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 Spreadsheet Notices of Penalty 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	TRE2018019425	Yes		Yes	Yes	Yes	Yes			Yes				Category 1: 3 years; Category 2 – 12: 2 years
2	TRE2017018017	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
3	TRE2017018012	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
4	TRE2017017934	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
5	TRE2017017935	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
6	WECC2018020557	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
TRE2018019425	CIP-002-5.1	R1	High	Lower	7/1/2016	12/26/2018	Self-Report	3/14/2019	2/25/2020

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

On March 21, 2018, the Entity submitted a Self-Report stating that, as a [redacted] it was in violation of CIP-002-5.1a R1. Specifically, the Entity failed to implement a process that considered the assets of its [redacted] and identified each of the medium impact Bulk Electric System (BES) Cyber Systems (BCS) according to Attachment 1, Section 1.

In 2013, the Entity engaged in efforts to [redacted] such that the systems were not connected in a manner that could adversely impact [redacted] These efforts were reviewed by a third-party contractor in 2015. These systems were considered by the Entity as Low Impact according to Attachment 1, Section 1. In 2017, the Entity engaged another third-party to conduct an independent study that included the [redacted] communication networks and associated BCS. The third-party identified items of concern that challenged the Low impact rating at [redacted] Upon completion of the 2017 assessment, the Entity began its own investigation and identified two avenues by which [redacted] The Entity then Self-Reported the noncompliance.

[redacted]
The first avenue was via [redacted] whereby [redacted] at the [redacted] Under these circumstances, the Entity's classification of its [redacted] as a low impact BCS was erroneous because, if the [redacted]

[redacted]
The second avenue was via the [redacted] Under normal conditions station output from [redacted] However, in the event that [redacted] Under these circumstances, the Entity's classification of the associated [redacted] as a low impact BCS was erroneous because, if the [redacted] It was determined that the [redacted] and therefore the [redacted] at that Facility was also erroneously classified as low impact.

The root cause of this noncompliance was the Entity's failure to adequately follow its own plan to [redacted] Specifically, the Entity failed to identify certain avenues whereby [redacted] Because the Entity failed to recognize these avenues, it failed to either appropriately designate [redacted] as Medium Impact and apply the appropriate security measures under the applicable Standards, or alternatively, properly implement its plan to [redacted]

This noncompliance began on July 1, 2016, the date CIP-002-5.1a became mandatory and enforceable, and ended on December 26, 2018, when the Entity completed initial and periodic CIP security requirements necessary for compliance.

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 failure to adequately protect the security of applicable BCS and associated Cyber Assets at [redacted] according to their Medium Impact classification could have resulted in the loss of those [redacted], which poses a risk to the reliability of the bulk power system.

In evaluating the risk posed by this issue, Texas RE considered that the Entity is [redacted] The risk associated with this noncompliance existed for 2 years, 6 months.

However, the risk identified above is mitigated by the fact that the Entity periodically engaged a third party to perform an independent assessment of its [redacted] and to identify any unknown changes that had occurred that could have impacted its [redacted] efforts and low impact ratings. In fact, this noncompliance was discovered during one such assessment conducted by a second, third-party vendor.

