs; 2. trained Subject Matter Experts on revised CIP-002 Process; 3. updated the CIP-002 Process document, [redacted] to document the process review for updates prior to the implementation of any process changes resulting from: A. performed BES Cyber System Identification; and B. performed BES Cyber Asset identification; 4. improved the formatting of [redacted] to improve asset classification clarity; 5. reconciled the Cyber Asset unique identifier in Network Diagrams, Firewall Rulesets, and [redacted]"; 6. implemented an onboarding checklist for BES Cyber Systems and their associated BCAs, Protected Cyber Assets (PCAs), Electronic Access Control and/or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS); and 7. implemented an off-boarding checklist for BES Cyber Systems and their associated BCAs, PCSs, EACMS, and PACS.

FFT

SERC Reliability Corporation (SERC)

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
FRCC2019021602	CIP-005-5	R2, P2.1	[redacted]	[redacted]	07/01/2016	07/27/2019	Compliance Audit	06/30/2020

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	During a Compliance Audit conducted from [redacted], SERC determined that the Entity, as a [redacted], was in noncompliance with CIP-005-5 R2, P2.1. The Entity allowed Interactive Remote Access (IRA) to BES Cyber Systems (BCSs) that did not originate from within another Electronic Security Perimeter (ESP) or an identified Intermediate System, and the access did not go through an Intermediate System. This noncompliance involved [redacted] Cyber Assets [redacted] of the [redacted] Cyber Assets included [redacted] physical workstation and [redacted] virtual workstations located in a demilitarized zone (DMZ) associated with the [redacted] ESP, which allowed the use of the operator console functionality and the ability for IRA with the production [redacted] BCS. The physical workstation was used as a training workstation for [redacted] and was assigned a second legacy unused host name within the firewall, which allowed the user to access certain BES Cyber Assets (BCAs) in the [redacted] BCS without using an Intermediate System. The [redacted] virtual workstations were installed, as part of a pilot program, to allow IRA for field employees to map functionality [redacted]. During the installation of the virtual workstations, a firewall rule was misconfigured to permit communications between the virtual workstations and a server in the [redacted] ESP. The firewall rule should have been configured to a server in a DMZ associated with the [redacted] ESP. Because the firewall rule permitted access, the [redacted] virtual workstations had IRA to the [redacted] BCS without using an Intermediate System. The Entity discontinued the pilot program, but did not remove the rule. The [redacted] Cyber Asset was a host system identified as an Electronic Access Control or Monitoring System (EACMS) and located in a DMZ off the [redacted] ESP. The Entity had installed an anti-malware [redacted] and a software update service that were used to manage anti-malware and system updating of the production [redacted] BCS. There were firewall rules for the EACMS permitting it to push changes into the [redacted] and [redacted] ESPs. The Entity did not identify the EACMS as an Intermediate System and afford the security controls necessary for an Intermediate System. The Entity performed an extent-of-condition by using a technical analysis visual inspection of the firewall policy reports and by using a software tool to perform network path analysis to identify potential IRA permitted by the firewall rules. The Entity also performed its CIP-002 based categorization process and did not identify any other Cyber Assets that it should have designated as Intermediate Systems or any other Cyber Assets that had direct IRA. This noncompliance started on July 1, 2016, when the Entity allowed IRA to BCAs inside the ESP without going through an identified Intermediate System, and ended on July 27, 2019, when the Entity properly identified and protected the [redacted] Cyber Asset as an Intermediate System. The causes of this noncompliance were management oversight, specifically, lack of internal control and lack of training. For the physical workstation and virtual workstations Cyber Assets, management failed to verify the accuracy of the firewall configurations to ensure that that IRA to BCAs inside the ESP went through an Intermediate System. For the EACM [redacted] the quality of the Entity's training was inadequate. Specifically, staff within different business units (silos) responsible for security and CIP compliance did not share a common understanding of the purpose of the [redacted] therefore, the [redacted] was not identified as an Intermediate 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 (BPS). The Entity's failure to limit IRA to BCAs through an identified Intermediate System allowed direct access to those BCAs from an uncontrolled environment, which increased the risk of compromise or misuse that could have impacted the reliability of the BPS. The risk was reduced as the server used for anti-malware administration activities resides in a restricted DMZ subnet, meaning that all the workstations were being patched, monitored, and logged, and access to the Cyber Asset is limited to specific Entity support staff. The other [redacted] Cyber Asset workstations also reside within a restricted development/test DMZ subnet. Access to these [redacted] Cyber Assets is also limited to specific Entity approved staff for authorized electronic and authorized, unescorted physical access to BES Cyber Systems at the Control Center. No harm is known to have occurred. SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) updated firewall rule sets to eliminate user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol without the use of an Intermediate System; 2) performed an extent of condition and a root cause analysis; 3) categorized the anti-malware [redacted] and software update service server as an Intermediate System and added the security controls necessary to an Intermediate System; 4) reconciled the Cyber Asset unique identifier in Network Diagrams, Firewall Rule sets, and Cyber Security; 5) created a Change Review Committee (CRC), whose scope includes the review of change control ticket actions (including configuration change management) and supporting documentation, once every three weeks; 6) created a firewall rule set review committee, whose scope includes a quarterly manual review of the firewall rule sets; 7) implemented an onboarding checklist for BES Cyber System and their associated BCAs, Protected Cyber Assets (PCA), EACMS, and Physical Access Control (PACS); 8) trained Subject Matter Experts on CIP-002 Process;

SERC Reliability Corporation (SERC) | FFT | CIP

	9) implemented an off-boarding checklist for BES Cyber Systems and their associated BCAs, PCA, EACMS, and PACS. 10) purchased software tool to enhance rule analysis capability; 11) built supporting physical hardware associated with the software tool implementation; 12) implemented software tool solution to enhance firewall rule analysis capability for each ESP; and 13) will implement software tool solution to continuously monitor, assess and track changes to protected networks for security issues related to network access rules that will augment and compliment the associated manual controls.

Texas Reliability Entity, Inc. (Texas RE) | 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
TRE2017018208	CIP-007-6	R2; P2.2	[redacted] (the "Entity")	[redacted]	5/7/2017	9/26/2019	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 Compliance Audit conducted per an existing multi-region registered entity agreement from [redacted], Texas RE determined that the Entity, as a [redacted], was in noncompliance with CIP-007-6 R2. Specifically, the Entity did not timely implement its process to evaluate security patches for applicability for [redacted] Cyber Assets, comprising [redacted] BES Cyber Assets (BCAs) and [redacted] Protected Cyber Assets (PCAs), at a [redacted] associated with a Medium Impact BES Cyber System. Regarding the [redacted] BCAs at issue, certain software installed on the BCAs was in end-of-life status but was needed for Facility operations. The Entity prepared and implemented draft documentation noting that no patch source was available and detailing activities to mitigate the risk posed by this issue, including monitoring and training, but the documentation was not finalized until July 28, 2017, ending the noncompliance with respect to these devices. Regarding the [redacted] PCAs at issue, following the Compliance Audit, the Entity reevaluated patching availability for the Cyber Assets and determined that patches were available. By September 26, 2019, the Entity confirmed that applicable security patches for these Cyber Assets were installed. The root cause of this issue is that the Entity did not have a sufficient process for compliance with CIP-007-6 R2 for the [redacted] at issue. In particular, to address this issue, the Entity has revised its patching process to include a continuously reviewing the patching process for the [redacted]. This noncompliance started on May 7, 2017, which is the 36 days after CIP-007-6 R2 became applicable to the BES Cyber System at issue, and ended on September 26, 2019, when the Entity either resumed patching or documented that no patch source exists for the software at issue for the [redacted] impacted 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. The Entity's failure to evaluate and apply patches in a timely manner through September 26, 2019, could have exposed the Entity's BES Cyber Systems to cyber security vulnerabilities such as the introduction of malicious code. This issue affected [redacted] BES Cyber Assets and [redacted] Protected Cyber Assets which are associated with the Medium Impact BES Cyber System for a [redacted]. However, the risk posed by this issue was reduced by the following factors. First, the Entity deployed an intrusion prevention system, as well as an additional preventative control that blocks applications and user activity that have not been previously whitelisted. Second, this issue impacted a limited number of Cyber Assets. In particular, for all BCAs at issue, the noncompliance was limited to a documentation issue, as there was no patch source available for the software at issue. However, regarding the [redacted] PCAs at issue, security patches were determined to be available. Security patching was completed on September 26, 2019. 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 that no patch source exists for the software at issue for the [redacted] impacted BCAs; 2) implemented its patching program for the software at issue for the [redacted] impacted PCAs; and 3) revised its patching process to include recurring monthly meetings to continuously review compliance with CIP-007-6 R2 for the Facility at issue. 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
TRE2017018673	CIP-007-6	R3; P3.3	[redacted] (the "Entity")	[redacted]	7/1/2016	8/7/2018	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 from [redacted] Texas RE determined that the Entity, as a [redacted] was in noncompliance with CIP-007-6 R3. In particular, the Entity did not implement a documented process to test signatures and patterns for the Entity's deployed method to deter, detect, or prevent malicious code. The Entity configured 25 clients running its antivirus system to automatically download and install signature updates multiple times per day. As a result, signatures and patterns were not tested before they were applied. On August 7, 2018, the Entity approved and implemented a new process for testing signatures for its antivirus system. The root cause of this issue is that the Entity's process documents did not adequately address the requirement to test signatures and patterns, which led to the Entity failing to implement the required process. Specifically, during the noncompliance, the Entity's process documents stated in general terms that signatures and patterns should be tested, but these documents did not provide sufficiently detailed instructions to ensure that the Entity's personnel implemented a process for testing signatures and patterns. As a result, the Entity's personnel followed the software vendor's instructions to automatically immediately install signature updates. The noncompliance started on July 1, 2016, when CIP-007-6 R3 became enforceable, and ended on August 7, 2018, when the Entity implemented a process for testing signatures for its antivirus software.
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 posed by this issue is that an untested signature update could adversely impact the integrity or functionality of the Entity's Cyber Assets by failing to protect against malicious code or by causing the protected BES Cyber Systems not to function as intended. In addition, this issue affected [redacted] that are associated with [redacted] that are associated with a High Impact BES Cyber System. However, the risk posed by this issue is reduced by the following factors. First, the Entity's transmission network has a [redacted] The Entity's [redacted]. The Entity does [redacted] Second, the Entity implemented other methods to deter, detect, and prevent malicious code, and the Entity had a documented process for testing and installing signatures for these other methods. No harm is known to have occurred. Texas RE determined the Entity's and its affiliates' compliance history should not serve as a basis for aggravating the risk posed by this issue. The Entity's and its affiliates' relevant compliance history involves three prior instances, under Violation IDs [redacted]. Regarding Violation ID [redacted], the Entity and its affiliates discovered and mitigated the prior instance when it was reviewing its compliance processes in addressing the instant instance of noncompliance. Regarding Violation IDs [redacted], the prior instances involved different factual circumstances and root causes from the instant instance of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) implemented a revised documented process that includes a process for testing signature updates for the antivirus system; and 2) created an annual training requirement regarding the new process and conducted training for the Entity's personnel. Texas RE 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
WECC2017017464	CIP-004-6	R2: P2.2	[redacted]	[redacted]	7/1/2016	11/28/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On April 25, 2017, the entity submitted a Self-Report stating that, as a [redacted] it was in potential noncompliance with CIP-004-6 R2. Specifically, the entity did not ensure that only authorized individuals with CIP training had electronic and unescorted physical access to a PACS server. Specifically, the entity issued [redacted] badges for access to a Physical Security Perimeter (PSP) [redacted]. Only [redacted] of the [redacted] employees with badges had CIP training. At least [redacted] of the [redacted] issued badges were "shared", reserved for emergency and service purposes. Most of the shared badges were stored in a locked cabinet or other secure location and were managed through multiple control activities. Additionally, the entity was a [redacted] As such, most of the [redacted] employees of the [redacted] were set up with the role of domain user and had the ability to login to the entity's PACS server; none of which had CIP training. Lastly, [redacted] employees with System Administrator privileges on the PACS server, which allowed users the ability to [redacted] Medium Impact BES Cyber System in the event of an emergency, did not have CIP training. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on November 28, 2017, when the entity limited electronic access and unescorted physical access to the PACS server to only [redacted] authorized personnel with CIP training. The root cause of the issue was attributed to a fundamental misunderstanding of the functionality of the affected PACS. Specifically, the entity identified the server as a PACS and made several attempts to apply protective measures such as adding firewall rules to remove [redacted] client access. The entity also changed the [redacted] user rights to [redacted] rights for authorized personnel. However, the entity did not recognize that these protective measures did not fully isolate the PACS server as intended [redacted]
Risk Assessment	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to require completion of CIP training prior to granting authorized electronic access and authorized unescorted physical access to a PACS server associated with its MIBCS as required by CIP-004-6 R2 Part 2.2. Such failure could have resulted in unauthorized personnel tampering with the PSP permissions to the entity's MIBCS with the intent to gain access to those systems and negatively impact the entity's [redacted]. However, as compensation, the physical access points to the affected PACS required biometric authentication that was beyond what was required for compliance with the Requirement, [redacted] No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity limited electronic access to four authorized personnel with CIP training when it built a server with restricted user accounts, active directory, local system accounts and the structured query language database account. To fully address the root cause of the noncompliance herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling system which automatically

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC) FFT CIP

	creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed. Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future noncompliance. 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
WECC2017017465	CIP-004-6	R3: P3.5	[redacted]	[redacted]	7/1/2016	11/28/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On April 25, 2017, the entity submitted a Self-Report stating that, as a [redacted] it was in potential noncompliance with CIP-004-6 R3. Specifically, the entity did not ensure that only authorized individuals with a personnel risk assessments (PRAs) had electronic and unescorted physical access to the PACS server. The entity issued [redacted] badges to a Physical Security Perimeter (PSP) [redacted] Only [redacted] of [redacted] employees with badges had a PRA. At least [redacted] of the [redacted] issued badges were "shared" badges reserved for emergency and service purposes. Most of the shared badges were stored in a locked cabinet or other secure location and were managed through multiple control activities. Additionally, the entity was a [redacted] As such, most of the [redacted] employees of the [redacted] were set up with the role of domain user and had the ability to login to the entity's PACS server; none of which had a PRA. Lastly, [redacted] employees with System Administrator privileges on the PACS server, which allowed users [redacted] Medium Impact BES Cyber System in the event of an emergency, did not have a PRA. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on November 28, 2017, when the entity ensured all employees with access to the affected PACS had a PRA. The root cause of the issue was attributed to a fundamental misunderstanding of the functionality of the affected PACS. Specifically, the entity identified the server as a PACS and made several attempts to apply protective measures such as adding firewall rules to remove [redacted] client access. It also changed the [redacted] user rights to [redacted] rights for unauthorized personnel. However, the entity did not recognize that these protective measures did not fully isolate the PACS server as intended which left it open and available for unauthorized user to control all the other PACS.
Risk Assessment	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to require completion of a PRA prior to granting authorized electronic access and authorized unescorted physical access to a PACS server associated with its MIBCS as required by CIP-004-6 R3 Part 3.5. Such failure could have resulted in unauthorized personnel tampering with PSP permissions to the entity's MIBCS with the intent to gain access to those systems and negatively impact the entity's transmission system, generation Facilities or load delivery. However, as compensation, the physical access points to the affected PACS required biometric authentication that was beyond what was required for compliance with the Requirement, [redacted] The server was manned 24/7 and was securely locked during non-business hours. [redacted] No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this issue, the entity has limited electronic access to [redacted] personnel with a PRA when it built a server with restricted user accounts, active directory, local system accounts and the structured query language database account. To fully address the root cause of the noncompliance herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC)	FFT	CIP
	and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling system which automatically creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed. Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future noncompliance. 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
WECC2017017511	CIP-006-6	R1: P1.1; P1.6; P1.7; P1.10	[redacted]	[redacted]	7/1/2016	2/23/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On April 28, 2017, the entity submitted a Self-Report stating that, as a as a [redacted] it was in potential noncompliance with CIP-006-6 R1. Specifically, the entity did not restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same ESP to those places where such cabling and components were located outside of a PSP. The cable subject to this instance [redacted] with [redacted] BES Cyber Assets (BCAs) associated with a MIBCS, and [redacted] EACMS located inside the same ESP. [redacted] The Part 1.10 issue began on April 1, 2017, when the Standard and Requirement became mandatory and enforceable and ended on June 30, 2017, when the entity implemented [redacted]. Additionally, [redacted] PACS workstations located outside of a PSP were not afforded the required protections of CIP-006-6 R1 Parts 1.6 and 1.7; and the entity did not define the operational or procedural controls to restrict physical access to these PACS as required by Part 1.1. The Part 1.1, 1.6, and 1.7 issues began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on February 23, 2018, when the entity completed Part 1.7, the last of the three Parts left to be completed, by issuing alarms or alerts in response to detected unauthorized physical access to the PACS to the personnel identified in the BES Cyber Security Incident response plan for the affected PACS. The root cause of the issue was attributed to a fundamental misunderstanding of the Standard and Requirement to protect cabling, for restricting physical access, monitoring, and responding to unauthorized physical access attempts to PACS workstations located outside of a PSP.
Risk Assessment	These issues posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In these instances, the entity failed, for CIP-006-6 R1 to define operational or procedural controls to restrict physical access (Part 1.1), monitor each PACS for unauthorized physical access to a PACS (Part 1.6), and issue an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection (Part 1.7), for [redacted] PACS associated with the entity's MIBCS. Additionally, the entity failed to restrict physical access to cabling used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter (Part 1.10). Failure to restrict access to physical cabling components could have resulted in cables being tampered with to allow access to communications, resulting in possible modifications of information. Additionally, not affording the affected PACS with the protective measures of CIP-006-6 R1 could have resulted in an attacker gaining access to critical systems without the entity's knowledge, prolonging the time the attacker could use for nefarious purposes, and possibly allow them to escape undetected. An attacker could also monitor, manipulate, or disable Cyber Assets without entity knowledge. However, as compensation, the area containing the cables required badge access for entry and the cabling was in an elevated rack and was not easily accessible. Additionally, access to some of the affected PACS required passing by a receptionist desk to sign in; other affected PACS were in an engineering building that required key access after-hours and was manned at the entry during business hours. Lastly, the affected PACS workstation screens automatically locked if unattended for [redacted] of load. No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this issue, the entity has: a) implemented armored fiber to restrict physical access to the cabling; and

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC)	FFT	CIP
	b) implemented operational and procedural controls to restrict physical access to the affected PACS, to including methods to monitor, alarm, and alert for unauthorized physical access. To fully address the root cause of the noncompliance herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling system which automatically creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed. Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future noncompliance. 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
WECC2017018579	CIP-006-6	R3: P3.1	[redacted]	[redacted]	7/1/2017	10/5/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On November 1, 2017, the entity submitted a Self-Report stating that, as a [redacted] it was in potential noncompliance with CIP-006-6 R3. Specifically, the entity did not perform the maintenance and testing for [redacted] PACS panels and [redacted] access readers which control physical access at the PSP to the MIBCS [redacted] as required by the implementation date of July 1, 2017, stated in the NERC Implementation Plan for Version 5 CIP Cyber Security Standards. This issue ended October 5, 2017 when the entity performed all maintenance and testing on the affected PACS and [redacted] access readers. The root cause of the issue was attributed an insufficient number of trained or experienced workers assigned to the task. Specifically, staff responsible for performing the maintenance and testing were not aware of the CIP Version 5 implementation plan which stated the initial performance of this tasked needed to be performed by July 1, 2016. They assumed they had 24 calendar months after the implementation date of July 1, 2016, as stated in Part 3.1 of CIP-006-6 R3.
Risk Assessment	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to implement a documented PACS maintenance and testing program that included the maintenance and testing of each PACS and locally mounted hardware or devices at the PSP for [redacted] PACS panels and [redacted] access readers as required by CIP-006-6 R3 Part 3.1. Such failure could have resulted in the misoperation of the PACS panels or the locally mounted hardware which could have prevented authorized personnel physical access or allow unauthorized personnel access to the [redacted] of the entity. However, as compensation the entity had only [redacted] facilities with PACS and locally mounted hardware that required maintenance and testing. These [redacted] facilities were regularly used, and the PACS and locally mounted hardware was required to function for physical access to each facility. Effectively, the PACS was tested through frequent and regular usage. Additionally, the entity had no previous PACS or locally mounted hardware failures at the [redacted] facilities. [redacted] No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this issue, the entity has: a) performed all maintenance and testing on the affected PACS panels and locally mounted hardware; b) hired consultants to serve as staff augmentation and provide CIP support, aid in the maturation of the compliance program, and identify areas were additional controls need implemented; and c) implemented a workflow system which automates the task of tracking and notifying employees of approaching compliance deadlines. To fully address the root cause of the noncompliance herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling system which automatically creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed. Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future noncompliance. 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
WECC2017017466	CIP-007-6	R1: P1.1	[redacted]	[redacted]	7/1/2016	6/28/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On April 25, 2017, the entity submitted a Self-Report stating that, as a as a [redacted] it was in potential noncompliance with CIP-007-6 R1 Part 1.1. Specifically, the entity did not have a formal documented process for enabling logical network accessible ports that had been determined to be needed, for [redacted] PACS associated with its MIBCS located at the [redacted]. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended June 28, 2018, when the entity completed mitigating activities described herein. The root cause of the issue was attributed a lack of written communication. Specifically, the entity did not have formal documentation for approval of the needed logical network accessible ports or the business justification for each open and listening port, which led to confusion of roles and responsibilities in the performance of the compliance obligation.
Risk Assessment	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to implement a documented process for enabling only logical network accessible ports that have been determined to be needed, including port ranges or services where needed to handle dynamic ports on [redacted] PACS as required by CIP-007-6 R1 Part 1.1. Such failure could have resulted in unauthorized or vulnerable applications running on the PACS that could install software, exfiltrate data or perform remote control of the affected systems and an anchor point for reconnaissance and spreading through the environment, which could have a negative effect on the BES. However, as compensation the entity had local firewall rules for both inbound and outbound traffic enabled on the PACS server which was also isolated [redacted] The remaining PACS were behind a firewall and the entity had implemented biometric fingerprint authentication that utilized a separate system to access the entity's PSP controlling access to the MIBCS. [redacted] No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this issue the entity has: a) documented its business justifications for approved ports on the server; b) removed the client software from the PACS workstations thus removing the ability to access the client system entirely; c) documented all PACS servers and workstations are part of the [redacted] environment to manage all [redacted] products and associated updates; d) added to its [redacted] sub-processes for compliance with CIP-007-6 relating to the affected Cyber Assets that included: i. documentation and justification for ports; ii. security patch management; iii. malicious code detection, which automated the updating of signatures or patterns; iv. security event alerting and log retention; v. system access control, which included changing the password length to eight or more characters on the affected EACMS, and where technically feasible enforced account authentication thresholds through Group Policy; and vi. roles and responsibilities; e) distributed the updated documentation to applicable personnel. To fully address the root cause of the noncompliance herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling system which automatically creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed.

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC)	FFT	CIP
	Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future noncompliance. 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
WECC2017017467	CIP-007-6	R2: P2.1; P2.2; P2.3; P2.4	[redacted]	[redacted]	7/1/2016	9/26/2018	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.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On April 26, 2017, the entity submitted a Self-Report stating that, as a as a [redacted] it was in potential noncompliance with CIP-007-6 R2 Parts 2.1 through 2.4. Specifically, for [redacted] PACS associated with its MIBCS located at the [redacted], the entity did not document a security patch management process. The entity had contracted with a third-party to act as a patching source for software associated with the affected PACS; however, no documentation for tracking, evaluation, and installing cyber security patches was created, as required by Parts 2.1 through 2.4. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on September 26, 2018, when the entity documented its security patch management process for the affected PACS. The root cause of this issue was attributed to a fundamental misunderstanding of the functionality of the affected PACS which led to undefined roles and responsibilities for performing compliance obligations. Regarding [redacted] BCAs and [redacted] EACMS associated with its MIBCS located at the [redacted], the entity identified that its automated tool did not always download updated patch information from external sources as timely as expected for evaluation as required by Part 2.2. This issue began on September 4, 2016, the day after the evaluation of released security patches since the last evaluation should have occurred and ended on September 30, 2018 when the entity performed patch evaluations on the affected Cyber Assets. The root cause of this issue was attributed to multiple interconnected manuals and automated controls including design and technical flaws.
Risk Assessment	These issues posed a moderate risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In these instances, the entity failed to implement a documented process that collectively included a patch management process for tracking, evaluating, and installing cyber security patches, including the identification of a source or sources for the release of cyber security patches (Part 2.1), for evaluating at least once every 35 calendar days the applicability of security patches (Part 2.2), for applicable security patches either apply the security patch, create a dated mitigation plan, or revise an existing plan (Part 2.3), and for implementing created mitigation plans within the specified timeframe (Part 2.4) for the affected [redacted] PACS, [redacted] BCAs and [redacted] EACMS associated with its MIBCS. Such failures could have resulted in unauthorized access to the MIBCS due to unpatched vulnerable applications running on the affected Cyber Assets, malware infection or other successful intrusion into the unpatched systems potentially resulting in the exfiltration of data or remote control of the affected systems and an anchor point for reconnaissance and spreading through the environment, which could have a negative effect on the BES. However, the noncompliance with the affected PACS was limited to a documentation issue. For the affected BCAs and EACMS the entity implemented host-based control and perimeter based malicious code monitoring, thereby limiting the risk. [redacted]. No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this issue the entity has: a) removed the client software from the PACS workstations thus removing the ability to access the client system entirely; b) implemented a documented patch management process for the Cyber Assets in scope; c) documented all PACS servers and workstations are part of the [redacted] environment to manage all [redacted] products and associated updates; d) added to its [redacted] sub-processes for compliance with CIP-007-6 relating to the affected Cyber Assets that included:

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC)	FFT	CIP
	i. documentation and justification for ports; ii. security patch management; iii. malicious code detection, which automated the updating of signatures or patterns; iv. security event alerting and log retention; v. system access control, which included changing the password length to eight or more characters on the affected EACMS, and where technically feasible enforced account authentication thresholds through Group Policy; and vi. roles and responsibilities; e) distributed the updated documentation to applicable personnel. To fully address the root cause of the noncompliance herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling system which automatically creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed. Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future noncompliance. 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
WECC2017017468	CIP-007-6	R3: P3.2; P3.3	[redacted]	[redacted]	7/1/2016	1/8/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On April 26, 2017, the entity submitted a Self-Report stating that, as a as a [redacted] it was in potential noncompliance with CIP-007-6 R3. Specifically, the entity did not document a malicious code prevention process that collectively included [redacted] PACS associated with its MIBCS located at the [redacted]. While endpoint protection software was monitored and leveraged to mitigate the threat of detected malicious code, a formal process had not been documented for mitigating the threat of detected malicious code as required by Part 3.2 and a formal process had not been created for testing signature updates to antivirus software as required by Part 3.3. This issue began on July 1, 2016, when the Standards and Requirement became mandatory and enforceable and ended on January 8, 2018, when the entity implemented a process for mitigating the threat of detected malicious code and controls for signature testing. The root cause of the issue was attributed to a fundamental misunderstanding of the functionality of the affected PACS which led to undefined roles and responsibilities for performing compliance obligations.
Risk Assessment	These issues posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In these instances, the entity failed to implement a documented process to mitigate the threat of detected malicious code as required by Part 3.2 or have a process for the update of signatures or patterns, to include addressing the testing and installing signatures or patterns for [redacted] PACS as required by Part 3.3. Such failures could have resulted in a PACS not having a method to mitigate detected malicious code. Lack of documentation defining the process for mitigation of malicious code could have resulted in the lack of or inappropriate response to detected malicious code resulting in the spread of malicious code throughout the entity's systems. In addition, the lack of documented signature update processes could have resulted in the failure of updates being applied, thus leaving the PACS vulnerable to malicious code attacks, potentially leading to physical access control failures or unauthorized access. However, the entity implemented biometric (fingerprint) authentication utilizing a separate system to physically access its MIBCS. Additionally, the entity implemented host-based controls on all EACMS and had implemented perimeter based malicious code monitoring for all BCAs. The entity configured thresholds for login failures for the BCAs and EACMS such that either an alert or account lockout occurred after a specific number of failed login attempts. [redacted] No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this issue the entity has: a) removed the client software from the PACS workstations thus removing the ability to access the client system entirely; b) updated its documented processes to include the affected PACS into its malicious code detection system which also automated the updating of signatures or patterns; c) documented all PACS servers and workstations are part of the [redacted]) environment to manage all [redacted] products and associated updates; and d) utilized [redacted] to detect for malicious code on managed systems.

	To fully address the root cause of the noncompliance herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling system which automatically creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed. Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future noncompliance. 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
WECC2017017469	CIP-007-6	R4: P4.2; P4.3	[redacted]	[redacted]	7/1/2016	1/11/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On April 26, 2017, the entity submitted a Self-Report stating that, as a as a [redacted] it was in potential noncompliance with CIP-007-6 R4. Specifically, the entity did not document a process for generating alerts for required security events (detected malicious code and detected failure of event logging) for [redacted] PACS associated with its MIBCS located at the [redacted] as required by Part 4.2. While formal documentation outlining alerting for detection of logging failure and malicious doe did not exist, required logs were maintained, and alerting for detected malicious code was performed. Event logs were maintained and available for testing and after-the-fact investigation of suspicious activity. Additionally, [redacted] BCAs and [redacted] EACMS were not configured to send logs to the entity's aggregation system; therefore, not retaining applicable event logs as required by Part 4.3. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity and ended on January 11, 2018, when the entity configured alerts for security events and enabled 90-day log retention on the affected Cyber Assets. The root cause of the issue was attributed to a fundamental misunderstanding of the functionality of the affected PACS which led to undefined roles and responsibilities for performing compliance obligations. The root cause of the issues related to the BCAs and EACMS was attributed to multiple interconnected manuals and automated controls including design and technical flaws.
Risk Assessment	These issues posed a moderate risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In these instances, the entity failed to generate alerts for security events and retain applicable event logs on [redacted] PACS, [redacted] BCAs, and [redacted] EACMS associated with its MIBCS located at the [redacted] as required by CIP-007-6 R4 Parts 4.2 and 4.3. Such failures could have resulted in an unawareness of malicious code activity or other security events related to the affected Cyber Assets and the inability to successfully investigate any potential malicious activity that may have taken place; thereby limited the entity's ability to determine the cause or source of malicious activity. Security events could quickly spread across systems and dramatically affect the operational performance of those systems. Additionally, unauthorized control of Cyber Assets could directly result in loss, degradation or misuse of the systems used to perform the required operational functions of the entity. However, the noncompliance with the affected PACS was a deficiency in documentation. As compensation, the entity implemented biometric (fingerprint) authentication utilizing a separate system to physically access its MIBCS. Additionally, the entity implemented host-based controls on all EACMS and had implemented perimeter based malicious code monitoring for all BCAs. The entity configured thresholds for login failures for the BCAs and EACMS such that either an alert or account lockout occurred after a specific number of failed login attempts. [redacted]. No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this issue the entity has: a) removed the client software from the PACS workstations thus removing the ability to access the client system entirely; b) documented its process for generating alerts for required security events and log retention for the Cyber Assets in scope. c) documented all PACS servers and workstations are part of the [redacted] environment to manage all [redacted] products and associated updates; d) added to its [redacted] sub-processes for compliance with CIP-007-6 relating to the affected Cyber Assets that included: i. documentation and justification for ports; ii. security patch management; iii. malicious code detection, which automated the updating of signatures or patterns; iv. security event alerting and log retention; v. system access control, which included changing the password length to eight or more characters on the affected EACMS, and where technically feasible enforced account authentication thresholds through Group Policy; and vi. roles and responsibilities; and e) distributed the updated documentation to applicable personnel.

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC)	FFT	CIP
	To fully address the root cause of the noncompliance herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling system which automatically creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed. Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future noncompliance. 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
WECC2017017470	CIP-007-6	R5: P5.2; P5.3; P5.4; P5.5 Subpart 5.5.1 and 5.5.2; P5.7	[redacted]	[redacted]	7/1/2016	5/23/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On April 26, 2017, the entity submitted a Self-Report stating that, as a as a [redacted] it was in potential noncompliance with CIP-007-6 R5. Specifically, the entity did not have a documented process that collectively include all the applicable parts in CIP-007-6 R5 for [redacted] PACS associated with its MIBCS located at the [redacted]. A listing of all accounts was producible and maintained in its systems of record; however, a listing had not been created that identified the default or generic accounts, and no formal documented process was in place that included Part 5.2. A listing of individuals with access to shared accounts did not exist and no formal documented process was in place that included Part 5.3. A formal documented process was not in place that included Part 5.4. Although sufficient length and complexity were enforced through a group policy in Windows Active Directory for a PACS server, one application for the affected PACS was not configured to enforce password length and complexity and no formal documented process was in place that included Part 5.5. Unsuccessful login attempts that were authenticated via Windows Active Directory were limited for all users via Group Policy, one application on the affect PACS was not configured to limit or alert for several unsuccessful login attempts, and no documented process was in place that included Part 5.7. Additionally, for [redacted] EACM associated with a MIBCS at the [redacted], the entity did not enforce the required password length and complexity requirements for password-only authentication for interactive user access as required by Part 5.5. Lastly, for [redacted] additional EACMS associated with MIBCS at both the [redacted], the entity did not limit the number of unsuccessful authentication attempts and therefore did not generate an alert after a threshold of unsuccessful authentication attempts was reached as required by Part 5.7. These issues began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on May 23, 2018 when the entity limited the number of unsuccessful authentication attempts on the affected Cyber Assets. The root cause of the PACS issue was attributed to a fundamental misunderstanding of the functionality of the affected PACS which led to undefined roles and responsibilities for performing compliance obligations. The root cause of the EACMS was attributed to an administrative oversight.
Risk Assessment	These issues posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In these instances, the entity failed to identify and inventory all known enabled default or other generic account types, identify individuals who have authorized access to shared accounts, and change known default passwords, per Cyber Asset capability, for [redacted] PACS as required by CIP-007-6 R5 Parts 5.2, 5.3, 5.4, and 5.7. Additionally, the entity also failed to either technically or procedurally enforce password length and complexity for password-only authentication for interactive user access for [redacted] EACMS as required by CIP-007-6 R5 Part 5.5, and failed to limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts for [redacted] EACMS when it configured lockouts based on time rather than limiting the number of unsuccessful authentication attempts as required by CIP-007-5 R5 Part 5.7. Failing to document processes for the affected PACS could have resulted in missing or inadequate controls, as well as controls that were not managed appropriately, thus rendering the affect PACS vulnerable to attack by a malicious actor. Additionally, weak passwords could have provided access to the affected EACMS by a malicious actor with the intent to craft targeted attacks within the entity's Energy Management System. Lastly, not providing lockouts or alerts upon unsuccessful login attempts could provide a malicious actor to the ability to continue to brute force passwords without being deterred or delayed. However, while formal documentation did not exist for the affected PACS as described herein, physical and electronic protective measures were in place to mitigate the threat of malicious activity; users seeking to perform administrative functions on the server [redacted] dditionally, the entity implemented host based controls on all EACMS, and had implemented perimeter based malicious code monitoring for all BCAs. The entity configured thresholds for login failures for the BCAs and EACMS such that either an alert or account lockout occurred after a specific number of failed login attempts. T[redacted] No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.

WESTERN ELECTRICITY COORDINATING COUNCIL (WECC)	FFT	CIP
Mitigation	To mitigate this issue the entity has: a) removed the client software from the PACS workstations thus removing the ability to access the client system entirely; b) documented all PACS servers and workstations are part of the [redacted] environment to manage all [redacted] products and associated updates; c) documented its processes for system access control that included all applicable requirement parts for CIP-007-6 R5 for the affected PACS; d) changed the password length to eight or more characters on the [redacted] EACMS; e) enforced account authentication thresholds through Group Policy, where technically feasible; and f) added to its [redacted] sub-processes for compliance with CIP-007-6 relating to the affected Cyber Assets that included: i. documentation and justification for ports; ii. security patch management; iii. malicious code detection, which automated the updating of signatures or patterns; iv. security event alerting and log retention; v. system access control, which included changing the password length to eight or more characters on the affected EACMS, and where technically feasible enforced account authentication thresholds through Group Policy; vi. roles and responsibilities; and g) distributed the updated documentation to applicable personnel. To fully address the root cause of the noncompliance herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling system which automatically creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed. Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future 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
WECC2017017471	CIP-009-6	R1: P1.1; P1.2; P1.3; P1.4; P1.5	[redacted]	[redacted]	7/1/2016	6/7/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On April 26, 2017, the entity submitted a Self-Report stating that, as a as a [redacted] it was in potential noncompliance with CIP-009-6 R1. Specifically, the entity had no formal documentation outlining the activities associated with the backup and recovery process for [redacted] PACS. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on June 7, 2018 when the entity updated its recovery plan to include the affected PACS. The root cause of this issue was attributed to a fundamental misunderstanding of the functionality of the affected PACS which led to undefined roles and responsibilities for performing compliance obligations.
Risk Assessment	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance the entity failed to have a documented recovery plan for [redacted] PACS associated with its MIBCS as required by CIP-009-6 R1 Parts 1.1 through 1.5. Such failure could have resulted in a longer recovery time if the PACS were compromised or disabled. A compromised PACS could result in unauthorized access to sensitive equipment or authorized individuals not being able to access the affected PACS. However, the entity had implemented a high-level backup and recovery process for the affected PACS server, but that process did not include all the affected PACS. Although the affected PACS were configured to be backed up, there was no documented process for doing so. [redacted] No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this issue, the entity documented a process for recovery plan specifications for the affected PACS. To fully address the root cause of the issues herein, (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling system which automatically creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed. Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future noncompliance. 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
WECC2017017472	CIP-010-2	R1: P1.1; P1.2; P1.3; P1.4 Subparts 1.4.1; 1.4.2; 1.4.3	[redacted]	[redacted]	7/1/2016	6/7/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On April 26, 2017, the entity submitted a Self-Report stating that, as a as a [redacted] it was in potential noncompliance with CIP-010-2 R1. Specifically, the entity had no formal documentation outlining the activities associated with CIP-010-2 R1 for [redacted] PACS server because the entity believed the server had all the necessary protective measures applied to it, of which CIP-010-2 R1 was not one of them. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on June 7, 2018, when the entity documented and implemented baseline configuration on the affected PACS. The root cause of the PACS issue was attributed to a fundamental misunderstanding of the functionality of the affected PACS server. Specifically, the entity identified the server as a PACS during its implementation of CIP Version 5 and made several attempts to apply protective measures such as adding firewall rules to remove client access at its headquarters. It also changed the [redacted]. However, the entity did not recognize that these protective measures did not fully isolate the server from the entity's regional PACS as intended. Due to a fundamental misunderstanding of how the PACS worked, the database connections between the servers at the entity's headquarters and its regions were still functioning, bringing additional PACS into scope for compliance.
Risk Assessment	These issues posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In these instances, the entity failed to implement one or more documented process that collectively included each of the applicable Requirement Parts for [redacted] PACS server associated with the MIBCS located at both the [redacted], that is to document baseline configurations as required by Part 1.1, authorizing and documenting changes to the baseline configuration as required by Part 1.2, updating the baseline configuration within 30 calendar days for changes that deviated from the existing baseline configurations as required by Part 1.3, and a process to verify the effect of a change to the baseline configuration on exiting CIP-005 and CIP-007 controls as required by Part 1.4. Such failures could have resulted in the PACS server being changed without the knowledge of the entity. The entity would be unable to detect unauthorized changes, such as the introduction of malicious code, which could potentially allow a bad actor to gain physical access to the MIBCS located at the primary and backup Control Centers to cause disruption to system operations of the entity's [redacted]. However, although the PACS server did not have a documented baseline configuration per CIP-010-2 Part 1.1, it had a system of record that recorded configuration changes including installed software, logical network accessible ports, and applied security patches which allowed the entity to identify changes to the PACS server. Additionally, to compromise the server, one would need [redacted]. No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this issue, the entity has: a) updated baseline configurations for the affected PACS; b) implemented its CIP-010-2 configuration change management to the affected PACS; and c) updated its change control and configuration management to account for new processes needed as a result of upgrading the PACS system; To fully address the root cause of the issues herein, (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling

	system which automatically creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed. WECC has verified the completion of all mitigation activity. Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future 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
WECC2017017891	CIP-010-2	R3: P3.1	[redacted]	[redacted]	7/1/2017	1/11/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible or confirmed violation.)	The entity did not provide all the protective measures of CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-010-2 to the affected Cyber Assets, as applicable and described herein (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891). On July 7, 2017, the entity submitted a Self-Report stating that, as a as a [redacted] it was in potential noncompliance with CIP-010-2 R3. Specifically, the entity did not conduct a paper or active vulnerability assessment on [redacted] PACS associated with the MIBCS located at both the [redacted]. This issue began on July 1, 2017, when the Standard and Requirement became mandatory and enforceable and ended on January 11, 2018, when vulnerability scans were performed on the affected Cyber Assets. The root cause of this issue was attributed to several factors. Specifically, a general lack of understanding of the Standards and Requirements, ongoing mitigation activities for many Self-Reports and preparation for an upcoming audit saturated the available resources required to complete compliance obligations.
Risk Assessment	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, the entity failed to conduct a paper or active vulnerability assessment at least once every 15 calendar months as required by CIP-010-2 R3 Part 3.1 on [redacted] PACS associated with its MIBCS. Such failure could have resulted in the affected Cyber Assets running vulnerable applications or services without the entity's knowledge which could potentially compromise those Cyber Assets and the applicable systems they were associated with by allowing the uploading of malicious code, changing system configurations, or adding or changing physical access counts. As compensation, the entity had implemented due date reminders; however, there were no escalations in place to ensure compliance. [redacted]. No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this issue, the entity has: a) performed cyber vulnerability assessments (CVA) on the affected PACS; b) implemented its CIP-010-2 configuration change management to the affected PACS; c) adopted a single CVA methodology company-wide to ensure CVA requirements and applicability are uniformly understood and account for; d) updated its change control and configuration management to account for new processes needed because of upgrading the PACS system; and e) updated its processes to include the requirement to perform a CVA at least every 15 calendar months on applicable Cyber Assets. To fully address the root cause of the issues herein, (NERC Violation IDs: WECC2017017464, WECC2017017465, WECC2017017511, WECC2017018579, WECC2017017466, WECC2017017467, WECC2017017468, WECC2017017469, WECC2017017470, WECC2017017471, WECC2017017472, and WECC2017017891), the entity has implemented a combination of technical controls via new tools and solutions as well as procedural changes. Together these changes provide internal controls that will be preventative and detective in nature. The entity has moved to a single source patch notification service to streamline administration and provide transparency. Additionally, the entity developed a responsibilities matrix for all Standards pertaining to the PACS to support regulatory and operations obligations, with dedicated resources to manage and ensure compliance. Lastly, the entity implemented a task management, workflow, and scheduling system which automatically creates tasks based on deadlines. When creating a task in the system, an initial due date is required. This tool will also escalate the task and initiates email alerts to subject matter experts and their manager until the task is completed. Additionally, in May 2018, the entity decommissioned a majority of the affected PACS to reduce its risk of future noncompliance. WECC has verified the completion of all mitigation activity.

COVER PAGE

This filing contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Find, Fix, Track, and Reports 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	SPP2018019309	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
2	RFC2019021402	Yes	Yes	Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
3	SERC2017017807			Yes	Yes				Yes	Yes	Yes	Yes		Category 2 – 12: 2 year
4	SERC2018019508			Yes	Yes	A-				Yes				Category 2 – 12: 2 year
5	SERC2017016833			Yes	Yes				Yes	Yes			Yes	Category 2 – 12: 2 year
6	SERC2017018663			Yes	Yes				Yes	Yes			Yes	Category 2 – 12: 2 year

Filing Date: April 30, 2020

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
SPP2018019309	CIP-007-6	R4	[redacted] (the Entity)	[redacted]	11/1/2016	02/21/2018	Self-Certification	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On February 28, 2018, the Entity submitted a Self-Certification stating that as a [redacted], it was in noncompliance with CIP-007-6 R4. [redacted] The Entity reported that after performing CIP-007-6 R4 internal review on February 14, 2018, that it could not produce sufficient evidence to prove that it was in compliance with CIP-007-6 R4. Specifically, the Entity was failing to collect, process, and retain logged events, which relates to parts 4.1, 4.2, 4.3, and 4.4 of CIP-007-6 R4. Specifically, the Entity's Security Information and Event Management (SIEM) tool had experienced a hardware failure. Per the Entity, there were insufficient employees assigned to monitor and maintain the SIEM, and the Entity did not address the hardware failure, which resulted in logging information not being collected or reviewed. The cause of the noncompliance was that the Entity failed to follow its documented procedures related to log collection, alert generation, retention, and logged event review. The noncompliance began on November 1, 2016, which was the day after the last day of stored event logs, and it ended on February 21, 2018, when the Entity replaced the defective SIEM hardware.
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 was moderate and not minimal because the Entity's control system was not compliant with CIP-007-6 R4 for an extended period of 478 days. The noncompliance was not severe because the affected BES Cyber Systems are Medium Impact and because the Entity's malware protection software continued to function continued to provide visibility of possible malicious activity; however, log collection, alert generation, log retention, and log reviews were not being performed for 478 days. Additionally, the Entity's awareness of the security state of its BES Cyber Systems was reduced, as would have been its ability to conduct forensic investigations had a successful attack occurred. No harm is known to have occurred. The Entity does not have any relevant compliance history.
Mitigation	To mitigate this noncompliance, the Entity: 1) repaired or replaced the defective SIEM hardware and returned it to service; 2) upgraded its SIEM software to current version; 3) configured BCAs to log to the SIEM; 4) removed [redacted] from service to correct a hardware failure; 5) reviewed its threat protection software for indications of suspicious or malicious activity that may have occurred during the SIEM hardware failure; 6) updated its threat detection software and incorporated it into its monitoring application; 7) assigned an additional resource for administration and training; 8) re-trained responsible primary and backup SME on documented policies and procedures; and 9) implemented internal procedures to start monthly for six months and then quarterly thereafter.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021402	CIP-005-5	R1	[redacted]	[redacted]	7/3/2018	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 April 22, 2019, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-005-5 R1. [redacted] On October 16, 2018, while implementing a change request, the entity discovered that an access control list (ACL) at a medium impact substation was not correctly configured on one of the router's embedded switch modules. [redacted] The embedded switch module misconfiguration allowed communications to occur without correct inbound and outbound access permissions. The entity determined that the embedded switch module was missing an ACL when the entity replaced it with a new module on July 3, 2018 to repair communications for a break fix event. When the entity replaced the embedded switch module, the entity used a configuration tool to develop and output the ACL to be uploaded to a new device. [redacted] During the noncompliance, the communication that was allowed to occur without the correct inbound and outbound restrictions [redacted] Between July 3, 2018 and October 16, 2018 normal communications and operations continued to function as expected. The noncompliance involved the management practices of asset and configuration management and reliability quality management. The root cause of this noncompliance was the design of the tool was not adequate [redacted] This noncompliance started on July 3, 2018, when the embedded switch module misconfiguration allowed the communications to occur without correct inbound and outbound access permissions and ended on October 16, 2018 when the module was successfully reconfigured.
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 this noncompliance is that improper configuration of the embedded switch could have allowed for the injection of malicious code and the possibility of the misoperation of the breakers protected by the router. The risk is not minimal because of the more than three month duration and that the entity did not discover this noncompliance through an internal control. The entity discovered this when implementing a change request. [redacted] here is no Internet access to any substation. [redacted] All of these protections make it difficult to remotely access the router. Lastly, ReliabilityFirst notes that the entity has multiple layers of physical protections [redacted] in place that make it more difficult for a bad actor to physically access the router in the substation. No harm is known to have occurred. ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1) fixed the misconfigured access control list. The technician applied the correct configuration to the embedded switch module; 2) improved the configuration tool (spreadsheet) to alert when CIP devices are being configured with a conditional format highlighting function that automatically marks the top red and the form labelling changes to be [redacted] This improvement in functionality allows the subject matter expert to become aware of the importance of the configuration as a CIP device. Also, the configuration tool now has a validation step that requires the user to input a station voltage for any network interface that's [redacted]; 3) evaluated all substations affected by the configuration tool that contained Routers with Ethernet switch modules to identify the locations where this device type would function without proper access control configuration. Based on those results, the entity determined that by adding a firewall in the path of the router\switch module device at these impacted substations increased the management capability, security posture, and consistent access control configurations; and 4) [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
RFC2019021402	CIP-005-5	R1	[redacted]	[redacted]	7/3/2018	10/16/2018	Self-Report	Completed
			[redacted] ReliabilityFirst has verified the completion of all mitigation activity.					