	Additionally, the [redacted] to these particular Cyber Assets. Given the [redacted], an individual had to be physically present [redacted] in order to compromise the [redacted]. To prevent such physical access, the Entity protected the [redacted] through [redacted], as well as limited physical access to those facilities to authorized personnel. In addition, the Entity had physical access revocation procedures in place throughout the issue duration. The Entity also implemented a process to [redacted] Texas RE also considered the fact that even if remote access to the [redacted] the Entity had additional, layered controls in place to reduce risk of a cyber-intrusion into the [redacted] First, the [redacted] which was [redacted] to the [redacted] were controlled by local login access only. Second, although the [redacted] (again only [redacted] to the [redacted] was [redacted], the Entity had implemented a number of cyber and physical security controls for that [redacted]. These controls are detailed in the "Other Factors" section below. Finally, the Entity's [redacted] was already appropriately categorized as High Impact and observed the applicable NERC Reliability Standards there.
Mitigation	To mitigate this violation, the Entity: • reclassified its [redacted] as a Medium Impact BCS; • documented its Cyber Assets at its Medium Impact BCS [redacted] • developed a comprehensive evaluation methodology for categorization of its low/medium/high impact BCS; • completed initial periodic requirements for its Medium Impact BCS [redacted] in accordance with CIP-007-6 R2.3 and CIP-010-2 R3.2; and • revised its [redacted] to follow the third party's 2017 assessment to ensure that [redacted] at other Facilities achieves the desired result. Texas RE has verified the completion of all mitigation activity.
Other Factors	Texas RE reviewed the Entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The Entity appears to have a strong ICP, with accompanying program documents and documented policies that are easily accessible by employees. The Entity's Regulatory Compliance Program includes monitoring and auditing, training, and remediation. As noted above, the [redacted] and was [redacted] Nevertheless, during the noncompliance period, the Entity implemented various activities and controls that reduced the risk of a threat actor [redacted], which further reduced the possibility of an intrusion into the [redacted] at either resource. These activities and controls included: • Implementing a cybersecurity plan that addresses all required topics, including training (CIP-003-6 R1, Part 1.1); • Implementing a corporate-wide cyber security awareness program that included [redacted] • Maintaining physical access controls to limit access to [redacted] • Performing patching activities on the [redacted] systems during scheduled outages; and • Maintaining a Cyber Security Incident Response Plan applicable to all High, Medium, and Low Impact BES Cyber Systems (CIP-008-5 R1); In addition to these activities, the Entity implemented the following specific protections for its [redacted] • Implementing a cybersecurity policy that addressed electronic access controls per CIP-003-6, Attachment 1. • Completing background checks and I9 identity verification within the last seven years as part of the new hire process for 55% of regular employees; • [redacted] • Restricting network access to systems and limited [redacted] • Installation of [redacted] • Configuring assets to log the required events per CIP-007-6 R4, Part 4.1 and providing such logs to [redacted] • Implementing authentication of interactive user access, and using password authentication, as required by CIP-007-6 R5, Part 5.1, for at least some cyber assets; • Implementing and enforcing password complexity rules that required [redacted] through either [redacted] where available or through manual configurations; • Maintaining a weekly backup schedule, policy, and procedure (CIP-009-6 R1, Part 1.3); and • Implementing a procedure for managing operational risk that requires communication and approval for changes performed [redacted] when there is potential for impact to production.

	Texas RE determined that the complexity of the issues involved in this matter, as well as the size of the facilities at issue, warranted disposition through a formal Spreadsheet Notice of Penalty instead of through the streamlined Find, Fix, Track, and Report (FFT) process. However, Texas RE determined a zero dollar penalty was appropriate based on a number of factors, including the Entity's effective compliance program, history as a Self-logging Program Participant, history of self-reporting, cooperation history, agreement to settlement, and lack of aggravating compliance history, including no prior history of serious risk violations. Texas RE also considered that [redacted] is an ERO endorsed approach and the Entity's activities were consistent with efforts to reduce overall risk on the system. Texas RE further considered that in performing these [redacted] activities, the Entity demonstrated good faith and cooperation in meeting with Texas RE on multiple occasions to discuss its [redacted] efforts. The Entity also performed the specific Engineering studies that ultimately determined that its [redacted] efforts were not fully successful. Once the Entity identified these issues through these efforts, the Entity self-reported appropriately to Texas RE Texas RE considered the Entity's and its affiliate's compliance history and determined there were no relevant instances of noncompliance.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
TRE2017018017	CIP-007-6	R2; R2.1; R2.2; R2.3	Medium	High	7/1/2016 (This is the date that CIP-007-6 R2.1 became enforceable.)	7/5/2017 (This is the date the that all security patches had received evaluations)	Self-Report	12/11/2019	01/17/2020

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

On July 26, 2017, the Entity submitted a Self-Report stating that, as a [redacted]), it was in violation of CIP-007-6 R2.2 and R2.3. In particular, the Entity failed to evaluate for applicability within 35 calendar days multiple security patches. The Entity also reported that on multiple occasions it failed to apply applicable security patches, create dated mitigation plans, or revise existing mitigation plans within 35 calendar days of the evaluations of applicable security patches. Upon reviewing the Self-Report, Texas RE determined that one of the reported instances of noncompliance was applicable to CIP-007-6 R2.1.

Issue #1 – The Entity stated that [redacted] software applications did not have identified patch sources pursuant to CIP-007-6 R2.1. By May 26, 2017, patch sources were identified for [redacted] software applications, and [redacted] software applications were deemed unnecessary and removed. The Entity was unable to demonstrate compliance with CIP-007-6 R2.1 between July 1, 2016, and May 26, 2017, for a total noncompliance period of 329 days. This issue is applicable to [redacted] PACS Cyber Asset associated with a High Impact BES Cyber System.

Issue #2 – The Entity stated that [redacted] security patches released prior to July 1, 2016, were not evaluated until January 17, 2017, and thus exceeded the 35-calendar day requirement for performing patch evaluations by 165 days. A [redacted] security patch released prior to July 1, 2016, was not evaluated until July 5, 2017, and thus exceeded the 35 calendar day requirement for performing patch evaluations by 334 days. These security patches were applicable to [redacted] High Impact BES Cyber Assets.

Issue #3 – The Entity stated that a security patch released on July 25, 2016, was not evaluated until July 5, 2017, and thus exceeded the 35-calendar day requirement for performing patch evaluations by 310 days. This security patch was applicable to [redacted] High Impact BCAs.

Issue #4 – The Entity stated that a security patch released on September 8, 2016, was not evaluated until December 5, 2016, and thus exceeded the 35-calendar day requirement for performing patch evaluations by 53 days. This security patch was applicable to [redacted] High Impact BCAs.

Issue #5 – The Entity stated that a security patch released on January 17, 2017, was not evaluated until February 22, 2017, and thus exceeded the 35-calendar day requirement for performing patch evaluations by one day. This security patch was applicable to [redacted] BCAs and [redacted] PCAs associated with High Impact BES Cyber Systems.

Issue #6 – The Entity stated that a security patch released on May 9, 2017, was not evaluated until June 29, 2017, and thus exceeded the 35-calendar day requirement for performing patch evaluations by 16 days. This security patch was applicable to [redacted] BCAs.

Issue #7 – The Entity stated that a security patch that was evaluated on July 29, 2016, was not installed and did not have a dated mitigation plan created (or an existing mitigation plan modified) until October 7, 2016, and thus exceeded the 35 calendar day requirement to install the patch or create a dated mitigation plan (or modify an existing mitigation plan) by 35 days. This security patch was applicable to [redacted] PACS Cyber Asset that is associated with a High Impact BES Cyber System.

The root cause of this noncompliance is a combination of inadequate patching procedures, a change in personnel performing patch management duties, resource constraints during the transition to CIP-007-6, and insufficient planning for handling the transition to CIP-007-6.

This noncompliance was noncontiguous and started on July 1, 2016, which is the day CIP-007-6 R2.1 became enforceable and ended on July 5, 2017, when all patch sources had been identified, all applicable security patches had been evaluated, and all patches had been installed or had dated mitigation plans created or modified.

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. Individually, most of the issues represent a minimal risk to the Bulk Power System. Issue #1 and Issue #2 represent a moderate risk to the Bulk Power System due to their duration, scope, or the Cyber Assets affected. In aggregate, these minimal and moderate risk issues indicate programmatic failures that must be addressed in order to ensure the reliability of the Bulk Power System. The risk to the Bulk Power System is increased as five of the instances of noncompliance are related to High Impact BCAs (and in some instances, their associated PCAs), and two instances of non-compliance are related to a PACS Cyber Asset associated with [redacted] High Impact BES Cyber Systems.

Entity specific factors that increase risk:

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
TRE2017018017	CIP-007-6	R2; R2.1; R2.2; R2.3	Medium	High	7/1/2016 (This is the date that CIP-007-6 R2.1 became enforceable.	7/5/2017 (This is the date the that all security patches had received evaluations)	Self-Report	12/11/2019	01/17/2020

- the Entity owns [redacted] Control Centers that each contain High Impact BES Cyber Systems;
- the Entity's system includes elements of a [redacted];
- the Entity's system load is [redacted];
- the Entity owns and operates [redacted]; and
- the Entity owns and operates [redacted].