SERC Reliability Corporation 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
SERC2017017807	CIP-005-5	R1, R1.2	[redacted]	[redacted]	7/1/2016	5/23/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On [redacted], SERC sent the Entity an audit notification letter of the CIP compliance audit scheduled for [redacted]. On [redacted], the Entity submitted a Self-Report stating that, as a [redacted] it had an instance of noncompliance with CIP-005-5 R1, P1.2. The noncompliance involved [redacted] where the Entity did not route all external routable connectivity to an Electronic Security Perimeter (ESP) through an identified electronic access point. In mid-2015, during the transition from CIP Version 3 to Version 5, the Entity initiated a project with a contractor to remove external routable connectivity from [redacted]. The contractor removed external routable connectivity for [redacted]. On January 22, 2016, the Entity performed a review of the changes performed at the [redacted] and determined that external routable connectivity still remained between [redacted] remote terminal unit (RTU) and the local control center. However, the Entity failed to follow-up on this issue and erroneously informed the [redacted] that external routable connectivity had been properly removed and thus compliant with CIP-005-5 R1. On [redacted] while reviewing network diagrams in preparation of an upcoming CIP Audit, the Entity discovered that external routable connectivity still existed. The Entity failed to confirm that the contractor tasked with the project removed all external routable connectivity during the transition to CIP Version 5. The Entity conducted an extent-of-condition assessment by reviewing all [redacted] that contained medium impact BCSs and found no other facilities had ERC enabled. This noncompliance started on July 1, 2016, when the standard became mandatory and enforceable, and ended on May 23, 2017, when the Entity removed the external routable connectivity from the substation. The causes of this noncompliance were insufficient process document and poor internal controls that failed to ensure the Entity maintained an accurate Bulk Electric System Cyber Asset (BCA) inventory. The Entity did not require its members to implement and maintain a CIP process document detailing their obligation to maintain accurate BCA inventory. Additionally, the Entity lack an internal control, e.g., a secondary approver, to ensure it followed up with its contractor to ensure all external routable connectivity had been removed before communicating with a [redacted] that all such activity had been removed.
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's failure to protect external routable connectivity through an identified ESP electronic access point could have permitted attackers to utilize communication from those paths to gain access to facility's BES Cyber System, which ultimately could have created conditions adversely affecting operations of the substation and local operations of the BPS. However, all network traffic to this substation was on a private fiber network. Also, the Entity enabled port security at the substation to prevent unauthorized Cyber Assets from attempting to connect and communicate with authorized Cyber Assets. Circuit state changes (up/down) are monitored and alerted upon. The Entity segmented all network traffic for the substation onto its own dedicated Virtual Local Area Network that prevented any cross communications from being able to be established from another substation that could become compromised. The Entity physically secured the substation with restricted access card readers, alarming door contacts, and camera feeds with active, 24x7 real-time monitoring by the network operations center. No harm is known to have occurred. SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) removed external routable connectivity from the substation; 2) verified external routable connectivity was removed by performing a physical inspection and reviewed substation network diagrams to ensure accuracy; 3) reviewed all of the substations to ensure all of the required external routable connectivity connections were removed; 4) coached the employee that performed the audit to ensure that accurate and reliable information is transmitted between the Entity and all members; and 5) completed a review of the its CIP-002-5.1 R1 impact rating criteria assessment process and determined the following actions/controls would be implemented: a) ensured each [redacted] executed and maintained a CIP certified process document which details their obligation to maintain an accurate BCA inventory. In

	addition the Entity CIP-002-5.1a certified process document has been revised to detail how the Entity performs an assessment of the BCA inventories maintained by each [redacted]; b) provided training on the new CIP process documents to each CIP [redacted] delegate; c) implemented nine new internal controls as result of the execution on the new process documents. Seven of these controls are for each [redacted] and impacted the Entity business unit to perform an annual update for their respective BCA inventory lists. Two additional controls were implemented by the Entity to perform an annual assessment of these BCA inventory lists and update the NERC RSAW as needed; d) implemented a management review and approval of each internal control and control test plan to allow for additional transparency, accountability, and reliability.

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
SERC2018019508	CIP-010-2	R1: P1.4	[redacted]	[redacted]	10/05/2016	03/02/2018	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			On April 5, 2018, the Entity submitted a Self-Report stating that, as a [redacted], it was in violation of CIP-010-2 R1, P1.4. The Entity failed to accurately verify and document that its CIP-007 cyber security controls were not adversely affected following an upgrade to its Energy Management System (EMS). On January 16, 2018, while working on the firewalls for its primary energy control center (ECC) and backup control center (BCC), the Entity received a logging alert for the ECC firewall, but not the BCC firewall. Upon further inspection, the Entity discovered that between December 5, 2017, and December 14, 2017, an employee unintentionally disabled the BCC firewall's logging settings during a rules update to the firewall. The rules update was part of a larger upgrade to its EMS. The entity conducted an extent-of-condition (EOC) by reviewing the logging status of all CIP Bulk Electric System Cyber Assets and the associated Electronic Access Control and/or Monitoring Systems and Protected Cyber Asset (PCAs). On February 13, 2018, the Entity completed the EOC and found [redacted] additional cyber assets, which were a part of the EMS upgrade, that were not sending logs. Additionally, the Entity also found that during a transition from manual to automatic logging on October 5, 2016, [redacted] PCAs were never configured to send logs. In total, as part of its EOC, the Entity found approximately 1/3 of all EMS cyber assets were not sending logs. This noncompliance started on October 5, 2016, when the Entity stopped manually reviewing the PCAs logs, and ended on March 2, 2018, when the Entity reconfigured the cyber assets to log. The cause of this noncompliance was management oversight, specifically, ineffective project management and a lack of an internal control to ensure adherence to its change control process. Management failed to allot sufficient time for personnel to complete all manual verifications while undergoing a large-scale update to its EMS. Here, management had previously automated verification for some cyber assets. Additionally, management failed to implement all necessary internal controls to ensure that its change control process was being followed. While the process required personnel to select whether verification was completed, there was not a control in place that identified which assets needed to be manually verified in addition to the assets that provided automated verification. Therefore, the assets which required manual verification were overlooked.				
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 verify that the required cyber security controls were unaffected by its upgrades allowed its high-impact BCS Control Centers to be partially unmonitored through logging and alerting, which could have allowed vulnerabilities in the system to go undetected. However, the risk is partially reduced because the devices reside within both an ESP and PSP and there are multiple firewalls, which separate the ESP from the internet. No harm is known to have occurred. SERC determined that the Entity's compliance history should not serve as a basis for applying a penalty because the causes between the prior and instant noncompliances are different, and the prior mitigation plans would not have prevented this instance of noncompliance.				
Mitigation			To mitigate this noncompliance, the Entity: 1) reconfigured the logging settings for all assets identified in the EOC; 2) implemented an automated review that confirms assets are sending logs and prompts a manual review if no log has been produced in seven days; 3) updated its change control process to include a spreadsheet that tracks the configuration and validation of security controls for each individual asset; and 4) trained the EMS support group and supervisor on the updated change control process.				

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
SERC2017016833	CIP-007-6	R5, P5.4	[redacted]	[redacted]	07/01/2016	04/29/2019	Self-Report	Completed

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

On January 25, 2017, December 6, 2017, May 3, 2018, and June 5, 2019, the Entity submitted Self-Reports stating that, as a [redacted] it was in noncompliance with CIP-007-6 R5, P5.4. The Entity failed to change known default passwords per Cyber Asset capability on multiple Cyber Assets.

Regarding Instance 1, the Entity initially self-reported that it had placed [redacted] new [redacted] into service at a substation without changing the factory default passwords. However, after discovery and further assessment of the issue, it was determined that the Entity had incorrectly identified the [redacted] as Bulk Electric System (BES) Cyber Assets (BCAs). Because the [redacted] are not BCAs, they are not subject to the requirements of CIP-007-6 R5. Additionally, the Entity identified [redacted] different [redacted] that it placed into service without changing the default passwords.

A-

The Entity discovered the [redacted] BCAs when an engineer queried a password status report and found 'scripting failures' that were not previously identified upon installation. Prior to July 1, 2016, the date CIP Version 5 became mandatory and enforceable, the Entity deployed the [redacted] BCAs into service in [redacted] substations, which were not Critical Assets under CIP Version 3. These same substations became facilities containing medium impact BCSs under CIP Version 5.

The Entity conducted an extent-of-condition (EOC) assessment on all substations that contained medium impact BCSs using the failed status report notes to verify that password changes had occurred. The Entity concluded the EOC review on April 5, 2017, and discovered an additional instance of noncompliance with CIP-007-6 R5, which is the subject of Instance 2 described below.

The scope of affected facilities in Instance 1 included [redacted] substations and [redacted] BCAs.

The noncompliance in Instance 1 started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on August 9, 2016, when the Entity changed default passwords on [redacted] BCAs.

The cause of Instance 1 was an inadequate internal control. Specifically, the software associated with the newly implemented reports that were generated and used to confirm that default passwords were changed had a bug. As a result, the generated reports incorrectly displayed "Updated" in the Status section of the report. Although the Notes section of the report displayed "Failure," the technicians had no reason to believe that the status was incorrect causing them to read other sections of the reports.

On December 6, 2017, the Entity submitted an additional Self-Report of CIP-007-6 R5, P5.4, designated NERC ID [redacted] (Instance 2). SERC determined that this noncompliance involves the same Standard and Requirement as Instance 1 and dismissed and consolidated [redacted] with SERC2017016833.

In Instance 2, on April 27, 2017, while conducting the 2017 Cyber Vulnerability Assessment (CVA), the Entity discovered that on April 13, 2016, it commissioned [redacted] without changing the default password. Prior to July 1, 2016, the date CIP Version 5 became mandatory and enforceable, the Entity did not classify the substation housing [redacted] as a Critical Asset under CIP Version 3. Beginning with CIP Version 5, the Entity determined that the substation housed a medium impact BCS. The Entity initially discovered this instance of noncompliance on July 21, 2016, while conducting the EOC assessment associated with Instance 1 above. After initial discovery, the Entity did not change the default password due to a task list copy and paste error while [redacted] anually manipulating a list of [redacted] requiring password changes. [redacted] was not included in the list. The Entity re-discovered this instance of noncompliance while conducting the CVA on April 27, 2017. On April 27, the Entity changed the password.

The Entity determined no additional EOC was necessary following the conclusion of the CVA since it identified no additional instances of noncompliance with CIP-007-6 R5.

The scope of affected Facilities in Instance 2 included [redacted]

The noncompliance in Instance 2 started on July 1, 2016, when the Standard became mandatory and enforceable, and ended April 27, 2017, when the default password of the affected [redacted] was changed.

The cause of Instance 2 was inadequate training. The technician was trained on the specific task at issue but the quality of the training was inadequate. Specifically, the training failed to clearly explain list editing techniques, which resulted in an application usage error (a copy and paste error).

On May 3, 2018, the Entity submitted an additional Self-Report of CIP-007-6 R5, P5.4, designated NERC ID [redacted]. SERC determined that this noncompliance involves the same Standard and Requirement as Instance 1 and dismissed and consolidated [redacted] with SERC2017016833.

In Instance 3, from January 22, 2018 through February 26, 2018, the Entity placed a total of [redacted] into service at a total of [redacted] transmission substations. The Entity determined that beginning January 22, 2018, [redacted] out of the [redacted] DFRs had not had their default passwords changed upon installation. On March 28, 2018, the Entity discovered the noncompliance while conducting a

	weekly internal control whereby managers review unfinished tasks of staff in their charge. The [redacted] noticed unfinished assigned tasks to change default passwords on the [redacted] DFRs at issue. The manager questioned the employee assigned to the tasks and discovered the tasks had not been completed, and thus, default passwords were not changed prior to placing the [redacted] DFRs into service. On March 29, 2018, the Entity changed the default passwords on the [redacted] DFRs. The Entity's EOC assessment consisted of a review of all tasks assigned to the affected employee. The Entity found no additional instances of noncompliance with CIP-007-6 R5 with respect to the affected employee. The scope of affected assets in Instance 3 included [redacted] substations, [redacted] medium impact BCSs, and [redacted] medium impact BCAs. The noncompliance in Instance 3 started on January 22, 2018, when the Entity placed the first DFR into service without changing the default password, and ended on March 29, 2018, when the default passwords were changed on the [redacted] DFRs. The cause of Instance 3 was inadequate internal controls for individuals managing change management tasks. The technician was trained and understood that the tasks were required to be completed, but needed controls to help manage completion of the tasks. For mitigation, the Entity added a [redacted] to oversee the project tasks, implemented weekly meetings for technicians to inform the manager of ongoing tasks and associated deadlines, and changed its process and change task template to require the default passwords to be changed before adding a device to the Electronic Security Perimeter (ESP). On June 5, 2019, the Entity submitted an additional Self-Report of CIP-007-6 R5, P5.4, designated NERC ID [redacted]. SERC determined that this noncompliance involves the same Standard and Requirement as Instance 1 and dismissed and consolidated [redacted] with SERC2017016833. In Instance 4, on October 29, 2018, an Entity [redacted] commissioned [redacted] at a substation without changing the default password. On April 29, 2019, the Entity's Operations [redacted] group discovered the issue while performing its yearly required password changes at CIP substations. Upon discovery, [redacted] changed the default password that same day. The Entity conducted an EOC assessment by completing the annual password change process and checking whether any "as found" passwords were set to factory default. No additional instances of noncompliance with CIP-007-6 R5 were found. The noncompliance in Instance 4 started on October 29, 2018, when the Entity placed [redacted] into service without changing the default password, and ended April 29, 2019, when the password was changed on [redacted] The cause of the noncompliance in Instance 4 was a deficient procedure. Management failed to ensure that its procedure clearly defined the individual roles and responsibilities to ensure adherence to the process. Specifically, the Entity's procedure did not contain a section for updating passwords upon commissioning. For all instances, this noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on April 29, 2019, when the password was changed for the device at issue in Instance 4.
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 change default passwords on [redacted] Cyber Assets within medium impact BCS could permit hackers to utilize default passwords to modify settings, cause misoperations, and create a potential opportunity for a cascading outage to occur. However, the existence of default passwords was fairly brief, lasting 35 days for [redacted] (Instance 1), 10 months for [redacted] (Instance 2), two months for [redacted] (Instance 3), and six months for [redacted] (Instance 4). Additionally, the Entity physically secured all BCAs within Physical Security Perimeters that restricted physical access, and within secure ESPs that restricted remote access. In all instances, no harm is known to have occurred. SERC considered the Entity's compliance history and determined there were no relevant instances of noncompliance
Mitigation	To mitigate this noncompliance, the Entity: 1) changed the passwords on the devices at issue (all Instances); 2) trained/coached individuals verbally on the requirement to change default passwords (Instance 1); 3) performed Human Performance Error Review with the team of engineers (Instance 1); 4) developed lessons learned and share with other grids to prevent future occurrences of similar conditions (Instance 1); 5) issued e-mail guidance to those individuals responsible for [redacted] installations and modifications at substations system-wide to ensure those individuals are aware of possible failures associated with the password report despite it stating that the password was changed (Instance 1); 6) established a schedule reminder to run the report on a quarterly basis (Instance 1);

	7) developed a work instruction that includes a self-check after each script has been completed, in addition to the self-check of running the Password Status Report. Once published, the Entity provides training to the relevant stakeholders (Instance 1); 8) documented a work instruction to be used when bringing in a new device or new firmware. The acceptance process for any new device and firmware must first be done in test environment to ensure that all upgrades are correctly implemented before it is introduced into the production environment (Instance 1); 9) implemented in production the release that contains the bug fix for the Password Status Report after testing is completed (Instance 1); 10) updated the [redacted] change task implementation template for the "run reports and send to document librarian" task and added "check both the Status and Notes" to Step 2 of the Password Report (Instance 1); 11) modified the Excel macro used by the CIP consultant to pull the Notes column (Instance 1); 12) trained/coached the individual at issue regarding the human error that occurred during manual manipulation of a list of [redacted] requiring password changes (Instance 2); 13) implemented a quarterly review of the Entity's password system to regularly scan for and identify any occurrences going forward (Instance 2); 14) completed and closed the password changes in the change management system (Instance 3); 15) held a compliance stand-down with the [redacted] group (Instance 3); 16) conducted a human performance learning opportunity review with the responsible individual (Instance 3); 17) added a Program Manager to the organization to coordinate the project tasks across all [redacted] projects, along with other external organizations to plan and schedule the due dates for changes (Instance 3); 18) implemented 5-10 minute meetings, where each team member states their workload, the task due dates, project deadlines, and any impediments to achieving those actions. This allows the manager to understand the current status, and to redirect the team to any higher priority tasks. This would include discussion/peer check as to whether it is appropriate to extend the date on a task (Instance 3); 19) sent a request for all DFR inventory information available to the [redacted] responsible for the DFRs along with a list of the fields needed for establishing compliance, and received a response that included a full list of DFRs with all inventory information that was available for each DFR (Instance 3); 20) created an [redacted] New Hire Checklist to ensure there is training or orientation related to CIP Requirements where the requirements are addressed in the IT Procedures and how that relates to the Change Tasks (Instance 3); 21) provided training on [redacted] New Hire Checklist (Instance 3); 22) changed "P5.3" to "P5.4" and added language requiring the default passwords to be changed before adding a device to the ESP, in the [redacted] change task template (Instance 3); 23) reviewed all CIP-related [redacted] change tasks for required updates and implemented the updated task templates, which included adding any required new tasks (Instance 3); 24) performed training for all affected organizations on the updated change tasks template (Instance 3); 25) added the tasks to [redacted] administrators project team to create a new overview page to help clean the backlog and keep current on emergent assignments to the group (Instance 3); 26) gathered/captured evidence of actions taken to resolve Instance 3 (Instance 3); 27) performed validation that fixes to Task Templates as identified are performed correctly (Instance 3); 28) reviewed all CIP devices during the EOC (Instance 4); 29) updated the Transmission Procedure and associated checklist to have a section for password updates on CIP designated devices during the device commissioning process (Instance 4); 30) reviewed/updated/created a quality review checklist to include checking all applicable line items (Instance 4); 31) created a work instruction to be used by [redacted] to formalize the work flow process and added language from the Supervisory Control and Data Acquisition (SCADA) bulletins used in the training processes. Specifically included language for verifying that new points added to the model are not commissioned until verified (Instance 4); 32) updated the [redacted] procedure and checklist to give an overall work process flow with verification steps including self-checks and peer checks. Work flow process should include sections covering the use of the HUER tools and logging into the devices to verify correct passwords for the self-check and peer check sections (Instance 4); 33) provided training to the team to review the [redacted] procedure updates (Instance 4); 34) created a process to have a scheduled review of pending [redacted] tasks that have potential CIP-related implications to assure these are addressed in the appropriate time frame by verifying schedule of the site with [redacted]. A daily report is already sent out to the appropriate team showing all open [redacted] tasks assigned to each team member; 35) conducted change management training and implemented the new process noted in Step 34 (Instance 4); 36) updated the DFR Commissioning Document to address CIP-compliant passwords being put in for [redacted] devices when a device is put into service and that the [redacted] must contact the [redacted] during the install process (Instance 4); 37) updated work instructions used by appropriate [redacted] to have procedures for CIP password updates and SCADA checkout during device install and commissioning process ,and provided training on process updates (Instance 4); 38) set up a schedule with [redacted] to distribute training and performed work instruction updates across all [redacted] for changes implemented with respect to the CIP password update process, SCADA checkout process, and the [redacted] password process for commissioning devices at CIP designated sites (Instance 4); and 39) formalized the commissioning procedure (Instance 4).

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
SERC2017018663	CIP-004-6	R3, P3.5	[redacted]	[redacted]	07/13/2017	07/25/2018	Self-Report	Completed

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

On November 16, 2017, October 16, 2018, and November 6, 2018, the Entity submitted Self-Reports stating that, as a [redacted], it was in noncompliance with CIP-004-6 R3. The Entity had three instances where it failed to timely update Personnel Risk Assessments (PRAs) of employees with authorized electronic and unescorted physical access to Bulk Electric (BES) Cyber Systems (BCSs).

In Instance 1, on August 2, 2017, the Entity discovered that access management software had not initiated automatic revocation of CIP electronic and physical access for one employee with an expired PRA.

A-

The Entity performed an extent-of-condition (EOC) assessment by using a new automated rule that was created to pull any instances where an employee had an expired PRA. The EOC identified two additional employee users who had not had a PRA completed within the last seven years. For all three employees, July 13, 2017, was the earliest instance of an overdue PRA. On August 7, 2017, the Entity revoked access from the three employees.