Entity specific factors that reduce risk:

- the Entity's service territory is [redacted]; and
- the Entity's [redacted].

Factors specific to this noncompliance that reduce risk:

- Issue #1 – The noncompliance was isolated to [redacted] PACS Cyber Asset. During the period of noncompliance three security patches were released for applications that were subsequently deemed unnecessary and removed from the Cyber Asset;
- Issue #2 – The noncompliance was isolated to vulnerabilities that would be difficult to exploit. The first vulnerability affected Cyber Asset modules that were not physically connected to any networks, and as such, remote access was not possible and intrusion into a monitored Physical Security Perimeter would be necessary to exploit the vulnerability;
- Issue #3 – The noncompliance was isolated to vulnerabilities that would be difficult to exploit. The vulnerability affected Cyber Asset modules that were not physically connected to any networks, and as such, remote access was not possible and intrusion into a monitored Physical Security Perimeter would be necessary to exploit the vulnerability;
- Issue #4 – The noncompliance was related to an application that is only executed when needed for troubleshooting and is otherwise left inactive. This greatly limits the time that the attack surface is available;
- Issue #5 – The noncompliance was short, less than one day. The security patch was installed in the same patching cycle it would have been installed in had the patch been evaluated on time, and as such the affected Cyber Assets did not experience a delay in patching due to this noncompliance. Additionally, the Entity had already implemented the recommended vulnerability mitigations, therefore the vulnerability could not be exploited;
- Issue #6 – The duration of the noncompliance was short, lasting only 16 days. Additionally, the vulnerabilities related to this noncompliance were limited to a Local Attack Vector. To exploit these vulnerabilities, an attacker would need to be logged into the Cyber Asset or would need to rely on a user to execute a malicious file; and
- Issue #7 – The duration of the noncompliance was short, lasting only 35 days. Additionally, the noncompliance was isolated to [redacted] PACS Cyber Asset.

No harm is known to have occurred.

Mitigation

To mitigate this noncompliance the Entity performed the following activities:

- to end this noncompliance the Entity updated patch source tracking list to include all applicable software;
- to end this noncompliance the Entity removed unneeded installed software from applicable assets;
- to end this noncompliance the Entity performed evaluations of outstanding security patches;
- to end this noncompliance the Entity installed applicable security updates;
- to prevent reoccurrence of this noncompliance the Entity created a lessons learned document relating to patch monitoring;
- to prevent reoccurrence of this noncompliance the Entity updated lessons learned document to include step-by-step guidance on navigating identified patch sources;
- to prevent reoccurrence of this noncompliance the Entity added secondary sources of vulnerability notifications;
- to prevent reoccurrence of this noncompliance the Entity review SME responsibilities; and
- to prevent reoccurrence of this noncompliance the Entity perform a root cause analysis, process improvement analysis, or other assessment of the existing process to identify potential improvements.

Texas RE has verified the completion of all mitigation activity.

[redacted] NOC-2682 $36,750

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
TRE2017018017	CIP-007-6	R2; R2.1; R2.2; R2.3	Medium	High	7/1/2016 (This is the date that CIP-007-6 R2.1 became enforceable.	7/5/2017 (This is the date the that all security patches had received evaluations)	Self-Report	12/11/2019	01/17/2020

Other Factors

Texas RE reviewed the Entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

The Entity's ICP demonstrates a focus on improving the security of the Bulk Power System. The Entity's [redacted] and the Entity's [redacted]. The Entity actively participates in multiple compliance related industry groups.

The Entity did not receive mitigating credit for self-reporting because the Self-Report was submitted after receiving notice of an upcoming Compliance Audit.

Texas RE considered the entity's CIP-007-6 R2 compliance history in determining the disposition track. Texas RE determined the entity's CIP-007-6 R2 compliance history to be an aggravating factor in the disposition determination.

In determining the penalty assessment for this issue, although the Entity did not receive mitigating credit for self-reporting, Texas RE considered the fact that the issue was part of a noncompliance spanning multiple regions and Registered Entities. Specifically, the Entity is [redacted]. The Entity and the affiliate share [redacted]. The Entity's affiliate company was assessed an aggregate penalty of [redacted]. Texas RE concluded that it was appropriate to adjust the Entity's penalty assessment for instances of noncompliance for which the Entity's affiliate company was already assessed a penalty.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
TRE2017018012	CIP-010-2	R1; R1.1.2; R1.1.5	Medium	Moderate	07/01/2016 (The date CIP-010-2 R1 became enforceable.)	02/14/2017 (The date all required baseline items were documented.)	Self-Report	04/21/2017	01/17/2020

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

On July 25, 2017, the Entity submitted a Self-Report stating that, as a [redacted], it was in violation of CIP-010-2 R1. In particular, the entity failed to include CIP-010-2 R1 R1.1.2 in its baseline documentation for [redacted] High Impact BES Cyber Assets (BCA), and failed to include CIP-010-2 R1.1.5 in its baseline documentation for [redacted] BCAs and [redacted] Protected Cyber Assets (PCA).

The root cause of this noncompliance was the use of older or insufficient change management processes.

For R1.1.2, the Entity implemented a new change management process on July 1, 2016. The BCAs found to be noncompliant with R1.1.2 were commissioned under the Entity's previous change management process. The commissioning of these BCAs occurred after the Entity had deployed their baseline monitoring tool and before the Entity had modified their change management processes to include steps to ensure changes would be detected by their baseline monitoring tool.

For R1.1.5, the Entity only considered applied security patches for items that were listed in the baseline as part of R1.1.1, R1.1.2, or R1.1.3. For devices where an independent operating system and firmware exists, the Entity opted to record the operating system as part of the baseline and did not include the firmware in their R1.1.1 documentation. As such, firmware updates that were security related were not added to the R1.1.5 baseline documentation.

This noncompliance started on July 1, 2016, which is the day CIP-010-2 R1 became enforceable, and ended on February 14, 2017, when all required parts of CIP-010-2 R1 were included in the Entity's baseline documentation.

Risk Assessment

This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risks in not including commercially available or open-source application software and installed security patches in the Entity's baseline documentation is that a malicious individual can make unauthorized changes to the software that could subsequently go undetected. If the unauthorized changes are malicious in nature, then this can result in the devices being rendered unavailable, degraded or misused.

Entity specific factors that increase risk:

- the Entity owns [redacted] Control Centers which each contain High Impact BES Cyber Systems;
- the Entity's system includes [redacted];
- the Entity's system load [redacted];
- the Entity owns and operates [redacted]; and
- the Entity owns and operates [redacted].

Entity specific factors that reduce risk:

- the Entity's service territory is [redacted]; and
- the Entity's [redacted].

Factors specific to this noncompliance that reduce risk:

- the scope of the noncompliance was limited. The R1.1.2 noncompliance affected [redacted] applicable Cyber Assets. The R1.1.5 noncompliance affected [redacted] applicable Cyber Assets;
- upon adding the required items to their baseline monitoring tool, the entity verified that the correct versions were present; and
- the Entity has deployed [redacted].

No harm is known to have occurred.

Mitigation

To mitigate this noncompliance the Entity performed the following activities:

- to end this noncompliance the Entity updated the path their baseline monitoring tool was looking at to determine software version;
- to end this noncompliance the Entity added a configuration change to their baseline monitoring tool to monitor firmware version; and

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
TRE2017018012	CIP-010-2	R1; R1.1.2; R1.1.5	Medium	Moderate	07/01/2016 (The date CIP-010-2 R1 became enforceable.)	02/14/2017 (The date all required baseline items were documented.)	Self-Report	04/21/2017	01/17/2020

- to prevent reoccurrence of this noncompliance the Entity updated their configuration monitoring procedure to explicitly indicate that firmware security patches must be included in the configuration baseline.

Texas RE has verified the completion of all mitigation activity.

Other Factors

Texas RE reviewed the Entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

The Entity's ICP demonstrates a focus on improving the security of the Bulk Power System. The Entity's [redacted] and the Entity's [redacted]. The Entity actively participates in multiple compliance related industry groups.

The Entity did not receive mitigating credit for self-reporting because the Self-Report was submitted after receiving notice of an upcoming Compliance Audit.

Texas RE considered the Entity's CIP-010-2 R1 compliance history in determining the disposition track. Texas RE determined the Entity's CIP-010-2 R1 compliance history should not serve as an aggravating factor in the disposition determination.