Combined, the three individuals had potential access to [redacted]

The cause of Instance 1 was a failure to verify that the software was properly functioning. Specifically, during testing of a new software project, an analyst incorporated a new software feature. The CIP access removal logic was an internal portion of the code in the workflow's set of events that gets triggered when an employee or contractor is terminated. When the new feature was introduced, the logic was corrupted and access revocation was automatically applied only to terminated employees.

On October 16, 2018, the Entity submitted an additional Self-Report of CIP-004-6 R3, P3.5 [redacted] which was dismissed and consolidated with the original November 16, 2017 Self-Report.

In Instance 2, on July 25, 2018, the Entity's [redacted] notified the Entity's [redacted] that a PRA expiration report identified one employee with an expired PRA.

As an overview of the Entity's process, the Entity's identity management system generated a PRA expiration report on a weekly basis. The Entity's [redacted] utilized a shared access management tracking spreadsheet with Human Resources (HR). HR manually entered upcoming PRA expirations into the spreadsheet. Due to a spreadsheet filtering oversight, an analyst inadvertently hid spreadsheet rows of three individuals in order to limit the display of relevant records. As a result of the hidden rows, [redacted] did not identify one employee with an expired PRA (the other two were not overdue). The expired PRA was due for completion on July 20, 2018. However, the Entity did not complete the PRA for the employee until July 31, 2018.

A more extensive EOC assessment conducted in relation to Instance 1 by analyzing the tracking spreadsheet to determine if there were any expired or missing records noted. As a result of the EOC, the expired PRA for the employee at issue was discovered. The Entity found no additional instance where an employee had an expired PRA. On July 25, 2018, the Entity revoked the employee's access.

The scope of the noncompliance in Instance 2 impacted physical access to [redacted]

On November 6, 2018, the Entity submitted an additional Self-Report of CIP-004-6 R3, P3.5 [redacted] which was dismissed and consolidated with the original November 16, 2017 Self-Report.

In Instance 3, on July 25, 2018, while performing an ad hoc access review the Entity discovered that its identity management system was not writing access prevention flags to a new user's record. The Entity used access prevention flags on user records to disallow access provisioning to personnel requesting access in the event of an expired PRA, training, etc. Later that day, further review resulted in the discovery that four users had expired PRAs. This instance involved a modification to a facility that required a PSP to be commissioned. Because of this, personnel working in that physical area needed to be upgraded to CIP-related roles even though there were no changes to their job function. The CIP PSP commissioning task template in the change management system did not account for this type of situation.

On the day of discovery, July 25, 2018, the Entity revoked access for all four users.

	On October 12, 2018, the Entity performed an EOC assessment by reviewing all individuals with CIP access and confirming their User IDs against the authorization records to confirm need and approval, and then confirmed that each individual with access had a current and valid PRA and recent cyber security training. The Entity identified no new or additional instances. The only facility that could have been affected through possible physical access by the personnel at issue was a single facility containing [redacted] The cause of Instance 2 and Instance 3 was a deficient procedure. The procedure did not clearly define the roles and responsibilities for the processing of authorization records, which created confusion as to ownership of specific tasks and resulted in inconsistent application of the procedure. This noncompliance started on July 13, 2017, when in Instance 1, the three employees' PRAs became due, and ended on July 25, 2018, when the Entity revoked access to the employee in Instance 2.
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 conduct a timely PRA increased the chance of malicious actors having physical/electronic access to BCAs. However, in each instance, the noncompliance period was brief (longest period was 151 days) relative to the seven year requirement period. Additionally, all other applicable CIP cyber protections were in-service, including automatic revocation of access for terminated individuals, and, all personnel at issue were in good standing with the Entity throughout the duration of the noncompliance. No harm is known to have occurred. SERC considered the Entity's CIP-004-6 R3, P3.5 compliance history in determining the disposition track. The Entity has one relevant prior noncompliance with CIP-004-6 R3, P3.5. SERC determined that the Entity's relevant compliance history should not serve as a basis for applying a penalty. The underlying cause of the instant and prior noncompliance is different. The cause of the prior noncompliance was an employee's failure to follow the manual procedures used to review access and PRA status. Therefore, the steps taken to mitigate the prior noncompliance could not have prevented the occurrence of the instant noncompliance.
Mitigation	To mitigate the noncompliance, the Entity: 1) removed CIP access from the employees at issue (all Instances); 2) corrected and verified the workflow that executes Request Access Change events (Instance 1); 3) implemented and executed a manual daily check to ensure automated tasks were properly executing and performing as expected (Instance 1); 4) trained users on the new manual daily check (Instance 1); 5) performed a Human Performance Error Review. (Instances 2 and 3); 6) updated background check process to ensure that all steps were included in the work instructions (Instance 2); 7) worked with team members to evaluate automation options for the manual background check process. (Instance 2); 8) updated the background check process Work Instruction to specify action steps for processing of authorization records (Instance 2); 9) trained [redacted] on the updated work instruction (Instance 2); 10) redesigned the background check alert spreadsheet to take advantage of data validation and automated status assignment updates, eliminate the need to hide row data, and simplify the renewal list (Instance 2); 11) conducted a stand down training completion acknowledgement (Instance 2); 12) documented an interim process for validation of authorization records (background check date, training date, manager authorization, and role authorization) in order to verify that the identity management system process was performed properly. The interim process was put in place to manually address each request for access that was submitted. The manual process was documented in a nonpublished work instruction during the transition to the new identity management system (Instance 3); 13) updated the background check process work instruction to specify actions steps for processing authorization records and distributed the nonpublished work instruction for team review and training (Instance 3); and 14) worked with change management to ensure that all change tasks specific to access management were included in the CIP PSP commissioning task template. As a result, in the future, any personnel working in a physical area that is converted to a PSP will have their roles updated as part of the zero day testing that happens with every PSP commissioning task (Instance 3).

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 Find, Fix, Track, and Reports 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	RFC2018019429	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 years
2	RFC2018019430	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 years
3	RFC2019021624	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 years
4	RFC2019021567	Yes		Yes	Yes		Yes		Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 years
5	RFC2019021568	Yes		Yes	Yes		Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 years
6	TRE2019020991			Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
7	TRE2017018207	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
8	TRE2017018211	Yes		Yes	Yes				Yes	Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
9	TRE2017018672	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
10	TRE2018019173	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
11	WECC2018019934			Yes	Yes					Yes				Category 2 – 12: 2 years
12	WECC2016016680	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
13	WECC2017017296	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
14	WECC2018019704	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years

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
RFC2018019429	CIP-010-2	R1	[redacted]	[redacted]	7/1/2016	12/14/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On March 15, 2018, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-010-2 R1. On February 20, 2018, during a quality review of work orders for baseline changes in 2016, the entity discovered several baseline updates at medium impact substations that were not documented within the 30-day timeframe. In total, the entity identified [redacted] instances where baselines were not updated within 30 days of a baseline impacting change, with durations ranging from 1 day to 323 days. [redacted] In all instances, the entity completed all authorization steps before making the baseline changes, but experienced issues on the back end of the process with respect to documenting the changes appropriately. The majority of these instances were either the result of documentation issues (i.e., the information was placed in the wrong field in [redacted] for baseline recordation) or supervisors failing to approve baseline updates in sufficient time. [redacted] these instances were the result of a technical issue where [redacted] failed to sync with the baseline system of record. In all cases, the entity had the relevant change information in the two databases used to facilitate its change management process, but the data did not always match between the two systems. While this discrepancy could have affected future reviews or changes, these issues did not impact any of the security controls related to the devices. All security controls [redacted] continued to protect the devices along with physical access restrictions to the location of the devices. The root causes of this noncompliance were (a) the failure by field personnel to follow the established procedure regarding the entry of information into the [redacted] software; and, (b) insufficient processes for ensuring that supervisor approval is performed on time when responsible individuals retire or take vacation. These major contributing factors involve the management practices of asset and configuration management, which includes controlling changes to assets and configuration items and baselines, and workforce management, which includes managing employment status changes and providing training, education, and awareness to employees. This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-010-2 R1 and ended on December 14, 2018, when the entity completed its Mitigation Plan, including implementing a technical solution to the syncing issue between [redacted] and the baseline system of record.
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 update baselines within 30 days of a baseline impacting change is that the entity may make future changes based on outdated or incorrect information, which could have an adverse impact on the system. The risk is not minimal in this case based on the number of occurrences and the length of time it took the entity to identify some of the issues. The risk is not serious or substantial in this case based on the following factors. First, for each of the instances discussed above, the entity completed the properly authorized physical field work in accordance with engineering expectations, but just did not document it properly. Second, the entity reviewed each of the changes for their operational and security controls prior to being made available for installation on each device, and each were determined to have no impact to the field operations of the devices. Additionally, after the changes were implemented, the entity also verified that the security controls were not adversely affected. Third, all security controls continued to protect the devices throughout the duration of these issues. Fourth, the entity manages baseline [redacted] Furthermore, the entity processes [redacted] per month. These factors support the conclusion that this was not indicative of a systemic issue. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history does not warrant an alternative disposition method and should not serve as a basis for applying a penalty because most of the prior noncompliances are distinguishable as they involved different root causes. For any issues that may arguably be similar, ReliabilityFirst determined that the current noncompliance continues to qualify for compliance exception treatment as it posed only minimal risk and is not indicative of a systemic or programmatic issue.
Mitigation	To mitigate this noncompliance, the entity: 1) assigned a specific group of people as approvers under a procedure to implement the baseline system of record approval process task; 2) ensured the approvers in their region are able to perform the required [redacted] approvals; 3) provided leadership to the assignments for the approvers in their region, areas of responsibility for performing the required [redacted] approvals; 4) ensured the [redacted] in the baseline system of record reflected the actual field configuration of the device; 5) reviewed options for an evidence review notification upon work order closure rather than [redacted] to create an oversight and evidence review process for authorized baseline changes; 6) worked with the [redacted] system of record vendor in order to evaluate the issues that occurred and propose possible solutions; 7) created an action plan to implement the selected option from step 5; 8) performed the Q2 2018 Quarterly Review to identify any issues amid ongoing mitigation, before implementation of vendor solution; 9) created an implementation plan for the possible solution found from step 6; 10) documented the prior root causes and their associated mitigation for reference in this Mitigation Plan as context for discussion regarding the sole repeat issue; 11) reviewed the prior root causes and determine if the proper causes were identified and if not, identify and address the root cause(s); and 12) performed a Quality assurance review of all applicable assets in Q4 2018 to validate that the mitigating actions are resulting in correct performance as expected.

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
RFC2018019429	CIP-010-2	R1	[redacted]	[redacted]	7/1/2016	12/14/2018	Self-Report	Completed
			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
RFC2018019430	CIP-010-2	R1	[redacted]	[redacted]	7/1/2016	6/30/2018	Self-Report	Completed

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

On March 16, 2018, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-010-2 R1. In February 2018, during routine reviews of data, the entity identified two issues: (a) the failure to properly classify Cyber Assets as Protected Cyber Assets (PCAs); and, (b) errors in adhering to the process for documenting the authorization of baseline changes.

With respect to the first issue, on February 15, 2018, during a review of an Electronic Security Perimeter (ESP) diagram, the entity identified differences between Cyber Assets listed on an ESP diagram for a substation and the associated Cyber Asset records. This information mismatch caused the entity to review all [redacted] of its ESP diagrams. The entity identified an additional [redacted] instances where a Cyber Asset was not properly classified as a PCA. These [redacted] assets are located at three different substations, each of which are medium impact substations without External Routable Connectivity (ERC). At the first substation, [redacted] were not identified. At the second substation, [redacted] were not identified. At the third substation, [redacted] were not listed correctly as PCAs. For these two devices, the entity missed performing a Cyber Vulnerability Assessment (CVA) on the specific devices because the devices were classified as out-of-scope. The entity also discovered that as a result of not being properly identified as PCAs, [redacted] assets at the first two substations were not enabled for logging as required by CIP-007.

Even though [redacted] devices were not properly classified as PCAs, key security controls were deployed and protected the devices. For example, [redacted]. Moreover, for [redacted] assets at the first two substations, the entity also had additional controls in place to prevent the introduction of unexpected changes and to provide the entity with visibility should the devices experience unexpected changes. Specifically, [redacted] With respect to [redacted] devices at the third substation, the baseline information was [redacted] The fact that they were not classified as PCAs resulted in these devices [redacted] or [redacted]. However, even though [redacted] devices were not included individually in a CVA during the time they were misclassified, the entity was managing ([redacted] devices with the same firmware which were part of the CVAs. Based upon that work, the entity determined that no updated firmware was issued related to these devices during the time the devices were misclassified.

The root cause of this issue was data entry errors in the entity's asset tracking system. The entity either entered incorrect information or was missing key information needed to properly identify the assets as PCAs in its queries and review.

With respect to the second issue, on February 16, 2018, as part of a routine engineering review, the entity identified 2 devices that did not have all levels of authorization for documenting baseline changes. Further review identified [redacted] additional devices without proper authorization of baseline changes. The baseline changes were all operationally necessary, but the authorization for the changes were not documented pursuant to the entity's procedures. The relevant part of the procedure constitutes one of the authorizations required for making baseline changes. [redacted] All of these instances involved firmware updates, and all were intentional, planned work, and not inadvertent installations. The result of missing the authorization review was that the entity missed an opportunity to identify a security control that needed to be enabled. However, during mitigation, the entity confirmed that no security controls were actually impacted by the firmware changes.

Even though the entity failed to conduct authorization reviews in these instances, the entity had additional controls in place that would have deterred the introduction of unexpected changes and would have provided the entity with visibility should the devices experience unexpected changes. Specifically, [redacted] Additionally, all devices were configured with [redacted].

The root cause of this issue was the fact that the entity's baseline management system was configured to allow new devices and CIP changes to be implemented without authorization reviews and gaps in understanding on the part of field engineers on CIP baseline change requirements.

The root causes of these two issues involve the management practices of verification, in that the entity failed to have sufficient internal controls in place to ensure that data was properly captured in its various databases, and workforce management, which includes providing training, education, and awareness to employees.

This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-010-2 R1 and ended on June 30, 2018, when the entity corrected all data discrepancies.

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 first issue (i.e., failing to properly identify assets as PCAs) is that the entity may not apply the required security controls (such as logging) or flag changes to these assets for future authorization reviews, which could have led to unexpected changes or missed baseline management and security controls review for future changes. This risk was mitigated by the following factors. First, these misclassifications are inherently low risk because, as PCAs, these devices do not have an operational impact if rendered inoperable. Second, the entity had additional security controls in place that protected the devices throughout the

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
RFC2018019430	CIP-010-2	R1	[redacted]	[redacted]	7/1/2016	6/30/2018	Self-Report	Completed

duration of the issue. Third, all of these devices were located at locations without ERC, meaning that even if the additional security controls were defeated, these devices would only have the capability to impact the local substation, which limits the opportunity for remote unauthorized or malicious access. Furthermore, to reduce the risk of physical access to the devices at issue, the entity protects all of these devices within [redacted]. Consequently, in order to potentially compromise these devices on site, an individual would need [redacted].

The risk posed by the second issue (i.e., failing to perform authorization for all applicable assets) is that security controls could have been impacted by the changes. The risk is not minimal in this case due to the number of instances and the time it took the entity to identify the errors. The risk is not serious or substantial in this case based on the following factors. First, the type of changes involved in these instances was firmware updates, which generally present a lower risk to the device because the updates are tested and issued by the vendor so any security controls testing performed would likely not have identified any impact to the device based upon the change. (The entity subsequently confirmed that the changes had no impact on the security controls. Furthermore, [redacted]) Second, additional security controls were in place on these devices, were documented within the settings records, and procedurally would be maintained as device settings even without the authorization reviews. Third, all but one of the affected devices are located at non-ERC substations, limiting the opportunity for remote unauthorized or malicious access. (For the one device located at a location with ERC, the entity performed the authorization review within a matter of days after the change.) Fourth, to reduce the risk of physical intrusion, the entity protects all of the devices within physically controlled zones, access to which is controlled through [redacted]. No harm is known to have occurred.

The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history does not warrant an alternative disposition method and should not serve as a basis for applying a penalty because most of the prior noncompliances are distinguishable as they involved different root causes. For any issues that may arguably be similar, ReliabilityFirst determined that the current noncompliance continues to qualify for compliance exception treatment as it posed only minimal risk and is not indicative of a systemic or programmatic issue.

Mitigation

With respect to the first issue, to mitigate this noncompliance, the entity:

1) reassessed [redacted] to include the routable protocol connectivity. The [redacted] should be correctly categorized as PCAs in the asset management database;
2) assessed [redacted] to include the routable protocol connectivity. The [redacted] should be correctly categorized as PCAs in the asset management database;
3) assessed the [redacted] as having routable connectivity to the ESP. The [redacted] should be correctly associated with the ESP in the asset management database;
4) created work orders to issue and deploy settings to [redacted];
5) performed [redacted] to identify any issues amid ongoing mitigation, before implementation of vendor solution;
6) created a specific job aid to be utilized when completing assessments in the asset management database; and
7) provided a communication on release of the specific job aid to be utilized when completing assessments in the asset management database.

With respect to the second issue, to mitigate this noncompliance, the entity:

1) sent a communication to all members of the department restating that [redacted]
2) sent a communication to the engineering group reinforcing the fact that authorization consists of [redacted];
3) initiated (a) authorization reviews for all instances in question to determine impact (if any) on the CIP Controls; and [redacted]; and
4) created and provided a robust training on issuing settings and authorization reviews as part of an annual and new hire training for engineers. Training must include some verbiage in settings reviews at Medium Impact sites.

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
RFC2019021624	CIP-004-6	R5	[redacted]	[redacted]	12/15/2018	1/29/2019	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On May 24, 2019, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-004-6 R5. On December 14, 2018, a contractor working on a project under the direction of an entity project leader voluntarily separated from the entity upon completion of assigned work. The assigned project leader was aware of the separation; however, the assigned administrative leader was unaware of the separation. The administrative leader was responsible for, *inter alia*, initiating removal of the contractor's ability for access within 24 hours of the separation. Upon learning of the separation on January 29, 2019, the administrative leader initiated removal of the contractor's ability for access. The entity had previously implemented a detective control to identify late access revocations, but in this case, it did not discover the noncompliance until February 4, 2019. The detective control was designed to [redacted] In this case, [redacted] An employee who regularly reviews NERC-related revocation records flagged this particular revocation for further investigation as a possible noncompliance. During the course of the engagement, the contractor was not provisioned physical access or an identification badge, thus no physical access revocation was necessary. The contractor had been provisioned the ability for Interactive Remote Access to Bulk Electric System (BES) Cyber System Information (BCSI) and numerous assets and systems. Examples of the contractor's remote access abilities included: [redacted] The root cause of this noncompliance was a lack of communication between the assigned project leader and the assigned administrative leader regarding the contractor's employment status. Further, the entity did not have any controls that would trigger or facilitate such communication. This noncompliance involves the management practices of planning and workforce management. The entity was relying on contractors as part of the above-referenced project, and it needed to identify and plan for risks associated with such engagements and more effectively manage those risks. One way to achieve this is through proper workforce management. Workforce management includes the development and implementation of clear, thorough, and executable processes, procedures, and controls that are designed to minimize the frequency of human factor issues, such as neglecting to communicate a contractor's last day of work to appropriate personnel who are responsible for initiating the removal of contractor access to BES Cyber Systems. This noncompliance started on December 15, 2018, after the entity failed to initiate removal of a contractor's ability for access within 24 hours of separation and ended on January 29, 2019, when the entity initiated the removal.
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 of this noncompliance is that an individual could exploit or misuse remaining access and cause corresponding harm to the BPS. The risk was not minimal in this case because of the duration of the noncompliance, the scope of the contractor's remote access abilities, roles, and privileges, and the entity's lack of preventative controls. Further, the entity's primary detective control failed [redacted] The risk was not serious or substantial in this case because this noncompliance involved a trusted contractor who voluntarily separated from the entity on good terms upon completion of assigned work. The entity reviewed its records and verified that the contractor did not use or attempt to use remote access capabilities during the period of this noncompliance. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances involved different issues and causes. Further, the current noncompliance posed only a moderate risk to the BPS, is not indicative of a systemic issue, and was self-identified and corrected.
Mitigation	To mitigate this noncompliance, the entity: 1) revoked the contractor's access; 2) reviewed access logs to verify that no unauthorized access to the BES Cyber Systems took place; 3) reviewed access revocation responsibilities with appropriate personnel and required said personnel to retake training; 4) conducted a stand-down to reinforce understanding of, and compliance with, CIP-004 R5 requirements, and the stand-down included leadership from business units involved in the project; 5) clarified with appropriate personnel the importance of entering specific and accurate information into the system; 6) issued a "required read" to all pertinent supervisors that reinforced their responsibility for timely management of access for all administrative reports and for proactively establishing lines of communications necessary to accomplish this task; and 7) added a standing bullet item to the weekly project update template for projects identified as having a NERC-related impact to review/discuss "upcoming changes in contractor status."

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
RFC2019021567	CIP-006-6	R2	[redacted]	[redacted]	6/14/2018	1/7/2019	Self-Report	Completed

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

On May 10, 2019, the entity submitted a Self-Report stating that [redacted] it was in noncompliance with CIP-006-6 R2. There are three separate instances in this noncompliance. The applicable systems affected by these three instances are as follows: [redacted]

First, on June 14, 2018, the entity discovered that an employee with authorized unescorted physical access provided access to an employee without authorized unescorted access into a Physical Security Perimeter (PSP) containing a [redacted] and did not follow visitor logging or escort procedures. This instance began and ended on June 14, 2018. The employee was unescorted inside the PSP for 1 hour and 24 minutes, and then left the PSP. The visitor-employee at issue was a [redacted]. He was in [redacted] and thus had a valid reason to be inside the PSP.

While inside the PSP, the entity discovered that the visitor-employee had not been logged or escorted in and was asked to leave. Upon this discovery, entity personnel triggered a physical access control system alarm and a follow-up call by security personnel was made on June 14, 2018.

The root cause of this first instance is ineffective training as the individual with authorized access did not follow the entity's visitor escorting procedure requirements.

Second, on November 12, 2018, the entity discovered that an employee without authorized unescorted access tailgated another individual into a PSP containing a [redacted] The individual was unescorted for 14 seconds and, once identified as being inside the PSP, was escorted back outside of the PSP area. This instance began and ended on November 12, 2018. The employee at issue is an [redacted] She was at the location to attend a meeting outside of the PSP. She mistakenly entered the PSP by tailgating behind personnel entering the PSP. She did not have a reason to enter the PSP.

An entity employee with authorized unescorted access discovered this second instance. The employee reported the incident to the security personnel at the [redacted] on November 12, 2018.

The root cause of this second instance is ineffective training as the individual with authorized access did not follow the entity's visitor escorting procedure requirements by allowing an employee to tailgate into the PSP behind him.

Third, on January 7, 2019, the entity discovered that an employee unknowingly tailgated into a PSP containing a [redacted] due to a change in his access related to a promotion. The employee followed another individual into a PSP after swiping his badge and not realizing that his badge was no longer active. While inside the PSP, the employee was not logged as a visitor inside the PSP and was not escorted. The instance began and ended on January 7, 2019. The employee was unescorted inside the PSP for 2 hours and 19 minutes. Upon discovery of the issue, he was logged as a visitor. The employee at issue is a [redacted] His unescorted physical access had been revoked by an automated process after a promotion. A timely re-approval of his access did not take place. He was reporting to work and had a valid reason to be inside the PSP. The entity promptly reapproved his access upon discovery of the issue.

The promoted employee's manager discovered this instance when the promoted employee informed his manager that he had lost electronic access to a CIP system within the PSP. Upon investigation, the entity determined that the employee had lost unescorted physical access as well. The employee's manager reported the event the same day it occurred.

The root cause of this third instance is ineffective training as the individual with authorized access did not check to see if he still had unescorted physical access following his promotion and unknowingly tailgated into a PSP by not checking to see if badge swipe had been recognized as authorized.

This noncompliance involves the management practices of workforce management, reliability quality management, and verification. Ineffective training is the root cause for each of the instances as all of the individuals involved did not follow the entity's visitor escorting procedures.

This noncompliance started on June 14, 2018, when, in the first instance, an employee with authorized unescorted physical access provided access to an employee without authorized unescorted access into a PSP and ended on January 7, 2019, when, in the third instance, the employee not logged as a visitor inside the PSP and not escorted within the PSP exited the PSP.

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 this noncompliance is allowing unauthorized employees to access BES Cyber Systems without supervision (an escort) and without logging their entrance and exit. The risk is not minimal because of the long duration of the first instance where the employee was unescorted inside the PSP for 1 hour and 24 minutes. The risk is lessened because in the first and third instances, the employees had valid reasons to be inside the PSP. In the second instance, the employee did not have a valid reason to be inside the PSP, but she was only inside the PSP for 14 seconds. In all three instances, all of the employees were in good standing with the entity. The employee involved in the third instance had both current CIP training and a valid Personnel Risk Assessment (PRA) and his access was never intended to be revoked due to his promotion. Lastly, the entity confirmed that there were no adverse effects to any equipment identified because of this lapse of continuous escorting in any of the instances. No harm is known to have occurred.

Although the current noncompliance involves conduct that is arguably similar to the previous noncompliance, the current noncompliance continues to qualify for FFT treatment as it involves high-frequency conduct for which the entity has demonstrated an ability to promptly identify and correct noncompliances.

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
RFC2019021567	CIP-006-6	R2	[redacted]	[redacted]	6/14/2018	1/7/2019	Self-Report	Completed
Mitigation			To mitigate this noncompliance: For the first instance, the entity: 1) advised the supervisor of the employee with authorized physical access of the incident and was requested to review the requirements for escorting visitors with the employee; 2) provided refresher training sessions for PSP entry requirements; and 3) issued letters of reaffirmation to each of the employees involved in this potential violation instance. For the second instance, the entity: 1) escorted the unescorted HR employee out of the PSP immediately upon discovery; 2) reminded the individual who allowed the tailgating incident of the importance of monitoring visitors and completed a review of the applicable [redacted] procedure with his supervisor; 3) reviewed and revised a [redacted] procedure, an escort card, to make it clearer that every visitor, will have an escort called to take the visitor to the meeting location, regardless of where it is; 4) reviewed the clarified [redacted] procedure with security guard personnel; 5) updated the applicable corporate policy to specify a person's responsibility to make certain no one tailgates behind them; and 6) updated awareness training to reflect the updated policy. For the third instance, the entity: 1) logged the employee as a visitor and escorted the employee inside the PSP; 2) re-authorized the employee's authorized, unescorted physical access; 3) updated the applicable corporate policy to specify a person's responsibility to make certain no one tailgates behind them; and 4) updated awareness training to reflect the updated policy.				

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021568	CIP-002-5.1	R1	[redacted]	[redacted]	7/1/2016	1/4/2019	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On May 10, 2019, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-002-5.1 R1. On September 28, 2018, the entity discovered that [redacted] BES Assets [redacted] containing Low Impact Bulk Electric System (BES) Cyber Systems had been excluded from the entity's approved list of BES Cyber Systems and BES Assets Containing Low Impact BES Cyber Systems pursuant to CIP-002-5.1. After making this discovery, the entity performed an extent of condition analysis. That analysis identified [redacted] additional BES Asset containing Low Impact BES Cyber Systems that had been excluded from the entity's approved list of BES Cyber Systems and BES Assets Containing Low Impact BES Cyber Systems. In total, [redacted] BES Assets were excluded from the entity's list. The entity discovered these issues while performing an internal control to review BES Cyber Systems and BES Assets Containing Low Impact BES Cyber Systems. The entity determined that these exclusions occurred due to an incomplete initial Impact Rating verification methodology. The [redacted] BES Assets, which are [redacted] are protected by the same programs and procedures that are in place for all Low Impact BES Cyber Systems that are currently enforceable, including Cyber Security Awareness and a Cyber Security Incident Response Plan. This noncompliance involves the management practices of asset and configuration management and implementation. Asset and configuration management is involved because a failure to correctly classify and capture [redacted] BES Assets was the result of an insufficient asset management process. Implementation management is involved because the entity operated [redacted] BES Assets without an effective process to determine the necessary protections required for the assets. The root cause of the noncompliance was an incomplete initial Impact Rating verification process pertaining to CIP-002-5.1. This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-002-5.1 R1 and ended on January 4, 2019, when the entity had designated and approved all [redacted] BES Assets Containing Low Impact BES Cyber Systems as BES Assets on a revised list.
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 this noncompliance is that an entity that is unaware of which assets it must protect may fail to implement the proper security measures on those devices thus increasing the probability of successful adverse infiltration of those assets. The risk is not minimal because of the long duration. The risk is lessened because the [redacted] BES Assets are protected by the same programs and procedures that are in place for all Low Impact BES Cyber Systems that were enforceable throughout the duration of the noncompliance, including Cyber Security Awareness and a Cyber Security Incident Response Plan making this primarily a documentation issue. Also, [redacted] of the [redacted] BES Assets did not have External Routable Connectivity. Further reducing the risk, the entity restricts electronic access to all BES Cyber Systems using appropriate access controls. Additionally, the entity restricts physical access to al [redacted] with the use of [redacted] and [redacted] No harm is known to have occurred. ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1) reviewed and approved a revised list of BES Cyber Systems and Assets Containing Low Impact BES Cyber Systems, which included [redacted] that contain Low Impact BES Cyber Systems; 2) entity reviewed and approved [redacted] BES Asset to be added to the list of locations containing Low Impact BES Cyber Systems; and 3) created and approved a new procedure that clearly delineates how all initial Impact Rating Criteria should be verified for the list of applicable substations currently in service or planned to be in service within the next five years. ReliabilityFirst has verified the completion of all mitigation activity.

Texas Reliability Entity, Inc. (Texas RE) 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
TRE2019020991	CIP-004-6	R4; 4.1 and 4.2	[redacted] (the "Entity")	[redacted]	07/01/2016	01/22/2020	Compliance Audit	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	During a Compliance Audit conducted from [redacted], Texas RE determined that the Entity, as a [redacted], was in noncompliance with CIP-004-6, R4. Specifically the Entity did not have sufficient evidence, consistent with the Entity's implemented documented access management program, for authorization records for vendor personnel with electronic access pursuant to CIP-004-6, R4.1. Additionally, the Entity did not verify at least once each calendar quarter (Q4 of 2016 to Q4 of 2017) that individuals with active electronic access or unescorted physical access have authorization records pursuant to CIP-004-6, R4.2. There were two different vendor providers involved with this issue. The root cause of this noncompliance was that the Entity erroneously believed that vendor-authorized personnel lists satisfied CIP-004-6 R4.1, and was erroneously treating this vendor's list as the authorization records for its quarterly verification under CIP-004-6, R4.2. This noncompliance started on July 1, 2016, when the standard became effective, and ended on January 22, 2020, when the Entity submitted evidence that showed that the electronic access of the second of the two vendors was revoked.
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 potential risk of unauthorized access to into a Physical Security Perimeter or to physical or electronic designated storage locations for BES Cyber System Information is that the unauthorized access could be used to compromise the physical security of BES Cyber Systems, and ultimately impact the reliability and security of the bulk power system. The potential risk from failing to regularly verify that individuals with active electronic access or unescorted physical access have the proper authorization records is that an Entity may fail to discover that an unauthorized individual provisioned themselves access. However, the risk of these noncompliances was reduced by the following factors. Upon creating proper authorization records for contract personnel with electronic access, the Entity did not discover any contract personnel who had been granted access who should not been given access. Additionally, the Entity has a relatively small footprint [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) created authorization records for contract personnel with electronic access for the first vendor; 2) decommissioned the SCADA EMS system of the first vendor and revoked electronic access for personnel of the first vendor; 3) revoked the second vendor's electronic access so that vendor only has view-only access; and 4) provided sufficient evidence for CIP-004-6, Part 4.2. Texas RE has verified the completion of all mitigation activity.

Texas Reliability Entity, Inc. (Texas RE) 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
TRE2017018207	CIP-007-6	R1	[redacted] (the "Entity")	[redacted]	07/01/2016	02/12/2018	Compliance Audit	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	During a Compliance Audit conducted per an existing multi-region registered entity agreement from [redacted], Texas RE determined that the Entity, as a [redacted] was in noncompliance with CIP-007-6 R1. Specifically, the Entity did not enable only logical network accessible ports that have been determined to be needed for individual Cyber Assets associated with the Entity's energy management system, which is identified as a High Impact BES Cyber System. Furthermore, the Entity did not document the justification for UDP ports determined to be needed at one of its generating facilities, which contains a Medium Impact BES Cyber System. The root cause of the noncompliance was an insufficient process for compliance with CIP-007-6 R1. Regarding the Control Center, the Entity mistakenly believed controlling ports and service at the Electronic Security Perimeter (ESP) was acceptable to meet compliance with this requirement, and the Entity failed to enable only logical network accessible ports on the individual Cyber Assets. For the issue at the [redacted], the Entity had not completed the documentation and justification of UDP ports by the effective date of the Entity's identification of that facility as an asset containing a Medium Impact BES Cyber System. This noncompliance started on July 1, 2016, when the Reliability Standard became enforceable, and ended on February 12, 2018, when the Entity verified only logical network accessible ports determined to be needed are enabled.
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. A failure to disable enabled logically accessible network ports that are not needed unnecessarily increases the attack surface of the affected Cyber Asset. For example, an attack on a Physical Access Control System can compromise the implemented physical security protections an entity has deployed, either by allowing unauthorized individuals to enter a Physical Security Perimeter (PSP) or by preventing authorized individuals from entering a PSP when needed. Regarding the energy management system BES Cyber System, the Entity's portfolio includes a [redacted], although the Entity stated that [redacted]. The specific generating facility at issue is a [redacted] with a [redacted], and the asset is associated with a Medium Impact BES Cyber System. However, the risk of this noncompliance was lessened by several factors. To begin, regarding the energy management system BES Cyber System, while the Entity was not justifying and documenting ports at the Cyber Asset level, they were documenting and justifying TCP and UDP ports at the ESP level and used methods to deter, detect, and prevent malicious code at the ESP boundary. Further, with regards to the generating facility issue, the Entity is also using endpoint security software for whitelisting. 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) deployed a [redacted] to verify only logical network accessible ports determined to be needed are enabled; 2) documented a justification for UDP Ports/Services for the substation location; 3) to prevent reoccurrence, ensured continued compliance with NERC CIP-007-6 R1 requirements by maintaining an automated compliance tracking system that, on a quarterly basis, automates scheduled tasks to review and validate the ports/services inventory; and 4) to prevent reoccurrence, ensured all unsupported/unpatchable Cyber Assets at the generating facility location are monitored by cloud-native endpoint security software. Texas RE has verified completion of all mitigating activities.

Texas Reliability Entity, Inc. (Texas RE) 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
TRE2017018211	CIP-006-6	R1; P1.2, P1.3	[redacted] (the "Entity")	[redacted]	07/01/2016	07/01/2019	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 Compliance Audit conducted per an existing multi-region registered entity agreement from [redacted], Texas RE determined that the Entity, as a [redacted] was in noncompliance with CIP-006-6 R1. Specifically, the Entity failed to, where technically feasible, utilize sufficient physical access controls to collectively allow unescorted physical access into Physical Security Perimeters (PSPs) to only those individuals who have authorized unescorted physical access for PSPs associated with the Entity's energy management system BES Cyber System.

The first instance of noncompliance involves PSPs at the Entity's [redacted] location, which are associated with the Entity's [redacted] BES Cyber System. The Entity stored [redacted] BES Cyber Assets (BCAs), which were used as operator workstations, in locked cabinets, with each cabinet considered by the Entity to be a PSP. However, on June 26, 2017, during the Compliance Audit, the Entity's personnel discovered that the electronic locks for these cabinets failed intermittently, allowing access to the BCAs without the use of physical access controls. During the same day that the issue was discovered, the Entity secured the cabinets using keyed physical locks, and on June 27, 2017, the electronic locks were corrected to function as intended. In addition, keyboards and mice connected to the BCAs extended beyond the cabinets and were physically accessible without the use of physical access controls. Because the keyboards and mice required the use of a badge and pin code to interact with the attached BCAs, the Entity's personnel mistakenly believed that this configuration was compliant with CIP-006-6 R1. During November 2017, the Entity began the process of constructing a single PSP enclosing all of the BCAs at issue, which was commissioned on July 1, 2019, ending the noncompliance.

The second instances of noncompliance involves a PSP at a different location, which is associated with the same BES Cyber System. A cabinet PSP, which housed switches, firewalls, and [redacted] BCAs, at the [redacted] backup Control Center had an aperture, potentially allowing access to the network cables inside the PSP without the use of physical access controls. During the Compliance Audit, a metal plate was installed over the aperture, ending this instance of noncompliance.

The root cause of the noncompliance was an insufficient process for compliance with CIP-006-6 R1. Regarding, the [redacted] location, the root cause was that the Entity's personnel mistakenly believed that it was permitted for the keyboards and mice to extend beyond the PSP cabinets because of the controls required for the keyboards and mice to control the BCAs at issue. In addition, the locks for the cabinets at the [redacted] location had been wired to fail to an unlocked state, instead of failing to a secure state. Finally, the aperture on the [redacted] PSP had been intended for a fan to be installed but was unintentionally omitted.

This noncompliance started on July 1, 2016, when CIP-006-6 R1 became enforceable, and ended on July 1, 2019, when the new PSP for the [redacted] location was commissioned.

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. These instances could have allowed unauthorized physical access to the Entity's [redacted] BES Cyber System. The Entity's portfolio includes [redacted] although the Entity stated that [redacted]. At the start of the noncompliance, the BES Cyber System was identified as a Medium Impact BES Cyber System subject to CIP-006-6 R1, Part 1.2, but it became a High Impact BES Cyber System subject to Part 1.3 during the noncompliance.

However, the risk posed by this issue was reduced by the following factors. First, the Entity possessed other controls that reduced the impact posed by these issues. Regarding the [redacted] location, the Entity implemented monitoring and alarms that would have detected unauthorized access inside the cabinets, as well as security guards and badge readers to allow only corporate employees and contractors access to all corporate areas, including the [redacted] location. Further, although [redacted] of the Entity's employees who were not authorized had potential physical access to the keyboards and mice that extended beyond the PSP area, the keyboards were equipped with a card reader in order to function, which would have prevented unauthorized access to control the BCAs at issue. Regarding the backup Control Center location, the Compliance Audit noted that multiple layers of physical controls were used, including fencing, electronic gates, security guards, and badge or fingerprint readers, which reduced the possibility of unauthorized access. The aperture in the backup Control Center PSP was raised off the ground, and the Compliance Audit only indicated that the aperture permitted physical access to certain network cabling. Second, although the duration of the noncompliance was three years, the Entity began mitigating these issues shortly after they were discovered. The [redacted] location locks and backup Control Center location aperture were mitigated before the end of the Compliance Audit. Similarly, the Entity began the process of constructing a new PSP around the [redacted] BCAs at issue in November 2017. 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) constructed a new PSP for the [redacted] location;
2) prior to constructing the new PSP, corrected the locks for the cabinets at the [redacted] location and rewired them to remain locked in case of an equipment failure;
3) installed a metal plate to cover the aperture at the top of the [redacted] PSP; and
4) provided training regarding physical security controls.

Texas RE has verified the completion of all mitigation activity.

Texas Reliability Entity, Inc. (Texas RE) 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
TRE2017018672	CIP-010-2	R3; P3.1, P3.3	[redacted] (the "Entity")	[redacted]	7/1/2016	3/23/2018	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 from [redacted], Texas RE determined that the Entity, as a [redacted], was in noncompliance with CIP-010-2 R3. In particular, the Entity did not conduct a paper or active vulnerability assessment for each applicable BES Cyber System at least once every 15 calendar months, as required by Part 3.1, and did not perform an active vulnerability assessment of [redacted] new applicable Cyber Assets before adding them to a production environment, as required by Part 3.3. Regarding CIP-010-2 R3, Part 3.1, the Entity did not document vulnerability assessment results for [redacted] Cyber Assets located at [redacted] containing Medium Impact BES Cyber Systems when the Entity performed vulnerability assessments during February and March 2017. During February and March 2018, the Entity revised its documented vulnerability assessments to include the Cyber Assets at issue, ending the noncompliance. Regarding Part 3.3, on July 1, 2016 and on September 13, 2016, the Entity added [redacted] Cyber Assets to its Control Center production environment without first performing an active vulnerability assessment. On March 23, 2018, the Entity documented a subsequent active vulnerability assessment that included the Cyber Assets at issue, ending the noncompliance. The root cause of this issue is that the Entity did not have a sufficient process for compliance with CIP-010-2 R3. Regarding Part 3.1, different personnel managed the Cyber Assets at issue than the personnel who were responsible for documenting the vulnerability assessment, and the Entity's documented process and form did not clearly instruct personnel to address the omitted Cyber Assets. Regarding Part 3.3, the Entity's process did not make personnel aware of the requirement to complete an active vulnerability assessment before placing the Cyber Assets at issue into a production environment. This noncompliance started on July 1, 2016, when CIP-010-2 R3 became enforceable and also when the Entity added [redacted] Cyber Assets to its Control Center production environment without first performing an active vulnerability assessment, and ended on March 23, 2018, when the Entity completed the required paper or active vulnerability assessments for the Cyber 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. The risk posed by failing to perform a vulnerability assessment is that the Entity would not be aware of the vulnerabilities of a Cyber Asset in use in its production environment. The instance regarding CIP-010-2 R3, Part 3.1 affected [redacted] firewalls classified as Electronic Access Control and Monitoring Systems (EACMS) and [redacted] BES Cyber Assets located at [redacted] containing Medium Impact BES Cyber Systems. The instance regarding Part 3.3 affected [redacted] BES Cyber Assets, including [redacted] operator consoles, and [redacted] firewalls classified as EACMS, located at the Entity's primary Control Center, which is used to control the Entity's [redacted] and is associated with a High Impact BES Cyber System. However, the risk posed by this issue was reduced by the following factors. First, the Entity's [redacted]. The Entity's [redacted]. The Entity does not [redacted]. Second, regarding Part 3.1, the noncompliance appears to be, in part, a documentation issue. In particular, the Cyber Assets at issue were included in some portions of the Entity's vulnerability assessment, including the Entity's scan of open discovered ports, but those Cyber Assets were not listed on other portions of the Entity's vulnerability assessment documentation where, for example, password complexity was reviewed. When the required vulnerability assessments were documented, no issues were detected. Third, regarding Part 3.3, other controls reduced the risk posed this issue. In particular, during the period of noncompliance, the Entity did complete a paper vulnerability assessment, including reviews of network discovery scans and security configuration controls, which identified potential vulnerabilities for the Cyber Assets at issue. In addition, the Compliance Audit did not note any missed security patches for the Cyber Assets at issue. 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) revised the vulnerability assessments for [redacted] assets to include the previously omitted Cyber Assets; 2) performed an active vulnerability assessment for the Control Center Cyber Assets; 3) revised the Entity's written processes for conducting paper or active vulnerability assessments; and 4) created a recurring training requirement and provided training to applicable personnel. Texas RE has verified the completion of all mitigation activity.