In determining the penalty assessment for this issue, although the Entity did not receive mitigating credit for self-reporting, Texas RE considered the fact that the issue was part of a noncompliance spanning multiple regions and Registered Entities. Specifically, the Entity [redacted]. The Entity and the affiliate share [redacted]. The Entity's affiliate company was assessed an aggregate penalty of [redacted]. Texas RE concluded that it was appropriate to adjust the Entity's penalty assessment for instances of noncompliance for which the Entity's affiliate company was already assessed a penalty.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
TRE2017017934	CIP-007-6	R1; R1.1	Medium	High	07/01/2016 (The date CIP-007-6 R1 became enforceable.)	05/26/2017 (This is the date the Entity disabled all unneeded ports.)	Self-Report	08/09/2017	01/17/2020

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

On July 10, 2017, the Entity submitted a Self-Report stating that, as a [redacted]), it was in violation of CIP-007-6 R1. In particular, the entity failed to enable only the logical network accessible ports that had been determined to be needed by the Entity. Specifically, the Entity reported that one unneeded listening port was identified on a Physical Access Control Systems (PACS) Cyber Asset.

The root cause of this noncompliance was a failure to remove unnecessary software and a failure to make full use of available tools. This noncompliance was due to an unneeded port being in an enabled and listening state. The port was opened by an application that the Entity does not use. If the software had not been present and running on the affected Cyber Asset, then this noncompliance would not have occurred. Additionally, the Entity uses a tool to monitor their baseline configurations. This tool has reporting features that could have alerted the Entity to this noncompliance sooner, however these reporting features were not being used.

This noncompliance started on July 1, 2016, which is the day CIP-007-6 R1 became enforceable, and ended on May 26, 2017, when all unneeded logically accessible network ports were disabled.

Risk Assessment

This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Enabled logically accessible network ports represent a potential entry point into a Cyber Asset. A failure to disable enabled logically accessible network ports that are not needed unnecessarily increases the attack surface of the affected Cyber Asset. An attack on a PACS 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.

Entity specific factors that increase risk:

- the Entity owns [redacted] Control Centers which each contain High Impact BES Cyber Systems;
- the Entity's system includes [redacted];
- the Entity's system load [redacted];
- the Entity owns and operates [redacted]; and
- the Entity owns and operates [redacted].

Entity specific factors that reduce risk:

- the Entity's service territory is [redacted]; and
- the Entity's [redacted].

Factors specific to this noncompliance that reduce risk:

- [redacted] unnecessary network accessible port was found to be enabled; and
- the enabled unnecessary network accessible port was not enabled due to malicious events. The port was enabled due to the existence of vendor management software that was installed by default on the Cyber Asset.

No harm is known to have occurred.

Mitigation

To mitigate this noncompliance the Entity performed the following activities:

- to end this noncompliance the Entity disabled any ports deemed unneeded;
- to end this noncompliance the Entity justified all ports deemed needed;
- to end this noncompliance the Entity removed unneeded software so as to prevent the software from opening unneeded ports; and
- to prevent reoccurrence of this noncompliance the Entity created a customized report for the Cyber Asset involved in this noncompliance.

Texas RE has verified the completion of all mitigation activity.

Other Factors

Texas RE reviewed the Entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

[redacted] NOC-2682 $36,750

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
TRE2017017934	CIP-007-6	R1; R1.1	Medium	High	07/01/2016 (The date CIP-007-6 R1 became enforceable.)	05/26/2017 (This the date the Entity disabled all unneeded ports.)	Self-Report	08/09/2017	01/17/2020

The Entity's ICP demonstrates a focus on improving the security of the Bulk Power System. [redacted] The Entity actively participates in multiple compliance related industry groups.

The Entity did not receive mitigating credit for self-reporting because the Self-Report was submitted after receiving notice of an upcoming Compliance Audit.

Texas RE considered the Entity's CIP-007-6 R1 compliance history in determining the disposition track. Texas RE determined the Entity's CIP-007-6 R1 compliance history should not serve as an aggravating factor in the disposition determination.

In determining the penalty assessment for this issue, although the Entity did not receive mitigating credit for self-reporting, Texas RE considered the fact that the issue was part of a noncompliance spanning multiple regions and Registered Entities. Specifically, the Entity [redacted]. The Entity and the affiliate share substantia [redacted]. The Entity's affiliate company was assessed an aggregate penalty of [redacted]. Texas RE concluded that it was appropriate to adjust the Entity's penalty assessment for instances of noncompliance for which the Entity's affiliate company was already assessed a penalty.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
TRE2017017935	CIP-007-6	R4; R4.1; R4.2; R4.3	Medium	High	07/01/2016 (The date CIP-007-6 R4 became enforceable.)	05/15/2017 (This is the date the Entity began using malicious code detection and removal software that was compatible with their logging infrastructure.)	Self-Report	05/07/2018	01/17/2020

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

On July 10, 2017, the Entity submitted a Self-Report stating that, as a [redacted]), it was in violation of CIP-007-6 R4. According to the Entity, it discovered that although its logging tool was receiving logs from one of its Physical Access Control System (PACS) Cyber Assets pursuant to CIP-007-6, R4, Parts 4.1.1 and 4.1.2, it was unable to normalize, alert on, and retain logs of detected malicious code on its PACS Cyber Asset in accordance with CIP-007-6 R4, Parts 4.1.3, 4.2.1, and 4.3. Additionally, the Entity stated that it was unable to detect event logging failure of detected malicious code pursuant to CIP-007-6 R4, Part 4.2.2.

The root cause of this noncompliance was insufficient procedures. The Entity implemented new tools as part of the transition from CIP-007-3a to CIP-007-6. With the transition the Entity's procedures were not in a sufficient state to ensure the Entity would be compliant with newly applicable requirements.

This noncompliance started on July 1, 2016, which is the day CIP-007-6 R4 became enforceable, and ended on May 15, 2017, when the Entity began using malicious code detection and removal software that was compatible with their logging infrastructure.

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 log events of detected malicious code and a failure to generate alerts on detected malicious code can result in cyber security staff being unaware that malicious code is present on one or more systems. Similarly, a failure to generate alerts on the failure of event logging can result in cyber security staff being unaware that logging is not functioning properly and subsequently can result in a failure to log events. A failure to retain event logs for the last 90 consecutive calendar days can impede the forensic analysis of a Cyber Security Incident.

Entity specific factors that increase risk:

- the Entity owns [redacted] Control Centers which each contain High Impact BES Cyber Systems;
- the Entity's system [redacted];
- the Entity's system load [redacted]
- the Entity owns and operates [redacted]; and
- the Entity owns and operates [redacted].

Entity specific factors that reduce risk:

- the Entity's service territory [redacted]; and
- the Entity's [redacted].

Factors specific to this noncompliance that reduce risk:

- the noncompliance was related to logs generated from the software used for detection and removal of malicious code. During the noncompliance, the malicious code detection and removal software continued to function as intended.

No harm is known to have occurred.

Mitigation

To mitigate this noncompliance the Entity performed the following activities:

- to end this noncompliance the Entity replaced their malicious code detection and removal software with one whose logging function was compatible with their existing logging infrastructure;
- to end this noncompliance the Entity tested and confirmed that logging and alerting works with the new malicious code detection and removal software;
- to prevent reoccurrence of this noncompliance the Entity setup a separate daily report for the affected PACS Cyber Asset;
- to prevent reoccurrence of this noncompliance the Entity conducted CIP-007-6 R4 training with applicable SMEs;and
- to prevent reoccurrence of this noncompliance the Entity updated work procedures used to execute CIP-007-6 R4 tasks.