FFT

Texas Reliability Entity, Inc. (Texas RE) CIP

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Mitigation Completion Date
TRE2018019173	CIP-007-6	R1; 1.1	[redacted] ("the Entity")	[redacted]	07/01/2016	01/16/2018	Compliance Audit	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	During a Compliance Audit conducted from [redacted], Texas RE determined the Entity, as a [redacted], was in noncompliance with CIP-007-6, R1. Specifically, the Entity did not enable only logically network accessible ports that have been determined to be needed for [redacted] sampled Cyber Assets, and did not document a business need for [redacted] sampled Cyber Assets. The root cause of the noncompliance was insufficient communication from the compliance specialist to the technology and transmission teams, and a lack of NERC CIP training for the technology team. This noncompliance started on July 1, 2016, when CIP-007-6, R1 became enforceable, and ended on January 16, 2018, when the Entity updated the list of ports with associated justifications.
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 failure to adequately document enabled ports has the potential to affect BPS reliability by providing an opportunity for the installation of unauthorized network traffic into an Electronic Security Perimeter (ESP) over a port that is not adequately monitored for malicious traffic. However, several factors limited the risk associated with this issue in the current circumstances. First, the Entity deployed methods to deter, detect, or prevent malicious code. Additionally, for some of the Cyber Assets, the Entity had a host-based firewall. Further, threat detection is running at every ESP perimeter. Finally, the Entity has a relatively [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) expanded its CIP-007-6 R1 ports and service worksheet to include a "justification" column to further detail the need for logical ports and services; 2) enabled only logically network accessible ports that have been determined to be needed; and 3) held trainings for all affected SMEs. Texas RE 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
WECC2018019934	CIP-010-2	R1: P1.1; P1.3; P1.4	[redacted]	[redacted]	7/1/2016	5/21/2018	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] determined that the entity, as a [redacted], was in potential noncompliance with CIP-010-2 R1 Parts 1 subpart 1.1.1, 1.3, and 1.4. Specifically, regarding Part 1.1, between, July 1, 2016 and March 15, 2018, the entity initiated a firmware upgrade on some of its Substation System Protection and Automation devices classified as BES Cyber Assets (BCAs). One version out of [redacted] of BCAs firmware (or .7%) and one version out of three versions of [redacted] classified as Electronic Access Control or Monitoring System (EACMS) firmware (or 33%) were left off the initial baseline but were recorded in a different engineering change management system [redacted] than the system originally used [redacted] to develop the baselines. A comparison of the entity's [redacted] systems uncovered a previously unidentified version of BCA firmware. All versions in production were approved and authorized when recorded in [redacted], but a single version was overlooked during development of the BCA baseline. The scope included [redacted] BCA and [redacted] EACMS. This issue began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on May 21, 2018 when the entity updated the baseline configurations to include the firmware, for a total of 690 days of noncompliance. Regarding Part 1.3, between July 1, 2016 and January 5, 2018, the entity had [redacted] firmware baseline configuration changes affecting [redacted] different BCA configuration baselines that were not updated within the required 30 calendar days after completion of the change. The scope included [redacted] BCAs associated with the Medium Impact BES Cyber System (MIBCS) located at [redacted] different substations, and [redacted] Protected Cyber Assets (PCAs) associated with [redacted] MIBCS at [redacted] substation. This issue began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on ended on May 21, 2018 when the entity updated the baseline configurations for the [redacted] firmware changes, for a total of 690 days of noncompliance. Regarding Part 1.4, the entity had eight occurrences of changes that lacked sufficient documentation or evidence of the review and verification of the impact to the CIP-005 and CIP-007 cyber security controls due to changes that deviated from the existing baselines. The scope included [redacted] Cyber Assets, including PCAs, EACMS, and Physical Access Control Systems (PACS), of which [redacted] were associated with MIBCS and [redacted] were associated with High Impact BES Cyber Systems (HIBCS). This issue began on July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on January 25, 2018 when the entity verified and documented that the required security controls were not affected, for a total of 574 days of noncompliance. The root cause of these issues was attributed to a manual process for updating baseline configuration documentation and a lack of management oversight to ensure infrequently performed tasks were executed accurately. Specifically, the sustainment of spreadsheet baselines was prone to human error and lacked data input validation.
Risk Assessment	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 these instance, the entity failed to develop baseline configurations which included the firmware where no independent operating system exits for [redacted] BCA and [redacted] EACMS as required by CIP-010-2 R1 Part 1.1; for a change that deviated from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the changes for [redacted] Cyber Assets, as required by CIP-010-2 R1 Part 1.3; and for a change that deviated from the existing baseline configuration, prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change, following the change verify the quired cyber security controls were not adversely affected, and document the results of the verification for [redacted] Cyber Assets, as required by CIP-010-2 R1 Part 1.4. Failing to have correct documented baselines could have resulted in a prolonged system restoration of the Cyber Assets had they needed to be restored or rolled back to a recommended and secured configuration. Additionally, the lack of baseline configuration information could have caused the entity to not know whether recommended security levels had been implemented on a Cyber Asset, whether changes to configurations were appropriate for the existing system state or whether changes would have an effect on other system protective measures. Lastly, failing to verify the CIP-005 and CIP-007 security controls that could possibly be affected before and after the changes could have resulted in inoperability issues with Cyber Assets hardware, software, and applications which could have affected the reliability and security of the BES. However, Part 1.1 was purely an administrative error between the engineering change management system and the CIP-010 R1 baseline development process documentation. Additionally, as compensation, the affected Cyber Assets had all other baseline configuration protective measures applied, were protected with electronic and physical access controls and monitor and were updated with the most recent firmware to ensure operational integrity and security. No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate these issues, the entity has: 1) updated and documented all baseline configurations for the affected Cyber Assets;

	2) verified and documented that the required security controls were not affected; 3) revised its CIP-010-2 R1 procedures to include additional controls (e.g., weekly check-ins, monthly certifications of changes with user aid checklist and monitoring whitelist); 4) trained personnel on the revised procedures; 5) implemented a Change Coordinator role and function for additional oversight of processes and monitoring; 6) implemented role-based training requirements to improve user awareness to combat attrition and role changes; 7) implemented a new control to monitor changes to the configuration baseline files (an email notification will be sent to the change coordinator anytime a change is made to a baseline file); 8) updated a form used by substation technicians that has a built-in drop-down list of approved firmware versions. This control will ensure that a firmware version that is not authorized, is not added to Cyber Assets; and 9) provided training on the updated form to all substation technicians; with follow-up training session to ensure awareness and support adoption of the new control. 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
WECC2016016680	CIP-007-3a	R:5; R5.2	[redacted]	[redacted]	2/15/2016	7/8/2016	Self-Report	Completed

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

On December 14, 2016, the entity submitted a Self-Report stating that, as [redacted], it was in noncompliance with CIP-007-3a R5.

Specifically, on July 8, 2016, during a review of the CVA of eight switches classified as CCAs, a vulnerability was identified. As part of this review, the results of the CVA scan showed a successful login with the default account and password combination. The default account was removed from the CCAs upon implementation, so the expected result was a login failure. However, the entity identified two configuration errors to the Access Control Server (ACS) classified as an Electronic Access Control and Monitoring System (EACMS). In the first error the ACS allowed access to the CCAs to [redacted] because the access policy that was applied to the CCAs was configured in a manner such that if a [redacted], it would continue instead of rejecting the access, and for the second error the ACS allowed access to the CCAs [redacted] because the wrong access policies were being applied to the CCAs. The CCAs were not in the correct "device type" that would allow the correct access policy to be applied. [redacted] These issues were localized to only the CCAs installed within the [redacted] This issue began on February 15, 2016 when access authentication controls should have been enforced and ended on July 8, 2016, when the entity corrected the authentication errors, for a total of 144 days of noncompliance.

The root cause of this issue was attributed to the entity not appropriately implementing its test procedures on the affected Cyber Assets as required by CIP-007-3a 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. In this instance, the entity failed to adequately implement its polity to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts as required by R5.2.

Such failures could have resulted in inoperability of Cyber Assets should a program, port, or software not be compatible between one or more assets that could lead to a loss of operating or monitoring within the Energy Management System; unauthorized access and exposure to critical systems with the entity's Control Centers with the intent to compromise, disrupt or misuse the entity's infrastructure; and access to switches by personnel within the ESP (authorized or unauthorized) could expose the entire configurations of these devices, thus providing topology, accounts, logging device access accounts, etc. exposing the entity's infrastructure details.

However, as compensation, the entity utilized two-factor authentication [redacted] to gain access to the ESP where the CCAs were located. [redacted] Additionally, the entity confirmed that no unauthorized access was gained to the CCAs in scope during the noncompliance. No harm is known to have occurred.

WECC determined that the entity's compliance history should not serve as a basis for applying a penalty. Due to the root cause, and timing of the entity's prior noncompliance, the current violation is not indicative of a systemic or programmatic issue.

Mitigation

To remediate and mitigate this violation, the entity has:

1) corrected the ACS rule on the CCAs in scope to [redacted], which included testing to ensure authentication was working as expected;
2) held a meeting as part of its internal compliance program with the personnel involved to determine cause and discuss lessons learned;
3) updated the [redacted]; and
4) modified its ACS test procedures to include testing of access to downstream devices using various passwords, including defaults and blank. This updated process will be used on all new installations to validate that no default or blank passwords exist prior to being put into production.

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
WECC2017017296	CIP-007-3a	R2: R2.1; R2.2	[redacted]	[redacted]	5/8/2016	3/23/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On DATE, the entity submitted a Self-Report stating that, as [redacted] it was in noncompliance with CIP-007-3a R2. Specifically, as part of the upgrade of its Energy Management System (EMS) supervisory control and data acquisition (SCADA) system, the entity added new Cyber Assets and upgraded existing Cyber Assets in its production environment. During the review and validation of documentation and evidence associated with the upgrade, and a subsequent Cyber Vulnerability Assessment (CVA), the entity identified for [redacted] of those Cyber Assets, that the ports and services were not correctly documented as part of their baseline configurations. The Cyber Assets were in both the primary and backup Control Centers. This issue began on May 8, 2016, when ports and services were not appropriately enabled or disabled on the Cyber Assets in scope and ended on March 23, 2017, when the entity appropriately accounted for the ports and services, for a total of 320 days of noncompliance. The root cause of this issue was attributed to the entity not appropriately implementing its test procedures on the affected Cyber Assets as required by CIP-007-3a 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. In this instance, the entity failed to enable only those ports and services required for normal and emergency operations and disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the ESP, as required by CIP-007-3a R2.1 and R2.2. Such failures could have resulted in inoperability of Cyber Assets should a program, port, or software not be compatible between one or more assets that could lead to a loss of operating or monitoring within the Energy Management System; unauthorized access and exposure to critical systems with the entity's Control Centers with the intent to compromise, disrupt or misuse the entity's infrastructure; and access to switches by personnel within the ESP (authorized or unauthorized) could expose the entire configurations of these devices, thus providing topology, accounts, logging device access accounts, etc. exposing the entity's infrastructure details. However, as compensation, the entity utilized two-factor authentication to a [redacted] to gain access to the ESP where the CCAs were located. The [redacted] Additionally, the entity confirmed that no unauthorized access was gained to the CCAs in scope during the noncompliance. No harm is known to have occurred. WECC determined that the entity's compliance history should not serve as a basis for applying a penalty. Due to the root cause, and timing of the entity's prior noncompliance, the current violation is not indicative of a systemic or programmatic issue.
Mitigation	To remediate and mitigate this violation, the entity has: 1) updated its baselines and ports and services documentation for the Cyber Assets in scope; 2) disabled or removed unnecessary ports on the Cyber Assets in scope; 3) updated its configuration management database to include applicable port changes to the Cyber Assets in scope; 4) identified all applicable Cyber Assets in its baseline configuration; 5) implemented a change control template to specifically address adding new device class and changing an existing device class; 6) created a visual add to help users spot the difference between the change workflows and to aid in choosing he correct one; and 7) conduced an in-depth Cyber Asset owner training focusing on all aspects of the Cyber Asset life cycle. 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
WECC2018019704	CIP-007-3a	R1:	[redacted]	[redacted]	5/8/2016	7/6/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On Date , the entity submitted a Self-Report stating that, as [redacted], it was in noncompliance with CIP-007-3a R1. On May 8, 2016, the entity did not appropriately implement its test procedures on the Cyber Assets identified in R5 (WECC2016016680) and R2 (WECC2017017296) noncompliance mentioned herein, ([redacted] total), to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter (ESP) did not adversely affect existing cyber security controls, as required by CIP-007-3a R1, which was the root cause of R5 and R2. On July 6, 2017, the entity completed validation testing, for a total of 425 days of noncompliance. The root cause of this issue was attributed to the entity utilized the wrong revision of its testing procedure. Specifically, the entity had a process document in place that included testing changes in a test environment for any existing devices. The entity also had a process for adding a new device. The entity used the add a new device process by accident instead of using the change to existing device process.
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 implement its test procedures when its added new Cyber Assets within the ESP to ensure they do not adversely affect existing cyber security controls, as required by CIP-007-3a R1. Such failures could have resulted in inoperability of Cyber Assets should a program, port, or software not be compatible between one or more assets that could lead to a loss of operating or monitoring within the Energy Management System; unauthorized access and exposure to critical systems with the entity's Control Centers with the intent to compromise, disrupt or misuse the entity's infrastructure; and access to switches by personnel within the ESP (authorized or unauthorized) could expose the entire configurations of these devices, thus providing topology, accounts, logging device access accounts, etc. exposing the entity's infrastructure details. However, as compensation, the entity utilized two-factor authentication to a jump host to gain access to the ESP where the CCAs were located. [redacted] Additionally, the entity confirmed that no unauthorized access was gained to the CCAs in scope during the noncompliance. No harm is known to have occurred. WECC determined that the entity's compliance history should not serve as a basis for applying a penalty. Due to the root cause, and timing of the entity's prior noncompliance, the current violation is not indicative of a systemic or programmatic issue.
Mitigation	To remediate and mitigate this violation, the entity has: 1) updated test process documentation to include the steps necessary to complete a change control processes for testing prior to a planned change to existing device(s) within the device class. This addresses existing devices and helps to mitigate CIP-007 in this instance and CIP-010-2 R1.4 and R1.5. There is also a process for new devices and when upgrading an existing device class, to confirm any substantial changes to the information in the change management database. The change control to add a new device class must be complete prior to adding the first device associated with that device class. This process also helps meet compliance for existing devices; 2) updated its test templates to include the required steps for testing new devices or changes to existing devices; 3) developed a change control template for new device class types; 4) held training with key business areas to kick off the updated processes; 5) added weekly change control meetings to it schedule to review and discuss change control templates for CIP Changes; and 6) upgrade its Energy Management System using the updated processes and templates. 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 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	RFC2018020074	Yes		Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
2	RFC2019021593	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
3	RFC2018019698	Yes		Yes	Yes		Yes				Yes			Category 1: 3 years; Category 2-12: 2 years
4	SERC2017018736	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
5	TRE2017018201	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
6	TRE2018019269	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
7	TRE2018019270	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 year
8	WECC2016016714			Yes	Yes					Yes				Category 2 – 12: 2 year
9	WECC2018020723			Yes	Yes					Yes				Category 2 – 12: 2 year
10	WECC2019022617			Yes	Yes					Yes				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
RFC2018020074	CIP-010-2	R1	[redacted]	[redacted]	10/30/2017	4/26/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On July 13, 2018, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-010-2 R1. The entity identified two separate occasions where it did not complete security controls testing on baseline configuration changes before implementing those changes. First, on October 30, 2017, a storage analyst submitted a change to update custom-developed scripts used for certain [redacted] transfers on four servers classified as Bulk Electric System Cyber Assets (BCA). The storage analyst performing the change indicated within the change request that the updates to the custom-developed scripts constituted a baseline configuration change to custom software. The identification of a baseline configuration change requires Security Controls Testing (SCT) to ensure changes to Cyber Assets will not unexpectedly impact the security of the system. The storage analyst correctly identified the need to perform SCT and added the appropriate SCT tasks to the change request, but the SCT tasks were not performed. The change was implemented in the production environment without conducting the required SCT pre-change scans and post-change scans to ensure the established security controls had not been adversely affected. The entity attributed the error to ineffective training and inadequate procedures. The entity did not perform the overdue SCT testing until April 26, 2018. Second, on April 25, 2018, a cyber-security engineer submitted a change request to [redacted] on two servers used as one of the entity's [redacted] systems which are [redacted] Similar to the first incident on October 30, 2017, the cyber security engineer correctly identified the need to perform SCT and added the appropriate tasks to the ticket, but the pre-change SCT tasks were not performed and the change was implemented in the production environment. Post-change SCT scans were conducted to ensure the security controls identified in CIP-005 and CIP-007 had not been adversely affected, and the entity performed a review of target systems baseline configuration scan taken from the previous day. The entity attributed the error to ineffective training and inadequate procedures. This noncompliance involves the management practices of workforce management, work management, and implementation. Workforce management is involved because entity employees were not properly trained to execute the internal process for change management. Implementation management is involved because the entity employees failed to execute internal processes while implementing system changes due to ineffective internal controls. The root cause of this noncompliance was an ineffective work procedure that resulted in the entity not performing SCT tasks before a change was implemented in the production environment. That poor work procedure is combined with ineffective training of entity employees tasked with performing SCT tasks. This noncompliance started on October 30, 2017, when the first instance began where the entity implemented the baseline configuration change without completing the required SCT, and ended on April 26, 2018, when the entity finished completing the post-change SCT scans on all impacted baseline configuration changes.
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 instance of noncompliance is that a change could be implemented that could have adversely affected system security and the BPS without having undergone security controls testing. This risk was mitigated in this case by the following factors. First, there were only two changes missed. Second, the entity maintained an effective security posture due to its defense-in-depth approach and production monitoring. The entity's configuration management process detects drifts from the known baseline for a particular CIP Cyber Asset and alerts the support teams for investigation, those drifts are tracked and monitored to ensure timely resolution, and those resolutions are documented. That process helped discover these missed changes, but did not discover the first instance because the security control testing scans were not properly executed in the first instance. ReliabilityFirst notes that subsequent testing and review performed by the entity confirmed that there were no adverse effects on security controls for either instance. No harm is known to have occurred. ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1) completed technical updates to the IT Service Management tool to centralize and enhance security controls testing processes; 2) updated procedural documentation, including process flow diagrams, procedures, and work-level instructions; and 3) developed and implemented education and training, ensuring all process participants have been educated on procedural changes implemented within IT Service Management tool. Since the first instance occurred in October 2017, the entity has made significant improvements to its configuration management process, including the implementation of a new [redacted] environment and automating the monitoring and alerting for configuration drifts. Because of this automation, a post-scan now occurs overnight, every day, outside of the SCT process. 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
RFC2019021593	CIP-010-2	R1	[redacted]	[redacted]	10/19/2018	10/19/2018	Self-Report	Completed

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

On May 21, 2019, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-010-2 R1. On October 19, 2018, the entity inadvertently patched 12 different [redacted] servers which were under CIP-scope. The change was part of an internal "patching initiative" which was planned, however, these specific servers were not intended to be patched on the day it occurred. The entity had patched roughly 85% of the platform, and the [redacted] servers which were inadvertently patched on October 19, 2018, were the remaining 15% which were scheduled to be patched by the end of November, 2018. While the 12 [redacted] servers were inadvertently patched on October 19, 2018, the servers were meant to have these patches implemented at a later date.

The inadvertent patching occurred at approximately 10:30 am. Later that day, at approximately 1:53 pm, the entity created an emergency change ticket to document what happened and to update the baseline based on the patch implementation. The inadvertent implementation occurred during a review of the patching initiative. Instead of using the reporting function to review what [redacted] servers had been patched, an entity employee inadvertently implemented the patching function, resulting in the noncompliance. The patching function was incorrectly applied to both the active and redundant database clusters which caused all database connections to fail until the servers were returned to service. [redacted]

The root cause of this noncompliance was a latent error in design in the patch management application which made it possible for an employee to accidentally initiate the patching function instead of the reporting function without a second confirmation step.

This noncompliance involves the management practices of asset and configuration management and implementation. Asset and configuration management is involved because the entity failed to properly implement a patch series resulting from an insufficient patch management tool. Implementation management is involved because the entity failed to properly execute a staged patch implementation plan due to an insufficient patch management tool.

This noncompliance started at 10:30 am on October 19, 2018, when the entity inadvertently implemented patching on 12 [redacted] servers and ended on October 19, 2018 at 1:53 pm, when the entity executed its emergency change ticket.

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 posed by failing to properly authorize a change here was that the change would be installed incorrectly, thus causing an operational outage. [redacted] The risk is partially reduced because the patches were tested, approved, and scheduled for implementation. The only issue is that an entity employee inadvertently implemented the patches before they were authorized to be implemented. Further reducing the risk, the patches had already been applied to approximately 85% of the scheduled devices already without issue. The entity promptly identified, assessed, and corrected this noncompliance. No harm is known to have occurred.

The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because while the result of the prior noncompliance was arguably similar, the prior noncompliance arose from a different cause.

Mitigation

To mitigate this noncompliance, the entity:

1) implemented a quick stop-gap to prevent reoccurrence;
2) reviewed the self-report with the CIP Senior Manager;
3) developed a long-term locking solution. [redacted]
4) implemented a long-term locking solution;
5) updated work level instructions and process documentation to reflect the locking solution;
6) developed a control to validate lock status; and
7) tested the control to validate lock status. The entity also created a quarterly report that shows that the systems are locked. The entity implemented a control to review the report on a periodic basis to ensure the feature is being used appropriately and to reduce the risk of reoccurrence.

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
RFC2018019698	CIP-005-5	R2	[redacted]	[redacted]	7/1/2016	4/17/2018	Compliance Audit	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	[redacted] ReliabilityFirst determined that the entity, [redacted], was in noncompliance with CIP-005-5 R2 identified during a Compliance Audit [redacted]. During the Compliance Audit, ReliabilityFirst reviewed the firewall configuration files utilizing NP-View. ReliabilityFirst noticed that a particular firewall group, consisting of two network hosts, permitted access using [redacted] and [redacted] directly into the Electronic Security Perimeter (ESP) without the use of an Intermediate System. Access requires the use of Interactive Remote Access; therefore, the entity should not have had firewall configurations that permit direct access into the ESP for [redacted] and [redacted] The root cause of this noncompliance was the entity's misunderstanding of the requirement. The entity mistakenly believed an Intermediate System was not required based on its network configuration. This root cause involves the management practice of workforce management, which includes providing training, awareness, and education to employees. This noncompliance started on July 1, 2016, when the entity was required to comply with CIP-005-5 R2 and ended on April 17, 2018, when the entity corrected the issue by changing its network configurations.
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 not utilizing an Intermediate System in this case was that it allowed devices to have direct access into the ESP, which introduces an additional attack vector. The risk is not minimal in this case based on the fact that the issue was identified at audit and the amount of time that the issue persisted. The risk is not serious in this case based on the following factors. First, this issue was present on only two network hosts, indicating that this was an isolated issue. Second, the two network hosts at issue were physically located in a secure area ([redacted] which protected them behind multifactor physical protection controls. Third, the two network hosts resided logically within a [redacted]. Therefore, even if they were compromised, an unauthorized individual would still need to bypass other security controls in place such as the entity's use of [redacted]. No harm is known to have occurred. ReliabilityFirst considered the entity's compliance history and determined there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity: 1) developed and implemented a better understanding of Interactive Remote Access to ensure that those with Interactive Remote Access to applicable Cyber Assets, understand the NERC glossary definition of Interactive Remote Access, how this term relates to CIP-005-5 R2, and what approach the entity must take to be in full compliance; and 2) developed and implemented change to Interactive Remote Access system currently in place to ensure that Interactive Remote Access does not allow for direct access to an applicable Cyber Asset in the set-up room or anywhere else. 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
SERC2017018736	CIP-010-2	R1, P1.2	[redacted]	[redacted]	07/01/2016	8/31/2019	Self-Report	Completed

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

On November 30, 2017, the Entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-010-2 R1, P1.4. SERC determined that this instance was more appropriately addressed under CIP-010-2 R1, P1.2. The Entity did not implement one or more documented process that included authorizing and documenting changes that deviated from the existing baseline configuration.

On August 7, 2017, an Entity manager conducted a post-work verification and discovered [redacted] protective relays that had actual configurations inconsistent with existing documented baseline configurations (Instance 1).

The Entity conducted an extent-of-condition assessment by reviewing [redacted] devices at [redacted] sites, which resulted in the identification of [redacted] additional protective relays with the same issue. Thus, a total of [redacted] relays were affected. [redacted]

On August 3, 2017 and August 17, 2017, during an annual documentation compliance review of all [redacted] the Entity discovered [redacted] switches that were classified as PCAs with [redacted] erroneously enabled, which was not consistent with the documented baseline configuration. Additionally, on November 4, 2017, during the same annual documentation compliance review, the Entity discovered [redacted] switches that were classified as PCAs with [redacted] service erroneously enabled, which was not consistent with the documented baseline configuration and not authorized.

On March 15, 2018, the Entity submitted a Scope Expansion (Instance 2). On December 14, 2017, while conducting commissioning activities at a construction site on a [redacted], the Entity identified another [redacted] at a different site that did not have an accurate documented baseline configuration record. A documented baseline record existed for the old version of the firmware, but not for the new version that was installed. The Entity did not properly tie the baseline record to the [redacted] being installed with the updated firmware version during commissioning.

The Entity conducted an extent-of-condition assessment by reviewing all assets deployed within its asset management system to confirm firmware versioning. The Entity identified [redacted] (one active and one inactive) that were commissioned without recording a baseline.

On September 5, 2018, the Entity submitted a Scope Expansion (Instance 3). On July 20, 2018, while reviewing baseline configurations for Cyber Assets involved with the first Scope Expansion, the Entity discovered inconsistencies between installed firmware for Cyber Assets and their associated baseline documentation records. The Entity had not recorded point release firmware versions as part of the baseline record.

This noncompliance started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on August 31, 2019, when the Entity completed it mitigation.

The cause of these instances of noncompliance was management oversight. Management failed to ensure that its configuration management process included a step to verify correct baseline configurations.

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's failure to authorize and document changes that deviated from the existing baseline configuration could have led to security administration errors decreasing cyber defenses and harming grid security. However, in all instances, the Cyber Assets did not have External Routable Connectivity or dial-up connectivity, and all Cyber Assets were placed within physically secure areas and Electronic Security Perimeters. Additionally, none of the instances involved a facility containing high impact BCSs. Furthermore, the Entity had malware detection, alerting and logging in place, and, the internal controls allowed for same day discovery of the problem, permitting a quick resolution. No harm is known to have occurred.

SERC determined that the Entity's CIP-010-2 R1 compliance history should not serve as a basis for aggravating any penalty. The prior instance of noncompliance was ten years ago and before a CIP program overhaul required by CIP Version 5, which does not demonstrate a programmatic failure.

Mitigation

To mitigate this noncompliance, the Entity:

1) modified the configuration documentation to clarify verification activities for the protective relays;
2) modified the configuration management process to include a step to validate configuration against baseline configuration documentation;
3) configured [redacted] per device baseline configuration documentation;

SERC Reliability Corporation (SERC) | FFT | CIP

	4) trained personnel on the updated configuration document; 5) upgraded [redacted] to an existing baseline; 6) performed an assessment to determine extent-of-condition; 7) reinforced CIP change management roles and processes via training; 8) determined the point release versions of firmware in scope of the issue; 9) provided awareness to affected personnel of the issue; and 10) identified and created needed BuildIDs to reestablish proper configuration for the devices.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
TRE2017018201	CIP-004-6	R4	[redacted] (the "Entity")	[redacted]	07/01/2016	09/06/2016	Compliance Audit	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	During a Compliance Audit per an existing multi-region registered entity agreement from [redacted], Texas RE determined that the Entity, as a [redacted] was in noncompliance with CIP-004-6 R4. Specifically, although CIP-004-6 R4, Part 4.1 required the Entity to implement a process to authorize access based on need, as determined by the Entity, as of August 25, 2016, there were [redacted] accounts for access to software that controls group policy settings for BES Cyber Assets at the Entity's Control Center and for which no documented approvals could be found. The root cause of the noncompliance was uncorrected legacy configurations upon conversion to a NERC CIP System that occurred one month prior to identifying the issue. This noncompliance started on July 1, 2016, when the Reliability Standard became enforceable, and ended on September 6, 2016, the date by which all [redacted] accounts had either been approved or revoked.
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 posed by this noncompliance arises from allowing multiple unauthorized individuals the ability to access software that controls access to BES Cyber Assets. Those unauthorized individuals could potentially compromise BES Cyber Assets and negatively affect the BPS. In particular, [redacted]. The Entity's portfolio includes a generating capacity of approximately [redacted]. However, the majority of the [redacted] accounts were approved after the Entity discovered the issue, most within a day of that discovery. 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) reviewed the need for the access to the accounts at issue, and revoked access for those accounts that did not need access; and 2) implemented quarterly access reviews to track, log, and to maintain the periodic reviews and related documentation. Texas RE has verified the completion of all mitigation activity.

Texas Reliability Entity, Inc. (Texas RE) 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
TRE2018019269	CIP-007-6	R2; R2.2; R2.3	[redacted] ("the Entity")	[redacted]	10/06/2016	12/13/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.	On February 24, 2018, the Entity submitted a Self-Report to Texas Reliability Entity, Inc. (Texas RE), under an existing Multi-Region Registered Entity (MRRE) agreement, stating that, as a [redacted], it was in noncompliance with CIP-007-6 R2. During a subsequent Compliance Audit conducted [redacted], additional evidence of the noncompliances was collected. Specifically, the Entity failed to implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-6, Table R2, Parts 2.2, and 2.3. On February 24, 2018, the Entity Self-Reported six separate instances where it had failed to evaluate security patches, in accordance with Table R2, Part 2.2, and/or apply the patches, in accordance with Table R2, Part 2.3. In the first two instances, a [redacted] update was not evaluated and the appropriate security patches were not applied, in accordance with Tables 2.2 and 2.3. These two instances of noncompliance ran concurrently, the longest of which occurred from October 6, 2016, until May 23, 2017. The third instance occurred when a security update was assessed as necessary for the [redacted] but not applied within 35 calendar days, in accordance with Part 2.3. The third instance occurred from March 23, 2017, until May 23, 2017. In the fourth and fifth instances, the Entity failed to recognize that an update for [redacted] was for the purpose of security, and failed to subsequently apply the security update. These two instances of noncompliance ran concurrently from September 11, 2017 until December 13, 2017. In the sixth instance, a newer version of [redacted] was assessed as a necessary security update, but was not applied within 35 calendar days, in accordance with Part 2.3. The sixth instance occurred from March 23, 2017, until November 4, 2017. The root cause of these instances of noncompliance was inadequate procedural controls. First, there was a lack of specificity in the procedure identifying the necessary activity after an evaluation occurs in accordance with Part 2.2. Second, there was insufficient peer and management review of each security patch evaluation conducted, and a lack of detail in the evidence maintained to show compliance with Part 2.3 and 2.3. These instances of noncompliance began on October 6, 2016, when the first instance of noncompliance occurred, and continued concurrently until December 13, 2017, when the last instance was mitigated.
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 to the BPS is that the Entity's failure to evaluate and install patches, in accordance with CIP-007-6 R2, Parts 2.2 and 2.3, could lead to network instability and vulnerabilities that would affect both the primary and backup Control Center. However, this risk is lessened by the fact that, although the Entity had not evaluated and/or applied patches for numerous Cyber Assets within the required timeframe in the six instances outlined by the Self-Report, the noncompliance was limited in scope as the auditors did not identify any additional instances of noncompliance. Further offsetting the risk is the fact that none of the Entity's [redacted] are contracted as Blackstart resources, and none are impacted by Remedial Action Scheme (RAS) operations. The size of this Entity supports the categorization of these noncompliances as moderate risk. [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) completed the required evaluations in accordance with Part 2.2, and installed the required patches in accordance with Part 2.3; 2) revised its security patch evaluation and management process to provide better instruction and guidance and to include peer and Compliance Coordinator review of patching process; 3) added steps to applicable procedures to require that details (Screenshots) of each patch assessment is attached to each change ticket to ensure that evidence of compliance is maintained; and 4) conducted a patching workshop to provide staff with additional training on reviewing and assessing patching protocols and data. Texas RE has verified the completion of all mitigation activity.

Texas Reliability Entity, Inc. (Texas RE) 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
TRE2018019270	CIP-010-2	R1	[redacted] ("the Entity")	[redacted]	07/01/2016	03/24/2018	Self-Report	Completed

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

On February 24, 2018, the Entity submitted a Self-Report to Texas Reliability Entity (Texas RE), under an existing Multi-Region Registered Entity (MRRE) agreement, stating that, as a [redacted] it was in noncompliance with CIP-010-2 R1. During a subsequent Compliance Audit conducted [redacted], additional instances of noncompliance with CIP-010-2 R1 were identified. Specifically, the Entity failed to implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-2, Table R1, Parts 1.1, 1.3 and 1.4.

Self-Report:
Part 1.3:
On February 24, 2018, the Entity Self-Reported four separate instances where it had failed to update the baseline configuration for Electronic Access Control or Monitoring System (EACMS) for Medium-Impact Bulk Electric System (BES) Cyber Assets (BCAs) within 30 days of the updates, in accordance with CIP-010-2 R1.3. On July 1, 2016, the operating system for the Entity's [redacted], an EACMS for a Medium-Impact BES Cyber System, was changed to a different feature release. This change occurred without commensurate documentation in the baseline-tracking document within 30 calendar days, as required by CIP-010-2 R1.3. The proper documentation occurred on September 16, 2016. This instance of noncompliance occurred for 77 days. The Entity further Self-Reported that, in separate instances, [redacted] electronic ports were opened on the [redacted], and [redacted] electronic ports were opened on the [redacted], both EACMS for Medium-Impact BES Cyber Systems, without commensurate documentation in the baseline-tracking document within 30 days of the port changes. Each instance was eventually properly documented, ending the noncompliance. These instances occurred from July 5, 2017 to August 5, 2017 (31 days), and June 5, 2017 to February 14, 2018 (8 months, and 9 days), respectively.

Compliance Audit:
Table R1, Part 1.1:
During a Compliance Audit subsequent to the Entity's Self-Report, Texas RE determined that the baseline for a [redacted] workstation, a Medium-Impact Cyber Asset, was not developed by July 1, 2016, as required by the Standard's Implementation Plan. This occurred due to a failure in the data collection functionality of the [redacted]. The failure in the tool was identified and corrected by the Entity, and the baseline was developed on July 6, 2016. This noncompliance occurred for 5 days.

Table R1, Part 1.3:
During the Compliance Audit, Texas RE also discovered an additional instance of noncompliance with Part 1.3. Texas RE determined that on November 27, 2016, a software update occurred on a [redacted] workstation, a Medium-Impact Cyber Asset, without the required update to the baseline within 30 calendar days. This instance also occurred due to a failure in the data collection functionality of the [redacted]. The failure in the tool was identified and corrected by the Entity, and the baseline was updated in accordance with CIP-010-2 R1, Table 1.3. The update to the Cyber Asset's baseline was due on December 27, 2016 and occurred on April 18, 2017. This noncompliance occurred for 3 months, and 22 days.

Table R1, Part 1.4:
During the Compliance Audit, Texas RE also determined that the Entity possessed a procedure for compliance with CIP-010-2 R1, but failed to maintain documentation to indicate compliance with the standard for any of their BCAs, as required in Table 1.4. The noncompliance began July 1, 2016, the effective date of the standard, and continued until March 24, 2018, when the Entity began attaching a document to change tickets to indicate that controls were verified in accordance with the standard. These instances of noncompliance occurred for 1 year, 8 months, and 23 days.

The root cause of these instances of noncompliance was inadequate procedural controls. First, there was a lack of specificity in the procedure regarding the version of software updates completed in the Entity's baseline tracking process. Second, there was a lack of software tools within the Entity's baseline tracking process that would scan for, and identify, open ports that are not accounted for in the Entity's baseline tracking spreadsheet.

The longest of the above instances of noncompliance began on July 1, 2016, when CIP-010-2 became effective and enforceable, and ended March 24, 2018, when the Entity began attaching a document to change tickets to indicate that controls were verified in accordance with Table 1.4.

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.

With regard to the Entity's noncompliances with CIP-010-2, Table 1.1 and 1.3, the potential harm to the reliability of the BPS that could derive from an Entity's failure to develop, or timely update, a baseline is that the Entity might rely on inaccurate information when conducting a reconciliation of baseline changes and that a BCA may not receive the appropriate updates. However, this risk is offset by the fact that the subject BCA received the appropriate updates, and that the noncompliance was limited to a failure in maintaining documentation to show compliance. Further mitigating

	the risk is the fact that, with regard to the Entity's noncompliances with CIP-010-2, Table 1.1 concerning the [redacted] workstation, the noncompliance lasted just 5 days, and affected only a single BCA at a Medium-Impact location. With regard to the Entity's noncompliance with CIP-010-2, Table 1.4, the risk to the BPS is that the Entity's failure to assess the security controls in CIP-005 and CIP-007, could lead to network instability and vulnerabilities that would affect both the primary and backup Control Center. However, this risk is lessened by the fact that the Entity provided evidence that it had a procedure in place during the period of noncompliance, but was unable to provide commensurate documentation for the security assessments conducted before the February 2018 patch cycle. The size of this Entity supports the categorization of these noncompliances as moderate risk. [redacted] Further offsetting the risks identified above is the fact that none of the Entity's [redacted] are contracted as Blackstart resources, and none are impacted by Remedial Action Scheme (RAS) operations. 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) developed and updated baselines to address noncompliances with Tables 1.1 and 1.3, and completed assessments for compliance with Table 1.4; 2) developed a tool to perform a comparison of the [redacted] scans run and the baseline list of approved ports to better identify deviations from the baseline of approved ports; 3) added steps to applicable procedures to verify that the version on the baseline documentation accurately reflects what is installed on the system, and for management review of change requests; and 4) revised the change request system to auto-generate sub-tasks for application updates. Texas RE 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
WECC2016016714	CIP-007-6	R2: P2.1; P2.2; P2.3	[redacted]	[redacted]	7/1/2016	4/12/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On December 8, 2016, the entity submitted a Self-Report stating, as a [redacted], it had a potential noncompliance with CIP-007-6 R2. Specifically, the entity had several issues during its implementation of CIP Version 5. Regarding R2 Part 2.1, the entity failed to identify patch sources associated with [redacted] software/firmware applications between July 1, 2016 and April 12, 2017. Regarding R2 Part 2.2, the entity failed to evaluate security patches on five separate occasions from [redacted] different sources for applicability at least once every 35 calendar days since the last evaluation between July 1, 2016 and October 26, 2016. Regarding R2 Part 2.3, the entity failed to either apply an applicable patch, create dated mitigation plan, or revise an existing mitigation plan, for [redacted] Cyber Assets between July 1, 2016 and January 24, 2017. The scope of these issues included [redacted] BES Cyber Assets, [redacted] Electronic Access Control or Monitoring Systems (EACMS), and [redacted] Protected Cyber Assets (PCAs) associated the High Impact BES Cyber System (HIBCS) located at the primary and backup Controls Centers. The aggregate of these issues began July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on April 12, 2017, when the entity evaluated all security patches for applicability, for a duration of 286 days (noncontiguous). The root cause was attributed to management not allocating enough resources and time to complete compliance with is transition to CIP Version 5. Specifically, the entity's management did not adequately monitory its transition to identity resource or implementation issues along the way.
Risk Assessment	These violations posed a moderate risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In these instances, for CIP-007-6, the entity failed 1) to identify patch sources associated with [redacted] software/firmware applications as required by R2 Part 2.1; 2) to evaluate security patches on five separate occasions from [redacted] different sources for applicability at least once every 35 calendar days since the last evaluation as required by R2 Part 2.2; and 3) to either apply an applicable patch, create dated mitigation plan, or revise an existing mitigation plan, for [redacted] Cyber Assets as required by R2 Part 2.3. The scope of these issues included [redacted] BES Cyber Assets, [redacted] EACMS, and [redacted] PCAs associated the HIBCS located in the primary and backup Controls Centers. These failures could have permitted vulnerabilities to remain unidentified, available, and open to exploit by malicious actors, who could potentially gain control over Cyber Assets and bulk power system facilities and adversely impact BES reliability. However, the Cyber Assets resided in a secure Electronic Security Perimeter, within a secured Physical Security Perimeter behind multiple layers of firewalls, anti-malware and monitory systems, two factor authentication for remote access and intrusion protection systems. No harm is known to have occurred. WECC determined that the entity's compliance history should not serve as a basis for applying a penalty because the previous relevant compliance history consisted of one minimal risk issue in 2011 and not indicative of a broader issue.
Mitigation	To remediate and mitigate this noncompliance, the entity has: 1) performed patch evaluations for the patch sources that had not been evaluated for the Cyber Assets in scope; 2) added the missing patch sources to the patch source list and begin patch assessment for those sources; 3) implemented the [redacted] Cyber Assets in scope into the patching process and began the patch assessment for those Cyber Assets; 4) created a revised tracking, reporting, and alerting process to provide better visibility and notice regarding the compliance deadlines; 5) ensured all instances of missing patch sources had been identified; 6) ensured all the BES Cyber Assets were included in the patching program; 7) identified and documented additional control(s) that resolved the root cause: a. development of scheduler tool to ensure tasks are created on a timely basis, the evaluation of standards are consistent, and multiple evaluators are assigned to provide redundancy, and continual improvement of that process; b. monitoring of patch management process via a SharePoint tool and continual improvement of that process; c. daily monitoring of software via its configuration management database which correlates to the identified patch source. As patches are implemented this monitoring ensures that all assets are upgraded, and all are patched to the same version; d. automated the manual baseline checks using its configuration management database; 8) identified and updated any CIP-007 review processes or procedures that needed updating based on new controls identified; 9) trained personnel to monitor for performance using the revised tracking, reporting, and alerting process; and

Western Electricity Coordinating Council (WECC)

	FFT	CIP
	10) performed formal training of personnel on identification of patch sources, patch assessment, mitigation, and installation processes. 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
WECC2018020723	CIP-010-2	R1: P1.1	[redacted]	[redacted]	7/1/2016	1/24/2017	Self-Report	Completed
Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			On November 21, 2018, the entity submitted a Self-Report stating, as a [redacted], it had a potential noncompliance with CIP-010-2 R1. Specifically, for [redacted] EACMS associated with the HIBCS located in the primary Control Center, the entity did not establish a system baseline configuration that satisfied the Part 1.1 sub-parts 1.1.1, 1.1.2, 1.1.3, and 1.1.4. This issue began on July1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on January 24, 2017, when the entity established a baseline configuration on [redacted] EACMS, for a duration of 208 days. The root cause was attributed to system interactions not considered or identified. Specifically, [redacted] EACMS [redacted] incorporated in the entity's CIP Version 5 implementation project; however, the role of [redacted] EACMS with regards to the other components of CIP were not understood, and the entity lacked internal controls and processes to detect the omission.				
Risk Assessment			WECC determined this violations 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 document a baseline configuration on [redacted] EACMS associated with the HIBCS that included sub-parts 1.1.1, 1.1.2, 1.1.3, and 1.1.4 as required by CIP-010-2 R1 Part 1.1. Such failure could have resulted in unauthorized system modifications to the HIBCS within the entity's Control Center which could have led to undetected malware infection or other successful intrusion into the network locations of the modified system. However, as compensation [redacted] EACMS [redacted] protected in an established demilitarization zone; had up to date anti-malware and security patches, was being monitored, and required authentication for interactive user access. No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.				
Mitigation			To remediate and mitigate this noncompliance, the entity has: 1) established a baseline configuration for [redacted] EACMS in scope; 2) updated its BES Cyber Asset on-board and change management procedure and templates to add check/review steps; and 3) updated its BES Cyber Asset inventory processes to improve the ability to detect BES Cyber Asset classification errors and improve oversight. This new process clarifies that the CIP Program Manager will create a BES Cyber Systems list and will send it to the CIP Senior Manager for approval, instead of a sending a Cyber Asset inventory list for approval. 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
WECC2019022617	CIP-010-2	R2: P2.1	[redacted]	[redacted]	8/6/2016	5/24/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On December 9, 2019, the entity submitted a Self-Report stating, as a [redacted], it had a potential noncompliance with CIP-010-2 R2. Specifically, on three separate occasions, the entity failed to monitor at least once every 35 calendar days for changes to the baseline configuration for [redacted] EACMS associated with the HIBCS located in the primary Control Center. The first occurrence began on August 6, 2016, when the Standard and Requirement became mandatory and enforceable and ended on January 24, 2017, when the entity updated the baseline configuration on [redacted] EACMS, for a duration of 172 days. The second occurrence began on March 1, 2017, 36 days after the previous monitoring and ended on April 12, 2017, when the entity updated the baseline configuration on [redacted] EACMS, for a duration of 43 days. The third occurrence began on May 18, 2017, 36 days after the previous monitoring and ended on May 24, 2017, when the entity updated the baseline configuration on [redacted] EACMS, for a duration of seven days. The root cause of these issues was attributed to system interactions not considered or identified. Specifically, [redacted] EACMS [redacted] incorporated in the entity's CIP Version 5 implementation project; however, the role of [redacted] EACMS with regards to the other components of CIP were not understood, and the entity lacked internal controls and processes to detect the omission.
Risk Assessment	WECC determined this violation 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 on three separate occasions to monitor at least once every 35 calendar days for changes to the baseline configuration for [redacted] EACMS associated with the HIBCS Such failure could have allowed changes to the baseline configuration to be undetected which could have exposed vulnerabilities or disruption to the entity's operations. However, as compensation [redacted] EACMS [redacted] protected in an established demilitarization zone; had up to date anti-malware and security patches, was being monitored, and required authentication for interactive user access. No harm is known to have occurred. WECC determined the entity had no prior relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the entity has: 1) implemented a programmatic, scheduled baseline configuration evaluation for [redacted] EACMS in scope. This implementation also addresses the entity's need to perform a baseline configuration evaluations on any irregularly powered-on Cyber Asset; 2) updated its BES Cyber Asset on-board and change management procedure and templates to add check/review steps; and 3) updated its BES Cyber Asset inventory processes to improve the ability to detect BES Cyber Asset classification errors and improve oversight. This new process clarifies that the CIP Program Manager will create a BES Cyber Systems list and will send it to the CIP Senior Manager for approval, instead of a sending a Cyber Asset inventory list for approval. 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	RFC2019021276	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
2	RFC2019021272	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
3	RFC2019021051	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2-12: 2 years
4	RFC2019021273	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 year
5	RFC2019021274	Yes	Yes	Yes	Yes		Yes		Yes					Category 1: 3 years; Category 2 – 12: 2 year
6	SERC2017018750	Yes	Yes	Yes	Yes				Yes				Yes	Category 1: 3 years; Category 2 – 12: 2 year
7	WECC2015015220	Yes		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
RFC2019021276	CIP-004-6	R4	[redacted]	[redacted]	2/1/2018	12/7/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On March 26, 2019, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-004-6 R4. On November 20, 2018, as a result of reviewing Cyber Vulnerability Assessment results on non-CIP devices, an entity employee discovered two fileshares containing Bulk Electric System Cyber System Information (BCSI) with read/write access set to "everyone" on two non-CIP devices (one fileshare per device). The data was part of a process to send CIP-010-2 R1 baseline data to a baseline management tool. This is an automated non-interactive process without any end-user involvement. One of the file share locations was designated as a BCSI repository/storage location, and the other one was not. Both fileshares did not have the proper permissions for BCSI required under CIP-004-6 R4. The root cause of this noncompliance was that the entity did not have a process in place to manage fileshares with BCSI resulting in a failure to appropriately restrict access to the fileshares. Secondarily, the entity did not perform any application structure reviews to assess the data flow of BCSI before the entity introduced the fileshares into the production environment. This noncompliance involves the management practices of workforce management and information management. Workforce management is involved because the entity failed to sufficiently train employees on the process to manage fileshares involving BCSI. Information management is involved because the entity failed to identify and assess BCSI. This noncompliance started on February 1, 2018, when the entity uploaded BCSI to the two impacted fileshares without proper permission restrictions and ended on December 7, 2018, when the entity corrected the permissions on the two fileshares.
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 this noncompliance is that unauthorized parties could potentially access BCSI which could in turn lead to alteration or misuse of the information. The risk is not minimal because of the long approximately ten month duration. The risk is minimized because the fileshares were stored on a restricted [redacted] Domain separate from the entity Corporate Domain with access limited to only [redacted] Staff via multi-factor authentication. Further minimizing the risk, the BCSI was part of a system-to-system process [redacted] which is an automated non-interactive process without any end-user involvement. (The entity concluded that there was no evidence that the fileshare data was known outside of the baseline management tool administrator who was authorized for BCSI access. Accessing the data requires multi-factor authentication.) 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 either different causes or involved different facts and circumstances.
Mitigation	To mitigate this noncompliance, the entity: 1) corrected the permissions on the two fileshare devices so that only individuals with approved NERC CIP Access would be able to have access. The entity also performed an extent of condition on all NERC CIP Asset fileshares to make sure that the permissions were restricted to individuals with approved NERC CIP access; 2) sent on a weekly basis, tasks to subject matter experts to remediate fileshares with "Everyone permissions". This weekly review will report any instance of a file share configured with "OPEN" permissions and requires the subject matter expert to remediate this level of access; 3) performed an extent of condition to review data protections of existing Bulk Electric System Cyber System Information (BCSI) repositories to identify unprotected data within the repositories. The entity will separately report any findings; 4) developed a policy regarding the creation of fileshares and reviewing permissions when such fileshares are set up; 5) implemented a new detective control to evaluate BCSI repositories on a quarterly basis to achieve the following: incorporate changes and verify accuracy of the BCSI repository inventory; ensure access permissions and data protections are in place for each BCSI repository; and communicate and raise awareness of BCSI repositories to end users. This control will examine the whole entity [redacted] environment to ensure BCSI data is properly protected; and 6) modified an existing preventative control to evaluate access permissions when commissioning new systems to verify that the systems containing BCSI have the proper access restrictions in place as part of the evaluation process.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021272	CIP-004-6	R4	[redacted]	[redacted]	2/1/2018	12/7/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On March 26, 2019, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-004-6 R4. [redacted] On November 20, 2018, as a result of reviewing Cyber Vulnerability Assessment results on non-CIP devices, an entity employee discovered two fileshares containing Bulk Electric System Cyber System Information (BCSI) with read/write access set to "everyone" on two non-CIP devices (one fileshare per device). The data was part of a process to send CIP-010-2 R1 baseline data to a baseline management tool. This is an automated non-interactive process without any end-user involvement. One of the file share locations was designated as a BCSI repository/storage location, and the other one was not. Both fileshares did not have the proper permissions for BCSI required under CIP-004-6 R4. The root cause of this noncompliance was that the entity did not have a process in place to manage fileshares with BCSI resulting in a failure to appropriately restrict access to the fileshares. Secondarily, the entity did not perform any application structure reviews to assess the data flow of BCSI before the entity introduced the fileshares into the production environment. This noncompliance involves the management practices of workforce management and information management. Workforce management is involved because the entity failed to sufficiently train employees on the process to manage fileshares involving BCSI. Information management is involved because the entity failed to identify and assess BCSI. This noncompliance started on February 1, 2018, when the entity uploaded BCSI to the two impacted fileshares without proper permission restrictions and ended on December 7, 2018, when the entity corrected the permissions on the two fileshares.
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 this noncompliance is that unauthorized parties could potentially access BCSI which could in turn lead to alteration or misuse of the information. The risk is not minimal because of the long approximately ten month duration. The risk is minimized because the fileshares were stored on a restricted [redacted] Domain separate from the entity Corporate Domain with access limited to only [redacted] Staff via multi-factor authentication. Further minimizing the risk, the BCSI was part of a system-to-system process [redacted] which is an automated non-interactive process without any end-user involvement. (The entity concluded that there was no evidence that the fileshare data was known outside of the baseline management tool administrator who was authorized for BCSI access. Accessing the data requires multi-factor authentication.) 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 either different causes or involved different facts and circumstances.
Mitigation	To mitigate this noncompliance, the entity: 1) corrected the permissions on the two fileshare devices so that only individuals with approved NERC CIP Access would be able to have access. The entity also performed an extent of condition on all NERC CIP Asset fileshares to make sure that the permissions were restricted to individuals with approved NERC CIP access; 2) sent on a weekly basis, tasks to subject matter experts to remediate fileshares with "Everyone permissions". This weekly review will report any instance of a file share configured with "OPEN" permissions and requires the subject matter expert to remediate this level of access; 3) performed an extent of condition to review data protections of existing Bulk Electric System Cyber System Information (BCSI) repositories to identify unprotected data within the repositories. The entity will separately report any findings; 4) developed a policy regarding the creation of fileshares and reviewing permissions when such fileshares are set up; 5) implemented a new detective control to evaluate BCSI repositories on a quarterly basis to achieve the following: incorporate changes and verify accuracy of the BCSI repository inventory; ensure access permissions and data protections are in place for each BCSI repository; and communicate and raise awareness of BCSI repositories to end users. This control will examine the whole entity [redacted] environment to ensure BCSI data is properly protected; and 6) modified an existing preventative control to evaluate access permissions when commissioning new systems to verify that the systems containing BCSI have the proper access restrictions in place as part of the evaluation process.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021051	CIP-011-2	R1	[redacted]	[redacted]	8/10/2016	4/13/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On January 30, 2019, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-011-2 R1. On April 12, 2018, an entity [redacted] analyst emailed a link to a "Confidential Special Handling: CIP" document to a director in the [redacted] Department. The director realized the two files, an [redacted] and a [redacted], were being stored on a SharePoint site that was not a Bulk Electric System (BES) Cyber System Information (BCSI) Repository and reported the potential incident the same day. The documents had been stored on this site since their initial posting on August 10, 2016. On April 13, 2018, the entity moved the documents to an area designated as a BCSI Repository. This noncompliance involves the management practices of workforce management and information management. The root cause is that an accessible, secure storage location was not readily available and easily known for this particular activity, and a list of BCSI locations was not routinely communicated as part of normal training activities. This noncompliance started on August 10, 2016, when the entity first posted the CIP files to a SharePoint site that was not a BCSI repository and ended on April 13, 2018, when the entity moved the files to a BCSI repository.
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 is that the content of these files could be used along with other access and information to gain unauthorized access to an Electronic Security Perimeter (ESP). The risk is not minimal because of the almost two year duration of this noncompliance. The risk is lessened because the files were stored on a [redacted] site. (Access from the corporate domain would require two-factor authentication and authorized access into the [redacted] domain.) Access to this site is controlled through [redacted] security and requested and approved through the entity's access management tool. Only individuals on the [redacted] access list could access the files. Of the two files posted, an [redacted] and a [redacted], the [redacted] file was password protected and only three employees had the password. [redacted]. Additionally, the entity's defense in depth model was in place protecting the BCSs/ESPs whose information was improperly stored during the time the files were posted and includes: (a) intrusion detection and prevention systems (IDS/IPS) monitoring of ESPs; (b) advanced monitoring intrusions from the external internet; (c) host IPS and antivirus protecting against potentially malicious software; (d) two-factor authentication is enabled which provides for stronger access controls; and (e) firewalls and other security tools securing the network perimeter. 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 either different causes or involved different facts and circumstances.
Mitigation	To mitigate this noncompliance, the entity: 1) moved the documents to a designated BES Cyber System Information (BCSI) Repository; 2) required the employee involved to take additional Information Protection Training in addition to the yearly NERC CIP training; 3) performed an extent of condition review to review documents that are Confidential Special Handling and Confidential Special Handling: CIP to ensure that they are stored in BCSI repositories within entity [redacted]; 4) added an [redacted] technical Preventive Control preventing BCSI documentation from being transferred outside of the entity by email or by using a USB drive. The control is managed by the entity's [redacted] team. When a user plugs in any removable media to an entity user's laptop or computer, a scan is performed of the removable media. If any files contain a classification of "Confidential Special Handling: CIP" a warning is presented to the user saying "You are attempting to copy NERC CIP data to removable storage" and the user must attest the contents are being transferred to an approved encrypted storage device or the transfer action is cancelled. For emails being sent outside of the entity email domain, if the email content contains a classification of "Confidential Special Handling: CIP" and the email is not encrypted, then the email is deleted at the email gateway perimeter and a message is sent to the sender that the email was blocked. 5) implemented a new detective control to evaluate BCSI repositories and BCSI (labeled as "Confidential Special Handing: CIP" or "Confidential Special Handling") that exist outside of designated BCSI repositories on a quarterly basis to achieve the following: (i) Incorporate changes and verify accuracy of the BCSI repository inventory; and (ii) ensure entity Confidential Special Handling: CIP documents are places in a BCSI repository. This control will examine the whole entity [redacted] environment to ensure BCSI data is properly protected; and 6) improved awareness of [redacted] BCSI repositories and associated protective measures through the following actions: (i) [redacted] Operations Compliance personnel will provide repository updates and best practices real-time during key [redacted] meetings (all-hands meetings, quarterly staff/leads meetings, quarterly safety meetings, etc.); and (ii) Distribution of BCSI repository updates and protective measures on a periodic basis to [redacted] personnel and users with access to [redacted] BCSI repositories.

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
RFC2019021273	CIP-011-2	R1	[redacted]	[redacted]	2/1/2018	12/7/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On March 26, 2019, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-011-2 R1. [redacted] On November 20, 2018, as a result of reviewing Cyber Vulnerability Assessment (CVA) results on non-CIP devices, an entity employee discovered two fileshares containing Bulk Electric System (BES) Cyber System Information (BCSI) with read/write access set to "everyone" on two non-CIP devices (one fileshare per device). The data was part of a process to send CIP-010-2 R1 baseline data to a baseline management tool. This is an automated non-interactive process without any end-user involvement. This incident had been occurring since February 1, 2018 based on the date of timestamps of the files in the two fileshares. The entity failed to adhere to its NERC CIP Information Protection Program and did not "protect and secure handle BES Cyber System Information, including storage, transit, and use". This noncompliance involves the management practices of asset and configuration management, work management, and information management. The root cause of this incident was that no procedures were in place to ensure the fileshares with BCSI were appropriately restricted when the application was developed and the file shares were created. There were also no application architectures reviews completed that considered the data flows of BCSI before the application was introduced into production. This noncompliance started on February 1, 2018, when the entity first had two fileshares containing BCSI with read/write access set to "everyone" on two non-CIP devices (one fileshare per device) and ended on December 7, 2018, when the permissions on the two devices were corrected.
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 this noncompliance is that the content of these files could be used along with other access and information to harm BES Cyber Assets. The risk is not minimal because of the long approximately ten month duration. The risk is lessened because the fileshares existed on a restricted [redacted] domain that is separate from the entity corporate domain with access limited to entity [redacted] personnel. Access from the corporate domain would require two-factor authentication and authorized access into the [redacted] domain. [redacted] The entity confirmed that there is no evidence the fileshare data was known outside of the baseline management tool administrator who was authorized for BCSI access. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances arose from either different causes or involved different facts and circumstances.
Mitigation	To mitigate this noncompliance, the entity: 1) corrected the permissions on the two fileshare devices so that only individuals with approved NERC CIP Access would be able to have access. An extent of condition was performed on all NERC CIP Asset fileshares to make sure that the permissions were restricted to individuals with approved NERC CIP access 2) sent tasks on a weekly basis to subject matter experts to remediate fileshares with "Everyone permissions". This control is a weekly review of a [redacted] scan that reports any instance of a file share configured with "OPEN" permissions and requires the subject matter expert to remediate this level of access. There are file shares that allow "OPEN" permissions meaning these access permissions have been set to "Everyone" instead to designating proper access for those who need it; 3) performed an extent of condition review to review data protections of existing BCSI repositories within the entity [redacted] to identify unprotected data within those repositories; 4) developed a policy regarding the creation of fileshares and reviewing permissions when such fileshares are set up; 5) implemented a new detective control to evaluate BCSI repositories on a quarterly basis to achieve the following: (i) Incorporate changes and verify accuracy of the BCSI repository inventory; (ii) Ensure access permissions and data protections are place for each BCSI repository; and (iii) Communicate and raise awareness of BCSI repositories to end users. This control will examine the whole entity [redacted] environment to ensure BCSI data is properly protected; and 6) modified an existing preventative control to evaluate BCSI data when commissioning new systems. This control will be modified to verify that any destinations for BCSI data leaving the system are also properly protected. This control will prevent future occurrences of BCSI data being passed to unprotected destinations.

NERC Violation ID	Reliability Standard	Req.	Entity Name	NCR ID	Noncompliance Start Date	Noncompliance End Date	Method of Discovery	Future Expected Mitigation Completion Date
RFC2019021274	CIP-011-2	R1	[redacted]	[redacted]	2/1/2018	12/7/2018	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed noncompliance.)	On March 26, 2019, the entity submitted a Self-Report stating that, [redacted] it was in noncompliance with CIP-011-2 R1. On November 20, 2018, as a result of reviewing Cyber Vulnerability Assessment (CVA) results on non-CIP devices, an entity employee discovered two fileshares containing Bulk Electric System (BES) Cyber System Information (BCSI) with read/write access set to "everyone" on two non-CIP devices (one fileshare per device). The data was part of a process to send CIP-010-2 R1 baseline data to a baseline management tool. This is an automated non-interactive process without any end-user involvement. This incident had been occurring since February 1, 2018 based on the date of timestamps of the files in the two fileshares. The entity failed to adhere to its NERC CIP Information Protection Program and did not "protect and secure handle BES Cyber System Information, including storage, transit, and use". This noncompliance involves the management practices of asset and configuration management, work management, and information management. The root cause of this incident was that no procedures were in place to ensure the fileshares with BCSI were appropriately restricted when the application was developed and the file shares were created. There were also no application architectures reviews completed that considered the data flows of BCSI before the application was introduced into production. This noncompliance started on February 1, 2018, when the entity first had two fileshares containing BCSI with read/write access set to "everyone" on two non-CIP devices (one fileshare per device) and ended on December 7, 2018, when the permissions on the two devices were corrected.
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 this noncompliance is that the content of these files could be used along with other access and information to harm BES Cyber Assets. The risk is not minimal because of the long approximately ten month duration. The risk is lessened because the fileshares existed on a restricted [redacted] domain that is separate from the entity corporate domain with access limited to entity [redacted] personnel. Access from the corporate domain would require two-factor authentication and authorized access into the [redacted] domain. [redacted] The entity confirmed that there is no evidence the fileshare data was known outside of the baseline management tool administrator who was authorized for BCSI access. No harm is known to have occurred. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history should not serve as a basis for applying a penalty because the prior noncompliances arose from either different causes or involved different facts and circumstances.
Mitigation	To mitigate this noncompliance, the entity: 1) corrected the permissions on the two fileshare devices so that only individuals with approved NERC CIP Access would be able to have access. An extent of condition was performed on all NERC CIP Asset fileshares to make sure that the permissions were restricted to individuals with approved NERC CIP access 2) sent tasks on a weekly basis to subject matter experts to remediate fileshares with "Everyone permissions". This control is a weekly review of a [redacted] scan that reports any instance of a file share configured with "OPEN" permissions and requires the subject matter expert to remediate this level of access. There are file shares that allow "OPEN" permissions meaning these access permissions have been set to "Everyone" instead to designating proper access for those who need it; 3) performed an extent of condition review to review data protections of existing BCSI repositories within the entity [redacted] to identify unprotected data within those repositories; 4) developed a policy regarding the creation of fileshares and reviewing permissions when such fileshares are set up; 5) implemented a new detective control to evaluate BCSI repositories on a quarterly basis to achieve the following: (i) Incorporate changes and verify accuracy of the BCSI repository inventory; (ii) Ensure access permissions and data protections are place for each BCSI repository; and (iii) Communicate and raise awareness of BCSI repositories to end users. This control will examine the whole entity [redacted] environment to ensure BCSI data is properly protected; and 6) modified an existing preventative control to evaluate BCSI data when commissioning new systems. This control will be modified to verify that any destinations for BCSI data leaving the system are also properly protected. This control will prevent future occurrences of BCSI data being passed to unprotected destinations.

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
SPP2017018750	CIP-005-5	R1, P1.5	[redacted]	[redacted]	07/01/2016	11/30/2017	Self-Report	Completed

Description of the Noncompliance (For purposes of this document, each noncompliance at issue is described as a "noncompliance," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On December 11, 2017, the Entity submitted a Self-Report stating that, as a [redacted], it was in noncompliance with CIP-005-5 R1, P1.5. The Entity failed to implement one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. There were two additional Self-Reports filed on February 6, 2017 [redacted] and October 6, 2017 [redacted]. Both instances involved deficiencies to the Entity's [redacted] and were related to this instant noncompliance. Both instances were dismissed and consolidated with this initial Self-Report as an expansion of scope. The first instance was discovered on October 10, 2016. The Entity installed a new firewall on October 5, 2016 and unintentionally disabled the primary [redacted] provided by the [redacted] Firewall. The Entity brought the device back online immediately upon identification, which was 5 days later. The second instance was discovered on September 7, 2017, during preliminary activities for the installation of an [redacted] upgrade. [redacted]. The duration of this second instance was 433 days. The third instance was discovered on November 16, 2017, which occurred during the same system upgrade identified in the second instance. When Entity's [redacted] changed out the [redacted] at the [redacted], the Analyst reviewed the weekly log, which revealed logging of traffic from and to the [redacted] monitoring device. The Analyst found that the [redacted] monitoring device installed on September 7, 2017 had been misconfigured, and that the traffic that appeared on the weekly log reports was only from the switch port in which the [redacted] plugged in and not all of the switch ports. The configuration of the [redacted] device is mostly a centrally-managed configuration, but there are a few local settings that the Entity must configure on the device for complete monitoring. Although the replacement monitoring device received the same mostly central-managed configuration as the device it replaced, the Entity did not configure the local setting of the device. The duration of this instance was 70 days. This noncompliance started on July 1, 2016, when the Standard became enforceable and the Entity had not configured the core switch properly for the second instance, and ended on November 30, 2017, when the Entity corrected the configuration of the [redacted] device for the third instance. There were several causes of this noncompliance. First, a technician failed to correctly identify the newly installed firewall device from the backside and unintentionally powered down the primary [redacted] device. The technician was installing a new firewall directly below the primary [redacted] due to a limited amount of rack space in the data center racks. Both devices are visually identical from the front and the technician had to circle the racks in order to turn the power on to the new firewall. However, when the technician got to the power source, he unintentionally powered down the primary [redacted] device as it protruded enough to block sight of the new firewall device (instance 1). Second, a technician failed to properly configure the disaster recovery core switch designated [redacted] port because of limited configuration procedures (instance 2). Third, a technician failed to verify the configuration during a system upgrade because of improper validation test procedures that involved quantitative rather than qualitative log review procedures (instance 3).
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's failure to implement one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications would have allowed unauthorized communication to occur undetected leading to potential compromise of BES Cyber Systems impacting the BPS. The risk was reduced in the first instance as the Entity's likelihood of noticing the intrusion would have been limited to a 5-day window. The Entity performs a mandatory check of the logs every week per its policies, however, in practice, the Entity's team is looking at those logs on an almost daily basis. The risk was reduced in the second and third instance as the Entity's switch and [redacted] misconfiguration was limited to the disaster recovery [redacted]. Furthermore, the Entity practices defense in depth (i.e., a layered security approach), and has event correlation tools using multiple log sources. The Entity's correlated [redacted] log sources would likely have identified any event that was not detected by the [redacted] due to the misconfiguration. The Entity protects its Cyber Assets through multiple layers of defense [redacted]. Additionally, all Entity Cyber Assets had up-to-date anti-malware software running during the time of this issue. No harm is known to have occurred. SERC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.
Mitigation	To mitigate this noncompliance, the Entity: 1) brought the primary [redacted] device back online (instance 1); 2) performed a review of the IP addresses that requested access to the CIP environment for the 5-day time period that the [redacted] was disabled and observed no suspicious or unexpected traffic connections in the logs reviewed (instance 1); 3) received approval of the board to pursue construction of a separate facility to address the limited rack space (instance 1); 4) applied adhesive labels to the front and back of the CIP devices (instance 1);

SERC Reliability Corporation (SERC) | FFT | CIP

	5) included the activation of a silent alarm [redacted] 6) corrected the misconfigurations under an emergency change (instance 2 and 3); 7) modified the device configuration procedures to specify configuration steps to enable the [redacted] monitoring over spanned ports (instance 2); 8) added [redacted] validation to the weekly log review to ensure the [redacted] remains correctly configured and verify each [redacted] is receiving current data from the generator control center environment (instance 3); 9) modified the weekly log review procedures to ensure direct traffic to the [redacted] device is filtered out of the review ensuring correct logging does not go unnoticed again (instance 3); 10) reviewed the revised procedures with all [redacted] during a Lessons Learned Meeting held on November 20, 2017 (instance 2 and 3).

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
WECC2015015220	CIP-005-3	R2: R2.1; R2.4	[redacted]	[redacted]	1/1/2011	12/21/2017	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 [redacted], WECC determined the entity, as a [redacted], had a potential noncompliance with CIP-005-3 R2.1 and R2.4. Specifically, during the configuration review of [redacted] Electronic Access Points (EAPs) the auditors found several access rules which were configured to allow any IP traffic from specific critical networks to any other network on the EAP, including identified ESPs. These rules superseded other explicit and implicit "deny all" rules applied on the specific critical network interfaces and as required by CIP-005-3 R2.1 did not provide the required explicit access permissions.

Additionally, where external interactive access into an ESP had been enabled, the entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party as required by CIP-005-3 R2.4. Specifically, the entity demonstrated strong technical controls for authenticating into the ESP while outside of the entity's networks. However, it did not include workstations connecting from within the entity's non-ESP networks. Instead, the entity mistakenly considered its use of a common access card to access its Physical Security Perimeters (PSPs) as one factor for ensuring authenticity of accessing party into the ESP and the login credentials of said party as a second factor, during external interactive access. The root cause of this issue was attributed to the entity not consulting with all departments involved in the task to ensure compliance prior to configuring the firewall rules, as well as an alternative implementation of its technical controls to its PSP access points rather than ESP access points.

These issues began on January 1, 2011, when the entity should have implemented explicit access permissions to the ESP at all EAPs and ended on December 21, 2017, when the entity completed mitigating activities, for a total of 2,547 days of noncompliance.

Risk Assessment

WECC determined this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In the first instance, for [redacted] EAPs, the entity failed to include in its processes and mechanisms, the use of an access control model that denied access by default, such that explicit access permissions must be specified as required by CIP-005-3 R2.1, and in the second instance, failed to implement strong procedural or technical controls at the EAPs to ensure authenticity of the accessing party where external interactive access into six ESPs had been enabled as required by CIP-005-3 R2.4.

The failure of R2.1 could have provided paths into the ESP that could have been exploited to gain unauthorized access and the failure of R2.4 could have provided attackers with additional vectors to gain unauthorized access. However, WECC confirmed, the entity provided adequate controls for network segmentation and an applicable access control list for each protected network at the affected ESPs, via a [redacted] that was placed in front of the [redacted]. Specifically, the entity asserted it had implemented VLAN segmentation controls such as vendor best-practices that were followed for the configuration of all [redacted] to resist VLAN hopping including; [redacted], [redacted], and having [redacted], which disables VLAN tagging. Nevertheless, no harm is known to have occurred.

The entity has no relevant prior compliance history with this or similar Standards and Requirements.

Mitigation

To mitigate R2.1 of this violation, the entity has:

1. changed the access list rules on the two access points in scope of R2.1;
2. removed the firewall rules that allowed workstations to access systems directly; and
3. reviewed final network design with Compliance to ensure all applicable requirements are being met and have sufficient documentation.

To mitigate R2.4 of this violation, the entity has:

1. implemented a jump server cluster which serves as Electronic Access Control or Monitoring System that requires dual-factor authentication for access to interactive remote access to the CCAs in the ESPs in scope. Workstations in the PSP but outside the ESP will no longer have access to CCAs in the ESP without first authenticating through the jump server; and
2. provided a Reliability Compliance Manager for addressing concerns with interpretation of Standards and Requirements, as well as attending compliance workshops and providing regular training to its subject matter experts.