Texas RE has verified the completion of all mitigation activity.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
TRE2017017935	CIP-007-6	R4; R4.1; R4.2; R4.3	Medium	High	07/01/2016 (The date CIP-007-6 R4 became enforceable.)	05/15/2017 (This is the date the Entity began using malicious code detection and removal software that was compatible with their logging infrastructure.)	Self-Report	05/07/2018	01/17/2020

Other Factors	Texas RE reviewed the Entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The Entity's ICP demonstrates a focus on improving the security of the Bulk Power System. The Entity's [redacted] and the Entity's [redacted]. The Entity actively participates in multiple compliance related industry groups. The Entity did not receive mitigating credit for self-reporting because the Self-Report was submitted after receiving notice of an upcoming Compliance Audit. Texas RE considered the entity's CIP-007-6 R4 compliance history in determining the disposition track. Texas RE determined the entity's CIP-007-6 R4 compliance history should not serve as an aggravating factor in the penalty determination because this instance of noncompliance does not share a root cause with the previous instance of noncompliance with CIP-007-6 R4. In determining the penalty assessment for this issue, although the Entity did not receive mitigating credit for self-reporting, Texas RE considered the fact that the issue was part of a noncompliance spanning multiple regions and Registered Entities. Specifically, the Entity [redacted]. The Entity and the affiliate share [redacted]. The Entity's affiliate company was assessed an aggregate penalty of [redacted] Texas RE concluded that it was appropriate to adjust the Entity's penalty assessment for instances of noncompliance for which the Entity's affiliate company was already assessed a penalty.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2018020557	CIP-011-2	R1: P1.2	Medium	Severe	4/23/2018 (when the contractor forwarded documents containing BCSI to their personal email address)	7/31/2018 (when the contractor removed all BCSI from their personal email account)	Self Log	3/2/2020	3/19/2020

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On October 19, 2018, the entity submitted a Self-Log stating that, as a [redacted], it was in noncompliance with CIP-011-2 R1. Specifically, one contractor did not adhere to the entity's procedure for protecting and securely handling BES Cyber System Information (BSCI). The contractor was engaged to document the implementation of the entity's [redacted] and was granted electronic access to BSCI. On five occasions, beginning April 23, 2018, the contractor forwarded documents containing BSCI, including [redacted], to their personal email account in contravention of the entity's documented information protection program. This issue ended on July 31, 2018, when the contractor removed all BSCI from their personal email account and hardware, for a duration of 100 days. The root cause of the issue was attributed to a contractor not following company policy. Specifically, the contractor had received the required cyber security and information protection training in accordance with company policy, but justified their actions based on their preference to use personal tools and technology to complete work.
Risk Assessment	This violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to adequately implement its documented information protection program for protecting and securely handling BSCI, including storage, transit, and use as required in CIP-011-2 R1 Part 1.2 regarding a contractor and five emails containing BSCI. Failure to adequately protect such information could have resulted in a malicious actor with access to the information selling the data for profit or a benign actor mishandling the information and causing an inadvertent public disclosure of the data. However, the entity reported that it had confirmed via attestation that the contractor did not forward the information to any other third-party individuals. Additionally, the entity had completed a personnel risk assessment for the contractor and had executed a nondisclosure agreement with the third-party vendor with whom the contractor was employed; the contractor, in turn, had executed a nondisclosure agreement with the third-party vendor. Additionally, the contractor did not mishandle any account login information, instructions regarding how to access the devices, nor information required for authentication. Further, the data associated with this issue included noncritical information interspersed with BSCI; this combination made the critical information indistinguishable to anyone not intricately familiar with the entity's environment. Finally, the entity has a minimal impact footprint with [redacted] and WECC confirmed that all [redacted] were unaltered and remained operational throughout the period associated with this issue, thereby reducing the risk of any potential impact.
Mitigation	To mitigate this violation, the entity: 1) recovered all data associated with this issue and obtained a signed affidavit from the contractor that all data had been purged from external environments; 2) terminated the contractor's authorized physical and electronic access; and 3) emailed communication to all contractors associated with the project reiterating the entity's information security process for protecting and handling BES Cyber System Information.
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. WECC determined that the entity has a comprehensive, well-organized, and fully implemented ICP. WECC considered the entity's history of noncompliance with CIP-011-2 and determined it should not serve as a basis for aggravating to a penalty because the root cause of the prior issues were attributed to a lack of training whereas the current issue was attributed to not following company policy. Therefore, the nature of the prior violations is distinct and separate from the current issue and not indicative of a broader issue.

	WECC determined that issues involving data exposures, even when contained, require heightened awareness to adequately protect the reliability and security of the Bulk Electric System. Therefore, although this instance was deemed minimal risk, information security is critical for the continued reliability of the BES. Therefore, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty.