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

Filing Date: July 30, 2020

[redacted] NOC-2671 $0

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.

[redacted] NOC-2671 $0

	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.

[redacted]	NOC-2671	$0

	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.

[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

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:

[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

- 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.

Texas Reliability Entity, Inc (Texas RE) Settlement Agreement (Agrees) CIP

[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.

[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
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

[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
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.

[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 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.

[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
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.

[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
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.

[redacted] NOC - 2683 $0

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.

[redacted]	NOC - 2683	$0

	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.

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	WECC2017017388	Yes	Yes	Yes	Yes		Yes	Yes	Yes	Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
2	WECC2017017390	Yes	Yes	Yes	Yes		Yes	Yes	Yes	Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years

Filing Date: May 28, 2020

[redacted] NOC-2674 $0

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
WECC2017017388	CIP-014-2	R5: P5.1	High	Lower	6/27/2016 (when the requirement was enforceable)	1/21/2020 (Mitigation Plan completion)	Compliance Audit	1/21/2020	1/29/2020

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.)

During a Compliance Audit conducted [redacted] WECC determined that the entity, as [redacted] was in violation of CIP-014-2 R5 Part 5.1. The entity did not develop physical security plans that included resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities that the entity had identified during its evaluation conducted pursuant to CIP-014-2 R4. Specifically, the entity's physical security plans lacked specific mitigating measures for many of the threats identified in its R4 threat & vulnerability evaluation. At [redacted] critical facility, an identified top threat was not listed in the physical security plan with a corresponding measure of protection against said threat. Additionally, some recommended mitigating measures could not clearly be linked to which critical BES assets within a critical facility would be protected, or the identified threat that would be countered.

WECC Enforcement concurred with the audit findings as described above. The root cause of this violation was a less than adequate understanding of how to document mitigating activities to specifically address identified vulnerabilities and threats pursuant to CIP-014-2 R5 Part 5.1. This violation began on June 27, 2016, when the entity was required to implement CIP-014-2 R5 and ended on January 21, 2020 when the entity completed mitigating activities, for a total of 1,304 days of noncompliance.

Risk Assessment

This violation posed a moderate risk and did not pose a serious and substantial risk to the Bulk Power System. In this instance, the entity failed to appropriately develop physical security plans that included resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted pursuant to CIP-014-2 R4. Failure to effectively counter identified critical facility and Critical Asset threats increased the risk of an unauthorized individual degrading or destroying a facility and/or Cyber Assets vital to the reliability of the BES. As CIP-014 critical facilities, these facilities are deemed necessary to the continuity of the entity's grid operations.

However, the likelihood of the risk occurring was reduced by the controls the entity had implemented. Specifically, the entity utilized [redacted] as a physical barrier at its CIP-014-2 identified facilities; had signage that provides warning information relating to video monitoring, trespassing, and safety; had multi-factor authentication access control to restrict access that alarms on detection at the perimeters; had camera surveillance strategically placed [redacted] had 24 hours-a-day, 7 days-a-week alarm monitoring and rapid response; coordinates and collaborates with law enforcement for responding to issues; [redacted] The perimeter detection provides awareness of intrusion [redacted] and [redacted] provide layered defense and alarm notification.

Additionally, the entity had [redacted] that it could use in conjunction with similar efforts [redacted] to mitigate threats to the BES. This [redacted] specifically included all Transmission stations and substations, as well as the control center identified as a part of CIP-014-2. The purpose of the plan was to use the results of a completed technical study and implement resiliency measures for each of these facilities [redacted] These additional controls helped to lessen the risk.

Mitigation

To mitigate this violation, the entity has:

1) revised its primary Control Center (PCC) threat and vulnerability assessment (TVA) documents as follows:
   a) identified and described each physical boundary and security controls deployed at each layer. The defense-in-depth description will begin at the outermost perimeter, working inward to assess potential TVAs as constructed;
   b) ensured the [redacted] assessment (PCC only) provides a clear and appropriate view of critical components that facilitate the function of the facility and most likely vulnerabilities based on present security system capabilities. Ensured each credible TVA maps directly to solutions defined in R5 and provided a more granular approach to site protection;
   c) investigated the inclusion of an Adversary Sequence Diagram within its documentation; and

[redacted] NOC-2674 $0

	d) provided more quantitative evidence for the establishment of its risk threshold. Re-evaluated all potential attacks against its risk threshold, with emphasis on providing content that only removes extreme events from assessment scope. 2) revised its PCC physical security plans documents as follows: a) ensured its response systems and personnel designed to detect physical attacks, respond within a timeframe suitable to mitigate those attacks to the PCC in a timely manner; b) ensured physical security plans created in R5 would effectively demonstrate the capability to deter, detect, delay, assess, communicate and respond to physical attacks; c) removed the language that identified that existing security measures at the PCC were sufficient for compliance with R5; d) reviewed and documented site deficiencies and included additional information on purpose and benefits of security measures to enhance deficiencies; and e) improved its security enhancement timeline by including security measure efficacy testing as part of implementation timeline; 3) revised substation(s) TVA documents to address items as follows: a) increased history of attacks analysis to incorporate more data on a national level to increase scope of TVA likelihood evaluation; b) provided more quantitative evidence for the establishment of its risk threshold. Re-evaluated all potential attacks against its risk threshold, with emphasis on providing content that only removes extreme events from assessment scope; and c) removed the justification (Critical Components Analysis) for the differentiation of critical and non-critical components at a substation, i.e., do not apply the R1 criteria to exclude specific components from the scope of R4 and R5; 4) revised substation(s) physical security plan documents as follows: a) ensured its response systems and personnel designed to detect physical attacks, respond within a timeframe suitable to mitigate or decrease the impact of physical attacks to substations and in a timely manner; b) ensured physical security plans created in R5 would effectively demonstrate the capability to deter, detect, delay, assess, communicate and respond to physical attacks. c) identified and described each security controls deployed at each defensible layer of the substation(s). The defense-in-depth description will begin at the outermost perimeter, working inward to assess potential threats and vulnerabilities as constructed. Each security control will address its security measure (i.e. deter, detect, delay, communicate, assess, respond) as well as the threat the equipment is attempting to provide its security measure for. Additional emphasis and details should be included within the documentation to describe the work the entity is committing to and using at the critical sites; d) ensured all substation(s) assets that comprise a critical facility are considered, in preventing and responding to potential physical attacks. Determined that additional security measures may be required to meet site or asset protection needs. Those deemed necessary for a comprehensive physical security solution should be considered for effectiveness to overall facility operation; e) reviewed and documented site deficiencies and included additional information on the purpose and benefits of security measures to enhance deficiencies; and f) improved its security enhancement timeline by including security measure efficacy testing as part of the implementation timeline; 5) began facilitation of interdepartmental meetings that includes [redacted] in order to provide further insight on the criticality of the equipment being protected at each defined critical site; 6) began facilitation of monthly meetings of [redacted] which includes Director-level leadership of BES Cyber Systems and CIP-014-2 leadership; 7) created communication avenues for CIP topics, to include CIP-014-2 Physical Security Plans; 8) created a new position [redacted] to assist in addressing the leadership items identified within CIP-014-2. With this new position, the following benefits are derived: a) Physical and Cyber Security report [redacted] as each department plays a role in the protecting the BES; b) [redacted] is responsible for the proper execution of the NERC CIP program where in the previous organizational structure CIP-014-2 ownership was an outlier within CIP program. [redacted] meets with [redacted] every two weeks to discuss physical and cyber security issues 9) Improving CIP-014-2 knowledge from WECC as follows: a) [redacted] attended the WECC Compliance Workshop in March 2017 in San Diego, California. [redacted] b) [redacted] personnel attended monthly WECC Compliance Open Mics, and the Fall 2017 and Spring and Fall 2018 WECC Reliability and Security Workshops; c) [redacted] attended [redacted]

Western Electricity Coordinating Council (WECC) Settlement Agreement Admits CIP

[redacted] NOC-2674 $0

	10) Improving CIP-014 Knowledge from Industry perspective as follows: a) Conducted immediate outreach to CIP specialists at [redacted] and the WECC Physical Security Working Group; b) [redacted] maintained regular attendance at WECC Physical Security Working Group meetings; c) Monthly meetings with CIP subject matter experts of [redacted] and 11) Partnered with the local Police Department and Fire and Rescue for conduction of an Active Shooter Exercise [redacted] The exercise was a full-scale exercise including voluntary participation from the its employees.
Other Factors	WECC confirmed the entity did not effectively complete its mitigation of the violation; therefore, rejected the Certification of Mitigation Completion, requiring the entity to expand its mitigation and resubmit. As such, WECC escalated this moderate risk violation from an FFT to a $0 Spreadsheet Notice of Penalty. WECC determined there was no relevant compliance history.

[redacted] NOC-2675 $0

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
WECC2017017390	CIP-014-2	R5: P5.1	High	Lower	6/27/2016 (when the requirement was enforceable)	1/21/2020 (Mitigation Plan completion)	Compliance Audit	1/21/2020	1/29/2020

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.)

During a Compliance Audit conducted [redacted] WECC determined that the entity, as [redacted] was in violation of CIP-014-2 R5 Part 5.1 The entity did not develop physical security plans that included resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities that the entity had identified during its evaluation conducted pursuant to CIP-014-2 R4. Specifically, the entity's physical security plans lacked specific mitigating measures for many of the threats identified in its R4 threat & vulnerability evaluation. At [redacted] critical facility, an identified top threat was not listed in the physical security plan with a corresponding measure of protection against said threat. Additionally, some recommended mitigating measures could not clearly be linked to which critical BES assets within a critical facility would be protected, or the identified threat that would be countered.

WECC Enforcement concurred with the audit findings as described above. The root cause of this violation was a less than adequate understanding of how to document mitigating activities to specifically address identified vulnerabilities and threats pursuant to CIP-014-2 R5 Part 5.1. This violation began on June 27, 2016, when the entity was required to implement CIP-014-2 R5 and ended on January 21, 2020 when the entity completed mitigating activities, for a total of 1,304 days of noncompliance.

Risk Assessment

This violation posed a moderate risk and did not pose a serious and substantial risk to the Bulk Power System. In this instance, the entity failed to appropriately develop physical security plans that included resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted pursuant to CIP-014-2 R4. Failure to effectively counter identified critical facility and Critical Asset threats increased the risk of an unauthorized individual degrading or destroying a facility and/or Cyber Assets vital to the reliability of the BES. As CIP-014 critical facilities, these facilities were deemed necessary to the continuity of the entity's grid operations.

However, the likelihood of the risk occurring was reduced by the controls the entity had implemented. Specifically, the entity utilized [redacted] as a physical barrier at its CIP-014-2 identified facilities; had signage that provides warning information relating to video monitoring, trespassing, and safety; had multi-factor authentication access control to restrict access that alarms on detection at the perimeters; had camera surveillance strategically placed [redacted] had 24 hours-a-day, 7 days-a-week alarm monitoring and rapid response; coordinates and collaborates with law enforcement for responding to issues; and [redacted] The perimeter detection provides awareness of intrusion [redacted] and [redacted] provide layered defense and alarm notification.

Additionally, the entity had [redacted] that it could use in conjunction with similar efforts [redacted] to mitigate threats to the BES. This [redacted] specifically included all Transmission stations and substations, as well as the control center identified as a part of CIP-014-2. The purpose of the plan was to use the results of a completed technical study and implement resiliency measures for each of these facilities [redacted] hese additional controls helped to lessen the risk.

Mitigation

To mitigate this violation, the entity has:

1) revised its primary Control Center (PCC) threat and vulnerability assessment (TVA) documents as follows:
   a) identified and described each physical boundary and security controls deployed at each layer. The defense-in-depth description will begin at the outermost perimeter, working inward to assess potential TVAs as constructed;
   b) ensured the [redacted] assessment (PCC only) provides a clear and appropriate view of critical components that facilitate the function of the facility and most likely vulnerabilities based on present security system capabilities. Ensured each credible TVA maps directly to solutions defined in R5 and provided a more granular approach to site protection;
   c) investigated the inclusion of an Adversary Sequence Diagram within its documentation; and

[redacted] NOC-2675 $0

	d) provided more quantitative evidence for the establishment of its risk threshold. Re-evaluated all potential attacks against its risk threshold, with emphasis on providing content that only removes extreme events from assessment scope. 2) revised its PCC physical security plans documents as follows: a) ensured its response systems and personnel designed to detect physical attacks, respond within a timeframe suitable to mitigate those attacks to the PCC in a timely manner; b) ensured physical security plans created in R5 would effectively demonstrate the capability to deter, detect, delay, assess, communicate and respond to physical attacks; c) removed the language 3 that identified that existing security measures at the PCC were sufficient for compliance with R5; d) reviewed and documented site deficiencies and included additional information on purpose and benefits of security measures to enhance deficiencies; and e) improved its security enhancement timeline by including security measure efficacy testing as part of implementation timeline; 3) revised substation(s) TVA documents to address items as follows: a) increased history of attacks analysis to incorporate more data on a national level to increase scope of TVA likelihood evaluation; b) provided more quantitative evidence for the establishment of its risk threshold. Re-evaluated all potential attacks against its risk threshold, with emphasis on providing content that only removes extreme events from assessment scope; and c) removed the justification (Critical Components Analysis) for the differentiation of critical and non-critical components at a substation, i.e., do not apply the R1 criteria to exclude specific components from the scope of R4 and R5; 4) revised substation(s) physical security plan documents as follows: a) ensured its response systems and personnel designed to detect physical attacks, respond within a timeframe suitable to mitigate or decrease the impact of physical attacks to substations and in a timely manner; b) ensured physical security plans created in R5 would effectively demonstrate the capability to deter, detect, delay, assess, communicate and respond to physical attacks. c) identified and described each security controls deployed at each defensible layer of the substation(s). The defense-in-depth description will begin at the outermost perimeter, working inward to assess potential threats and vulnerabilities as constructed. Each security control will address its security measure (i.e. deter, detect, delay, communicate, assess, respond) as well as the threat the equipment is attempting to provide its security measure for. Additional emphasis and details should be included within the documentation to describe the work the entity is committing to and using at the critical sites; d) ensured all substation(s) assets that comprise a critical facility are considered, in preventing and responding to potential physical attacks. Determined that additional security measures may be required to meet site or asset protection needs. Those deemed necessary for a comprehensive physical security solution should be considered for effectiveness to overall facility operation; e) reviewed and documented site deficiencies and included additional information on the purpose and benefits of security measures to enhance deficiencies; and f) improved its security enhancement timeline by including security measure efficacy testing as part of the implementation timeline; 5) began facilitation of interdepartmental meetings that includes [redacted] in order to provide further insight on the criticality of the equipment being protected at each defined critical site; 6) began facilitation of monthly meetings of [redacted] which includes Director-level leadership of BES Cyber Systems and CIP-014-2 leadership; 7) created communication avenues for CIP topics, to include CIP-014-2 Physical Security Plans; 8) created a new position [redacted] to assist in addressing the leadership items identified within CIP-014-2. With this new position, the following benefits are derived: a) Physical and Cyber Security report [redacted] as each department plays a role in the protecting the BES; b) [redacted] is responsible for the proper execution of the NERC CIP program where in the previous organizational structure CIP-014-2 ownership was an outlier within CIP program. [redacted] meets with [redacted] every two weeks to discuss physical and cyber security issues 9) Improving CIP-014-2 knowledge from WECC as follows: a) [redacted] attended the WECC Compliance Workshop in March 2017 in San Diego, California. [redacted] b) [redacted] attended monthly WECC Compliance Open Mics, and the Fall 2017 and Spring and Fall 2018 WECC Reliability and Security Workshops; c) [redacted] attended [redacted]

Western Electricity Coordinating Council (WECC) Settlement Agreement Admits CIP

[redacted] NOC-2675 $0

	10) Improving CIP-014 Knowledge from Industry perspective as follows: a) Conducted immediate outreach to CIP specialists at [redacted] and the WECC Physical Security Working Group; b) [redacted] maintained regular attendance at WECC Physical Security Working Group meetings; c) Monthly meetings with CIP subject matter experts of [redacted] and 11) Partnered with the local Police Department and Fire and Rescue for conduction of an Active Shooter Exercise [redacted] The exercise was a full-scale exercise including voluntary participation from the its employees.
Other Factors	WECC confirmed the entity did not effectively complete its mitigation of the violation; therefore, rejected the Certification of Mitigation Completion, requiring the entity to expand its mitigation and resubmit. As such, WECC escalated this moderate risk violation from an FFT to a $0 Spreadsheet Notice of Penalty. WECC determined there was no relevant compliance history.

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	RFC2017016915	Yes		Yes	Yes		Yes				Yes		Yes	Category 1: 3 years; Category 2 – 12: 2 years
2	RFC2016016509	Yes		Yes	Yes		Yes		Yes		Yes			Category 1: 3 years; Category 2 – 12: 2 years
3	RFC2017016917	Yes		Yes	Yes		Yes		Yes		Yes			Category 1: 3 years; Category 2 – 12: 2 years
4	RFC2017016918	Yes		Yes	Yes		Yes				Yes		Yes	Category 1: 3 years; Category 2 – 12: 2 years
5	RFC2018019980	Yes		Yes	Yes		Yes		Yes	Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
6	RFC2018019981	Yes		Yes	Yes		Yes		Yes		Yes		Yes	Category 1: 3 years; Category 2 – 12: 2 years
7	RFC2017016919	Yes		Yes	Yes		Yes			Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
8	RFC2017016924	Yes		Yes	Yes		Yes		Yes		Yes			Category 1: 3 years; Category 2 – 12: 2 years
9	RFC2017018532	Yes		Yes	Yes	Yes	Yes			Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
10	RFC2017016920	Yes		Yes	Yes		Yes		Yes		Yes			Category 1: 3 years; Category 2 – 12: 2 years
11	RFC2017018530	Yes		Yes	Yes	Yes	Yes			Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
12	RFC2017018533	Yes		Yes	Yes	Yes	Yes		Yes	Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
13	RFC2016016473	Yes		Yes	Yes		Yes				Yes			Category 1: 3 years; Category 2 – 12: 2 years
14	RFC2017016922	Yes		Yes	Yes		Yes		Yes		Yes			Category 1: 3 years; Category 2 – 12: 2 years
15	RFC2017016923	Yes		Yes	Yes		Yes			Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
16	RFC2017018534	Yes		Yes	Yes	Yes	Yes			Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years

Filing Date: March 31, 2020

[redacted] NOC-2664 $225,000

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
RFC2017016915	CIP-002-5.1	R1	High	Lower	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	1/26/2017 (the date the entity properly classified the virtual server and included it in the Asset Identification list)	Self-Report	2/15/2017	2/1/2018

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On January 31, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-002-5.1 R1. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in this Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets. The entity identified and classified all of its Bulk Electric System (BES) Cyber Systems prior to its new CIP environment go-live date on [redacted]. On February 19, 2016, during an internal control and reconciliation activity before the go-live date, one virtual server at the primary control center was classified in the asset management system, the entity's system of record, as a high impact device. (The virtual server is used as an [redacted] device for syslog files and should be classified as a high impact device with a BES type of Electronic Access Control or Monitoring Systems.) However, this device was mistakenly reclassified as a low impact device on March 2, 2016. Consequently, the virtual server did not appear on the entity's CIP-002 Asset Identification list, which does not contain low impact BES Cyber Assets. The root cause of this violation was an insufficient process for categorization that did not include a section for validating virtual servers as part of the steps for inventory identification. This major contributing factor involves the management practices of asset and configuration management, which includes identifying assets and configuration items, and validation, in that the entity failed to validate the virtual server during its inventory identification process.
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 based on the following factors. First, this is a documentation issue. Despite being mistakenly classified as a low impact asset, the virtual server in question had been consistently afforded the protections of a high impact BES Cyber System, except for the CIP-007-6 deficiencies that are discussed later in this Agreement (Specifically [redacted], [redacted] and [redacted] Second, the virtual server in question was decommissioned less than a year after it was improperly classified because it was no longer necessary to be in the Electronic Security Perimeter. This fact reduced the time period that the misclassification could have caused any adverse effect on the BES.
Mitigation	To mitigate this violation, the entity: 1) validated the virtual hosts and virtual servers as being on the CIP-002 Asset Identification list and properly classified in the asset management system; 2) decommissioned the relevant virtual server; and 3) updated its CIP-002 BES Cyber Systems Categorization process to include a section for validating virtual servers as part of the steps for inventory identification and the annual review steps.
Other Factors	ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in Self-Reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level. ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.

[redacted] NOC-2664 $225,000

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
RFC2016016509	CIP-004-3a	R4	Lower	Moderate	3/31/2015 (when the entity first failed to include the applications in the quarterly reviews)	10/5/2016 (the date the entity completed a comprehensive review to ensure that all access information is correct for Critical Cyber Assets/Bulk Electric System Cyber Systems.)	Self-Report	1/31/2017	4/4/2018

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

On November 8, 2016, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [redacted], it was in violation of CIP-004-3a R4. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.

As part of the entity's regular quarterly access reviews in the first and second quarters of 2016, the entity discovered 10 instances where it failed to revoke access in a timely manner. (Eight of these individuals still retained access to other Critical Cyber Assets (CCAs), and the other two should have had their access removed from all CCAs. The durations for these specific issues ranged from 8 to 60 days, with an average duration of 21 days.) Additionally, the entity discovered that it also failed to update the corresponding Critical Cyber Asset (CCA) access lists within 7 calendar days from when the managers requested access to be removed for these 10 individuals. The entity remediated each of these issues as they were identified.

After the entity discovered these failures, it took steps to ensure that authorization records for Bulk Electric System (BES) Cyber Systems were in place as well as to ensure that all authorized access was appropriate. This effort revealed the following five additional issues: (a) First, two existing applications had not been included in both the first and second quarter 2016 Access Reviews; (b) Second, these same applications were not included in the 2015 quarterly Access Reviews; (c) Third, two new applications were not included in the second quarter 2016 Access Review; (d) Fourth, electronic access for a non-shared user account for one application was not removed for a single user within 30 calendar days following termination, although the user was later rehired for a new position (This individual's access was removed 42 days late.); and (e) Fifth, twelve users did not have authorization records to support all of their access. (Ten of these 12 users should have had access. The durations for these individuals ranged from 27 to 76 days, with an average duration of 57 days. For the two who should not have had access, the durations were 35 and 31 days.)

The root cause of these issues was overall process inadequacies. Specifically, the [redacted] team was using a manual process for provisioning and revoking access. Furthermore, the [redacted] team was not included in the process for implementing new applications, which left them unaware of the need to provision appropriate access. This major contributing factor involves the management practices of workforce management, which includes managing employee permissions and access to assets, and integration, which includes identifying groups that require the exchange of information to accomplish a task.

Risk Assessment

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to have accurate and up-to-date access records is that individuals can retain access when they are no longer authorized to have it (which happened here), which increases the likelihood that one of those people could use that access for improper purposes. Moreover, active, but unused accounts, present additional, unnecessary attack vectors for a cyber-attack. This risk was mitigated in this case by the following factors. First, all of the individuals involved, while no longer requiring access, were still qualified to have that access because they had current background checks and CIP training. Second, only two of the individuals involved maintained Interactive Remote Access after they no longer required it. Third, although the applications were missed in the quarterly reviews, all of the personnel with access were determined to have appropriate and continuous authorized access to these applications. Fourth, the single user whose electronic access was not removed from a single non-shared account for one application within 30 calendar days following a voluntary termination was rehired for a new position. Fifth, of the 12 users who did not have authorization records to support all of their access, only two were determined to not be authorized based on need for the specific access, which was removed. In both cases, the users were still qualified to have the access because they had current background checks and CIP training.

Mitigation

To mitigate this violation, the entity:

1) conducted a meeting with the [redacted] team to reinforce the current access management processes;
2) made the administrators aware that all requests for removal of electronic access to CIP protected Cyber Systems must go through the access request form to ensure the list remains accurate;
3) included the [redacted] team in the [redacted] and the [redacted] team must approve change controls that involve new assets. This will allow [redacted] to be aware of any new application requiring provisioning of access and allow [redacted] to set parameters for such provisioning;
4) performed and will perform a review of all access transactions each business day. This will ensure the list of users with authorized access to CCAs/BES Cyber Systems remains accurate;

[redacted] NOC-2664 $225,000

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
RFC2016016509	CIP-004-3a	R4	Lower	Moderate	3/31/2015 (when the entity first failed to include the applications in the quarterly reviews)	10/5/2016 (the date the entity completed a comprehensive review to ensure that all access information is correct for Critical Cyber Assets/Bulk Electric System Cyber Systems.)	Self-Report	1/31/2017	4/4/2018

5) revised the departmental electronic access review procedure to be utilized as a part of the annual and quarterly review process, to include an additional QA step. This additional step will consist of a second [redacted] analyst confirming that the proper action has been performed for each access review response;
6) assigned to the [redacted] team, sole ownership of account provisioning for all applications within the CIP environment. This will ensure that all requests for access removal are handled in a uniform manner;
7) performed a comprehensive review in order to ensure that all electronic and informational access was correct for all CCAs/BES Cyber Systems;
8) engaged a consultant to review all of [redacted] procedures relative to access management. A comprehensive review of [redacted] procedures was completed to identify short-term and long-term recommendations for improvement; and
9) developed an automated reporting process for streamlining the analysis of user access authorizations for all Cyber Systems within the CIP environment. This process will be used for quarterly and annual access reviews and authorizations.

Other Factors

ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level.

ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.

[redacted] NOC-2664 $225,000

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
RFC2017016917	CIP-007-6	R2	Medium	High	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	11/28/2016 (the date the entity created and implemented security patch workbooks for each of the applications at issue)	Self-Report	3/26/2019	7/8/2019

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

On January 31, 2017 and March 20, 2019, the entity submitted Self-Reports to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R2. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.

In September 2016, while reviewing baseline monitoring reports for unauthorized software changes, the entity discovered several instances where applications that were active on Bulk Electric System Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, or Protected Cyber Assets, were not reviewed for available security patches within the required 35 days.

Specifically, the following software components were installed on system management servers, but were not listed in a security patch workbook: [redacted]. Moreover, the following SCADA-supporting applications were also discovered with no corresponding entry in a security patch workbook: [redacted]. Additionally, during a subsequent Cyber Vulnerability Assessment, the entity discovered that two security patches for a single software application and three security patches for an operating system were released during this time period, and the entity failed to fully assess and apply those patches.

The root cause of this violation was the entity's mistaken assumption that these supporting component applications would be patched with the primary vendor application suite. A contributing factor was the immaturity of the entity's CIP Version 5 program and its new documented processes and tools. The root cause of the additional instance of noncompliance was the responsible individual's failure to update the security patching workbook for the affected application, and the failure to fully complete all actions for patch application. These root causes involve the management practices of asset and configuration management, which includes controlling changes to assets and configuration items, and information management, which includes establishing and maintaining information items.

Risk Assessment

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based (BPS) on the following factors. The risk posed by failing to assess and apply security patches is that it creates the opportunity for infiltration of unauthorized network traffic into the Electronic Security Perimeter (ESP). This risk is not minimal in this case because some of the software applications affected are used to support the SCADA system. The risk is not serious or substantial in this case based on the entity's defense-in-depth strategy and the relatively short duration of the violation. Specifically, the entity deploys several preventative methods such as [redacted]. (The entity's defense-in-depth strategy included [redacted], which were implemented at all times and are considered mitigating factors for this and the other violations included in this agreement. Other elements of the entity's defense-in-depth strategy including physical security controls, [redacted] were also mitigating factors to this and the other violations included in this agreement. However, regarding these other elements, in some cases as described below, there were at isolated times limitations that impacted full implementation (e.g. [redacted]). Even with these isolated limitations, the entity's defense-in-depth elements as a whole continued to function in limiting risks to the BPS.) This preventative strategy ensures that no energy management systems have internet access to or from the ESP. Additionally, the entity also deploys several detective measures such as [redacted] to detect anomalous activity.

Mitigation

To mitigate this violation, the entity:

1) removed [redacted] from the primary Control Center application server;
2) created a security patch workbook and have gone through the security patch review process for [redacted]. The entity added applications to existing security patch workbooks and have also gone through security patch review process for [redacted];
3) initiated work with [redacted] Professional Services to assist with [redacted] configurations for monitoring the CIP-010-2 R1 and R2;
4) removed [redacted] from the backup Control Center application server;
5) performed a [redacted] to [redacted] reconciliation to ensure all assets that are capable of being monitored through [redacted] are configured correctly to do so;
6) created a process for manual monitoring of assets where [redacted] cannot be used;

ReliabilityFirst Corporation (ReliabilityFirst) Settlement Agreement (Neither Admits nor Denies) CIP

[redacted] NOC-2664 $225,000

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
RFC2017016917	CIP-007-6	R2	Medium	High	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	11/28/2016 (the date the entity created and implemented security patch workbooks for each of the applications at issue)	Self-Report	3/26/2019	7/8/2019

7) conducted a manual reconciliation of ports and services in [redacted] as compared to [redacted]
8) conducted a manual reconciliation of the applications in [redacted] as compared to [redacted]
9) conducted a manual reconciliation of installed software patches;
10) fully documented the [redacted] environment and provided templates to users to more easily identify differences in test configurations;
11) documented a process to document, investigate, and report on unauthorized baseline changes for systems being monitored by [redacted]
12) completed whitelist reconfiguration for ports and services, applications, custom applications, operating system/firmware version, and security patches;
13) reviewed, revised, and implemented the necessary changes to the Configuration Change Management procedures;
14) provided user training for any changes to the Configuration Change Management Procedure to the subject matter experts who use the program. Training included updates in the processes; proper documentation of evidence; identification of CIP security controls which may be impacted; documentation of test templates to document the differences in [redacted] and enhancement in the change ticketing process;
15) initiated additional Manual Reconciliation of Applications in [redacted] vs. [redacted] to validate;
16) initiated additional Manual Reconciliation of Ports and Services in [redacted] vs. [redacted] to validate;
17) initiated additional Manual Reconciliation of Patches using Patch workbooks vs. [redacted] to validate;
18) completed manual reconciliation of applications, ports and services and patches;
19) updated the security patch workbook for the additionally-identified software application and upgraded to most recent version;
20) took necessary steps to fully apply operating system patches;
21) updated procedures to include an independent annual validation of patching source contact method and details required; and,
22) updated procedures to require as part of a patch evaluation in the patching workbook, documentation of additional patching steps required if the patch is not enabled by default at patch installation.

Other Factors

ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level.

ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.

[redacted] NOC-2664 $225,000

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
RFC2017016918	CIP-007-6	R3	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	2/28/2017 (Mitigation completion)	Self-Report	2/28/2017	2/1/2018

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On January 31, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R3. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets. As part of ongoing proactive compliance reviews in November 2016, the entity discovered that it failed to include in its system security management documentation, and in practice, a process for updating intrusion detection system (IDS) signatures, the immediate notification through malicious code alerts, and the response activities that should be executed when malware is detected. The IDS is used to monitor the [redacted] network traffic for malicious code [redacted] This monitoring has continued to be utilized even though the signatures have not been updated regularly. The root cause of this violation was the lack of a documented process for updating IDS signatures. This root cause involves the management practice of asset and configuration management, which includes controlling changes to assets and configuration items.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by having outdated IDS signatures is that newer types of malicious code could go undetected. This risk was not minimal because the IDS is used to monitor for malicious code [redacted] and the length of time that the issue persisted. This risk is not serious or substantial based on the following factors. First, the entity identified and corrected the issue through a mock audit within four months of the start date of the noncompliance. Second, the entity designed its network infrastructure in a way that reduces the risk of unauthorized or malicious traffic [redacted]. Specifically, unauthorized or malicious traffic would have to pass through multiple different layers of protection before entering the ESP. First, [redacted] Second, [redacted]. Third, [redacted] Fourth, [redacted] Fifth, [redacted].
Mitigation	To mitigate this violation, the entity: 1) updated the IDS signatures per vendor's white paper on the network IDS; and 2) developed and implemented a process to update signatures for the IDS that includes testing, escalation, and language to show the interface to the Cyber Security Incident Response Plan when malicious code is detected.
Other Factors	ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level. ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. However, with respect to the two violations related to the entity's process for updating intrusion detection system signatures (i.e. [redacted] and

[redacted] NOC-2664 $225,000

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
RFC2017016918	CIP-007-6	R3	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	2/28/2017 (Mitigation completion)	Self-Report	2/28/2017	2/1/2018
			[redacted] ReliabilityFirst considered the latter violation to be a repeat issue because it resulted from the entity's failure to fully mitigate the former violation. For that reason, ReliabilityFirst aggravated the monetary penalty.						

[redacted] NOC-2664 $225,000

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
RFC2018019980	CIP-007-6	R3	Medium	Severe	1/20/2018 (the day after the entity deactivated the account used to run the antivirus instance at the alternate operations center)	4/12/2018 (the date the entity moved the antivirus task to an active account)	Self-Report	2/15/2019	7/7/2019

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 June 27, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R3. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets. While investigating a different issue in [redacted], the entity discovered that it had not updated the antivirus (AV) definitions on [redacted] Windows servers and workstations at its alternate operations center (AOC) since January 19, 2018. [redacted] The entity investigated and concluded that the AV instance at the AOC was attempting to perform the updates under a user account that had been removed from the application on January 19, 2018. Once the action was moved to an active account, the updates were applied. The root cause of the violation was a lack of procedure to identify and track the accounts running the AV update task. The AV application runs on the account that was used to create it or last modified it, so the entity needed to establish controls to ensure that when such an account is deactivated, the associated AV tasks are transferred to another account. This root cause involves the management practice of asset and configuration management, which includes controlling changes to assets and configuration items.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by having outdated AV definitions is that newer types of viruses could go undetected. This risk was not minimal in this case because the issue affected the AOC. Although the entity did not have to fail over to the AOC at any point during the timeframe, if it did have to fail over, this could have presented a bigger risk. The risk was not serious or substantial because the entity was deploying updated AV signatures on its POC, ensuring that it was mitigating those threats. Moreover, the entity has deployed [redacted] to all workstations and servers where technically feasible, which would have alerted to any new software or malware installed or any configuration changes to these systems. The entity confirmed that no security events occurred during the period of this violation.
Mitigation	To mitigate this violation, the entity: 1) recreated the AV task, and all outstanding definitions were applied to the AOC [redacted] servers and workstations; 2) performed a full system antivirus scan in the AOC environment after the antivirus definitions were updated to verify that no identified malicious code existed; 3) implemented a daily health check to validate that antivirus definitions in the CIP environment are being updated in compliance with CIP regulations. On a daily basis, a detailed report generated by [redacted] is reviewed showing the version date of the antivirus definitions on all CIP High Impact [redacted] assets. This report lists all individual nodes and their current status and any associated issues. In addition, an Executive summary dashboard including the status of all CIP High Impact asset [redacted] antivirus protection is also sent to [redacted] Senior Management; 4) restricted all accounts except for AV administrative accounts from having the ability to create or modify AV tasks; 5) engaged a third-party vendor who performed an active vulnerability assessment; 6) completed (third-party vendor) the field work for the active vulnerability assessment; 7) created a process for a method to escalate potential critical malicious security events identified by the entity security tools to the [redacted] team during non-business hours; and 8) reviewed and finalized the vulnerability assessment report including the plan to address any required mitigation actions.
Other Factors	ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level.

[redacted] NOC-2664 $225,000

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
RFC2018019980	CIP-007-6	R3	Medium	Severe	1/20/2018 (the day after the entity deactivated the account used to run the antivirus instance at the alternate operations center)	4/12/2018 (the date the entity moved the antivirus task to an active account)	Self-Report	2/15/2019	7/7/2019
			ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.						

[redacted] NOC-2664 $225,000

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
RFC2018019981	CIP-007-6	R3	Medium	Severe	3/2/2017 (the date the entity first failed to apply updated intrusion detection signatures)	6/19/2018 (the date the entity applied updated signatures and actually implemented the email notifications in the software tool)	Self-Report	4/22/2019	10/22/2019

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 June 27, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R3. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.

On May 16, 2018, while verifying system security protections, the entity discovered that network intrusion detection system (IDS) signature reviews and updates were not being performed according to company policy. IDS signature updates were not applied to the primary operations center (POC) network during the 3rd quarter of 2017 and the 1st quarter of 2018, and were not applied to the alternate operations center (AOC) network during the 3rd and 4th quarter of 2017 and the 1st quarter of 2018.

The root cause of the violation was the entity's failure to properly configure notifications in its corresponding software system. The entity's processes for reviewing and updating IDS signatures included a [redacted], but they were never implemented. This root cause involves the management practice of asset and configuration management, which includes controlling changes to assets and configuration items, and implementation, because the entity failed to properly implement its process.

Risk Assessment

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by having outdated IDS signatures is that newer types of malicious code could go undetected. The risk is not minimal in this case because the issue affected the POC and AOC for several quarters. The risk is not serious or substantial due to the entity's defense-in-depth strategy. Specifically, the entity designed its network infrastructure in a way that reduces the risk of unauthorized or malicious traffic [redacted]. In other words, unauthorized or malicious traffic would have to pass through multiple different layers of protection before entering the ESP. First, [redacted] Second, [redacted] Third, [redacted] Fourth, [redacted] Fifth, [redacted].

Mitigation

To mitigate this violation, the entity:

1) developed a [redacted] report that displays the install date and current version of the IDS signatures which are reviewed on a daily basis to ensure signatures are within the current quarter;
2) updated the network with the May 17, 2018 IDS signatures updates;
3) created automated reminders for the quarterly review and implementation of IDS signature updates and sent to the supervisors of [redacted] and [redacted];
4) engaged a third-party vendor who performed an active vulnerability assessment;
5) updated the current system security management process and the IDS signature update procedure to require mitigation plans and approvals when IDS signature updates cannot be applied within the required period;
6) collaborated and developed a process for evaluating IDS signature updates whenever they are made available. IDS signature updates categorized as critical will be expedited and installed outside of the normal quarterly IDS signature update process;
7) completed (third-party vendor) field work for the active vulnerability assessment; and
8) reviewed and finalized the vulnerability assessment report including the plan to address any required mitigation actions.

Other Factors

ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the

[redacted] NOC-2664 $225,000

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
RFC2018019981	CIP-007-6	R3	Medium	Severe	3/2/2017 (the date the entity first failed to apply updated intrusion detection signatures)	6/19/2018 (the date the entity applied updated signatures and actually implemented the email notifications in the software tool)	Self-Report	4/22/2019	10/22/2019

entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level.

ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. However, with respect to the two violations related to the entity's process for updating intrusion detection system signatures (i.e., [redacted] and [redacted] ReliabilityFirst considered the latter violation to be a repeat issue because it resulted from the entity's failure to fully mitigate the former violation. For that reason, ReliabilityFirst aggravated the monetary penalty.

[redacted] NOC-2664 $225,000

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
RFC2017016919	CIP-007-6	R4	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	1/31/2017 (the date the entity corrected the issue and reviewed all logs to ensure no anomalous activity occurred)	Self-Report	1/31/2017	2/1/2018

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On January 31, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R4. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets. In preparation for EOP-008 failover testing from the primary operations center (POC) to the alternate operations center (AOC), the entity discovered an improper configuration within the secondary instance of [redacted]) located at the AOC. Due to this misconfiguration, the entity failed to generate alerts for security events and to review the security event logs at the requisite time intervals for certain CIP devices at the AOC. ([redacted].) Logs were collected by the secondary instance of [redacted] but were not forwarded to the primary instance of [redacted] at the POC for review by the appropriate team. The root cause of the violation was a misconfiguration of [redacted] combined with a failure to verify that the secondary instance of [redacted] was properly configured. This root cause involves the management practice of implementation, because the entity failed to properly implement the secondary instance of [redacted] and verification, because the entity failed to verify proper implementation.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to generate alerts for security events and to review security event logs at the requisite time intervals is that security incidents may go unidentified, leaving the entity's system at risk of compromise. This risk was mitigated in this case by the following factors. First, the AOC is not always in operation, so the affected devices generate a very small number of security event logs. Second, the entity's defense-in-depth strategy mitigates the risk of security incidents occurring. For example, the entity's preventative controls include [redacted] The entity also [redacted]
Mitigation	To mitigate this violation, the entity: 1) redirected any device that was reporting to the AOC [redacted] instance to the primary [redacted] instance; 2) configured the [redacted] to also send their logs to an additional syslog server; 3) imported all logs for the impacted [redacted] into the primary operations center's [redacted] instance. When the spooled logs were imported to the primary [redacted] the logs were immediately processed and started to generate alerts. These alerts were reviewed for any anomalous events and none were identified; 4) gathered logs from the impacted [redacted] and imported into a security tool to manually review for any security events. No anomalous events were detected; 5) reconfigured the IP addresses on the [redacted] to send their logs directly to the primary [redacted] and 6) reviewed the logs from the impacted switches and no anomalous events were identified.
Other Factors	ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level.

[redacted] NOC-2664 $225,000

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
RFC2017016919	CIP-007-6	R4	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	1/31/2017 (the date the entity corrected the issue and reviewed all logs to ensure no anomalous activity occurred)	Self-Report	1/31/2017	2/1/2018
			ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.						

[redacted] NOC-2664 $225,000

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
RFC2017016924	CIP-007-6	R4	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	4/15/2017 (Mitigating Activities completion)	Self-Report	4/15/2017	2/1/2018

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

On January 31, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R4. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.

The entity utilizes [redacted] as its primary tool to log events for identification of Cyber Security Incidents including detected successful login attempts, detected failed access attempts, failed login attempts, and detection of malicious code. The entity experienced various challenges with the implementation of [redacted] during its CIP Version 5 transition efforts, including issues with logging of events, generating alerts, retention of event logs, and the review of logged events every 15 calendar days. The entity identified these issues as violations of CIP-007-6 R4 during proactive compliance reviews and a mock audit.

First, the entity discovered that it failed to include all asset types capable of logging in its [redacted] implementation. Additionally, [redacted] at the backup control center were not configured or connected to [redacted] The root cause of this instance of the violation was the fact that the vendor incorrectly validated that the logs were being captured and being directed to the Security Incident and Event Management System (SIEM) for review and the failure of the entity to verify the technical implementation of [redacted]

Second, the entity failed to generate immediate notification of alerts for detected malicious code and unsuccessful login attempts. Alerting for malicious code by [redacted] was not being sent to the SIEM; rather it was being presented in a report every 24 hours to [redacted] for review from implementation to January 12, 2017. The root cause of this instance of the violation was the lack of a process to document consistent review of the entity's anti-virus console and associated events.

Third, the entity did not consistently configure the log retention periods for asset types which were not reporting through [redacted] for 90 calendar days from implementation of [redacted] The root cause of this instance of the violation was the entity's failure to have a manual process to retrieve the logs for the retention period of the devices' capabilities.

Fourth, the entity failed to review the logs from High Impact Bulk Electric System Cyber Systems at intervals no greater than 15 calendar days for the devices that had been misconfigured in [redacted] and for the devices that needed to have logged events reviewed manually since the implementation of [redacted] The root cause of this instance of the violation was the failure to implement manual monitoring processes that took into account the requirement for those assets which were unable to report to [redacted]

The root causes of these instances of the noncompliance involve the management practices of reliability quality management, which includes maintaining a system for identifying and deploying internal controls, and external interdependencies, in that the entity failed to validate the vendor's work.

Risk Assessment

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to properly capture and review logs is that it may impede the entity's ability to identify and investigate Cyber Security Incidents. This risk was mitigated in this case by the fact that the issue only affected a small number of devices, which reduces the potential exposure. Further, the entity's defense-in-depth strategy mitigates the risk of security incidents occurring. For example, the entity's preventative controls include [redacted]. The entity also [redacted] ReliabilityFirst also notes that the entity determined that no Cyber Security Incidents actually occurred during the time of this violation.

Mitigation

To mitigate this violation, the entity:

1) initiated work with [redacted] Professional Services to assist with [redacted] configuration for event logging;
2) documented a comprehensive review of logging activities for all asset types with their capability;
3) reconfigured [redacted] for event logging where it had previously been misconfigured. Also, the devices that were omitted in the initial implementation were configured for logging in [redacted] Log Center;
4) created a manual review process for devices that are not able to be configured in [redacted]. The process will include retention and review;

[redacted] NOC-2664 $225,000

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
RFC2017016924	CIP-007-6	R4	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	4/15/2017 (Mitigating Activities completion)	Self-Report	4/15/2017	2/1/2018
			5) updated the system security management process with reference to the new manual review process for devices that are not able to be configured in [redacted]; and 6) implemented SIEM Ticket Tracking as part of the [redacted] Professional Services engagement to ensure appropriate workflow and review of event logs.						
Other Factors			ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level. ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.						

[redacted] NOC-2664 $225,000

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
RFC2017018532	CIP-007-6	R4	Medium	Severe	4/14/2017 (the date the entity installed the affected components)	12/15/2017 (Mitigating Activities completion)	Self-Report	12/15/2017	5/3/2018

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On October 18, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R4. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets. In June 2017, while investigating Syslog issues with a device, the entity discovered that it failed to comply with the security event monitoring requirements on [redacted] components that make up the [redacted] including the [redacted] The [redacted] is a [redacted] and is technically capable of logging security events, but the entity failed to configure it at the time of installation to send Syslog messages for security event review and to detect the failure of logging events. Additionally, the entity implemented the components of the [redacted] without completing the required cyber security controls testing. The root cause of this violation was the lack of knowledge by the entity's subject matter experts of the technical capabilities of the new assets and the applicable compliance requirements. This root cause involves the management practices of implementation, in that the violation arose out of the improper configuration of devices at installation, and workforce management, which includes providing training, awareness, and education to employees.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The risk posed by failing to send Syslog messages for security event review is that it hinders the entity's ability to identify a cyber-attack in progress. This risk was mitigated in this case by the following factors. First, the affected assets are protected physically inside the Physical Security Perimeter, access to which is restricted to a limited group of personnel with knowledge of the [redacted] Second, the affected assets are protected electronically within the Electronic Security Perimeter, [redacted]. Third, the [redacted] equipment does not have a 15-minute impact on the BPS.
Mitigation	To mitigate this violation, the entity: 1) worked with vendor support to deploy the functionality that limits [redacted] 2) implemented new protocols and functionality to capture security events and authentication attempts; 3) augmented the CIP change management process to include a review of any new asset type to validate the security capabilities are understood and documented before the installation and implementation of the devices into the entity CIP environment. This will facilitate comprehensive identification of Technical Feasibility Exceptions, setup and authorization for shared accounts, initiation of security events and configuration monitoring, and other required security controls; and 4) provided training to subject matter experts about the additions to the CIP change management process for new asset types.
Other Factors	ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level. ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.

[redacted] NOC-2664 $225,000

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
RFC2017016920	CIP-007-6	R5	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	2/28/2017 (Mitigating Activities completion)	Self-Report	2/28/2017	2/1/2018

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

On January 31, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R5. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.

During a mock audit in November 2016, the entity discovered the following issues related to system access controls: 1) the entity did not properly enforce password complexity for two (2) applications, 2) the entity did not change the default passwords for two (2) service accounts prior to implementation in production, and 3) the entity did not change one (1) service account's password within fifteen (15) calendar months.

With respect to the first issue, the entity failed to configure [redacted] and the [redacted] tool to enforce password complexity. The entity uses [redacted] to reset and enforce complex passwords for certain field devices. However, during the mock audit, the entity discovered that it had not configured [redacted] to enforce complex passwords on the field devices from implementation (May 2016) until December 2016. Notably, even though [redacted] was not enforcing complex passwords during this time, the entity confirmed that all but one of the field devices actually had complex passwords. The password for that one device was not complex for 15 calendar days, from December 6, 2016, through December 21, 2016. The root cause of this issue was a miscommunication between the consultants who configured the [redacted] application and the entity's IT group responsible for ongoing support, who mistakenly assumed that the appropriate settings had been configured at initial setup.

The entity uses the [redacted] tool to control certain user accounts on [redacted] machines. During the mock audit, the entity discovered that it failed to configure this tool to enforce complex passwords for 4 individuals on the entity's [redacted] team from implementation, March 18, 2016 to January 18, 2017. However, the entity confirmed that these 4 individuals actually did have complex passwords because they followed the written guidelines for always using complex passwords. The root cause of this issue was a problem during implementation. The password complexity parameters were properly configured prior to implementation, but they were modified while correcting a different issue, and the entity failed to reset the complexity parameters prior to implementation.

The entity also discovered that one local [redacted] account and two [redacted] shared accounts, which did not have the ability to have complex passwords technically enforced, did not have written procedures for these specific account types to enforce the use of complex passwords procedurally.

With respect to the second issue, the entity failed to change the default password for 2 Supervisory Control and Data Acquisition (SCADA) service accounts on [redacted] servers that were part of the image configuration and required by the vendor at implementation. The root cause of this instance of the violation was the lack of a documented procedure for managing these types of accounts.

With respect to the third issue, the entity failed to change the password for one SCADA [redacted] service account within the requisite 15 calendar month time frame. The root cause of this instance of the violation was a misunderstanding by the entity that the 15 calendar month time frame began to run from the date the device was put into production, as opposed to the build date.

The root causes of these issues involve the management practices of implementation, in that many of these instances arose from problems during the implementation of new devices, asset and configuration management, which includes controlling changes to assets and configuration items, and workforce management, which includes providing training, education, and awareness to employees.

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 based on the following factors. The risk posed by failing to properly enforce complex passwords and to change them in a timely manner is that the passwords could be used to exploit the corresponding accounts and cyber assets. This risk was mitigated in this case by the following factors. First, even though procedural and technical controls were not in place to enforce password complexity, all but one of the affected passwords actually were complex, minimizing the risk that they could be compromised. Second, the only password that was not complex was only in that state for three weeks, and password history showed that only one employee in good standing logged onto that device during that period of time. Third, the ability to access either of the two accounts using the default passwords required a user to either have [redacted]. Fourth, the entity's defense-in-depth strategy also provides multiple layers of protection around the affected devices. ReliabilityFirst also notes that the two service accounts with default passwords were never used or accessed during the period involved.

[redacted] NOC-2664 $225,000

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
RFC2017016920	CIP-007-6	R5	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	2/28/2017 (Mitigating Activities completion)	Self-Report	2/28/2017	2/1/2018

Mitigation	To mitigate this violation, the entity: 1) configured [redacted] to enforce password complexity on the medium impact field devices and verified that the passwords are complex; 2) configured the [redacted] tool to enforce password complexity; 3) reset and disabled the two SCADA service account default passwords; 4) submitted Technical Feasibility Exceptions for [redacted] for assets not technically feasible to meet the requirements of CIP-007 R5.7; 5) developed a documented procedure to manage SCADA vendor services accounts; 6) implemented a documented procedure detailing how the entity will procedurally enforce complexity for the two [redacted] shared accounts; 7) implemented a documented procedure detailing how the entity will procedurally enforce complexity on the local [redacted] password; and 8) established a documented process to review quarterly the password policies for high and medium impact assets to confirm the password parameters are configured for complexity.
Other Factors	ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level. ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.

[redacted] NOC-2664 $225,000

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
RFC2017018530	CIP-007-6	R5	Medium	Severe	4/14/2017 (the date the entity placed the components into production)	10/25/2017 (the date the entity submitted the Technical Feasibility Exceptions)	Self-Report	12/15/2017	5/3/2018

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

On October 18, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R5. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.

In July 2017, while preparing material change reports, the entity failed to file Technical Feasibility Exceptions (TFEs) for two of the [redacted] components of the [redacted] ([redacted] at the Alternate Operations Center (AOC), which was implemented on [redacted]. The [redacted] for the AOC. The [redacted] components are classified as High Impact Bulk Electric System Cyber Assets and are located inside the Electronic Security Perimeter (ESP), which is inside a Physical Security Perimeter (PSP).

[redacted]. These components do not have the capability to limit the number of unsuccessful attempts and generate alerts, requiring the submittal of a TFE.

The root cause of the entity's failure to submit the TFEs was the entity's failure to follow its TFE process. The person who initiated the process sent the initiating request to the wrong department for processing, and the recipient did not open the email. This root cause involves the management practice of reliability quality management, which includes maintaining a system for identifying and deploying internal controls.

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 (BPS) based on the following factors. The risk posed by failing to submit the appropriate TFEs is that it could result in responsible personnel being unaware of the components' inability to limit the number of unsuccessful login attempts, and implement mitigating measures to address the technical deficiency, which increases the likelihood that they may miss a potential cyber-attack. This risk was mitigated in this case by the following factors. First, the affected components have multiple layers of electronic security. For example, [redacted] Second, the affected components are also protected physically through Physical Access Control Systems that [redacted]. Furthermore, physical access requires [redacted]. Third, the [redacted] equipment does not have a 15-minute impact on the BPS.

Mitigation

To mitigate this violation, the entity:

1) completed validation of the components of the [redacted] for applicable TFEs by searching vendor documentation and completing an analysis worksheet for the TFEs;
2) filed the appropriate TFEs for the [redacted] components;
3) augmented the CIP change management process to include a review of any new asset type to validate that the security capabilities are understood and documented before the installation and implementation of the devices into the entity CIP environment. This will facilitate comprehensive identification of TFEs, setup and authorization for shared accounts, initiation of security events and configuration monitoring, and other required security controls; and
4) provided training to subject matter experts about the additions to the CIP change management process for new asset types.

Other Factors

ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level.

ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.

[redacted] NOC-2664 $225,000

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
RFC2017018533	CIP-007-6	R5	Medium	Severe	4/14/2017 (the date the entity placed the components into production)	3/21/2019 (Mitigating Activities completion)	Self-Report	3/21/2019	5/16/2019

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 18, 2017 and March 21, 2019, the entity submitted Self-Reports to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R5. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.

On August 22, 2017, during a paper vulnerability assessment for the [redacted] ([redacted] the entity identified several issues with CIP-007-6 R5, affecting 3 components of the [redacted] including [redacted]s. The issues were as follows: (a) The shared account passwords were not identified or inventoried in the password management system; (b) The two employees who knew the passwords [redacted] did not have authorization records for the use of the shared accounts, although they both had current CIP background checks, current CIP training, and authorization for physical access; (c) Neither technical nor procedural controls were in place to enforce password complexity or length requirements, although the passwords did actually meet those requirements; (d) Changes to passwords were not being technically or procedurally enforced although it was technically feasible; and (e) the functionality to limit the number of unsuccessful authentication attempts, or generate corresponding alerts, had not been configured on the [redacted] Even though the [redacted] was logging, it did not have [redacted] implemented to limit authentication attempts or allow central authentication. The [redacted] configuration to send authentication alerts to the Syslog was not established.

Subsequently, the entity conducted an extent of condition review and discovered additional issues with CIP-007-6 R5. Specifically, the entity discovered [redacted] unique enabled accounts spread across [redacted] Cyber Assets that were not previously identified or inventoried. The local accounts are associated with software applications installed on High Impact Cyber Assets in the entity's CIP environment. Seven of these accounts were shared accounts capable of interactive user access to software applications, but were not inventoried and tracked in the entity's password management system, which would have identified the account name and authorized users. The remaining local accounts are associated with software applications installed on High Impact Cyber Assets in the entity's CIP environment. Additionally, the entity discovered another [redacted] interactive user accounts on which it did not technically or procedurally enforce password changes at least once every 15 calendar months.

The root cause of this violation was a combination of process gaps and administrative errors. First, with respect to process gaps, the entity did not have sufficient processes in place around the verification of accounts during the addition/removal of software applications. The result was that when the entity added or removed software applications, it failed to identify how that change impacted the associated accounts. Second, with respect to the administrative errors, several accounts were not properly identified or inventoried due to lack of awareness on the part of the responsible individual. This root cause involves the management practices of reliability quality management, which includes maintaining a system for deploying internal controls, and workforce management, which includes providing training, education, and awareness to employees.

Risk Assessment

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. The risk posed by these various issues with shared accounts is that they impede the entity's ability to detect whether an unauthorized individual had compromise these assets, and if so, what actions that person may have taken. The risk is not minimal in this case considering the duration that the issue persisted and the number of assets affected. The risk is not serious in this case based on the following factors. First, the affected components have multiple layers of electronic security. For example, the entity's electronic defense includes [redacted]. Second, the affected components are also protected physically through Physical Access Control Systems that [redacted] Furthermore, physical access requires [redacted]. Third, the [redacted] equipment does not have a 15-minute impact on the BPS.

Mitigation

To mitigate this violation, the entity:

1) established the shared account passwords in the password management system and [redacted] groups were created by [redacted];
2) submitted an access request for the employee who assumed responsibility for the [redacted] The request was approved for authorized access to the shared accounts;
3) developed and approved a procedure for password changes for the [redacted] that includes password length and complexity;
4) worked with vendor support to deploy the functionality that limits the number of unsuccessful authentication attempts and to generate alerts after a threshold of unsuccessful authentication attempts on the [redacted] This includes configuring the [redacted] for [redacted]
5) augmented the CIP change management process to include a review of any new asset type to validate the security capabilities are understood and documented before the installation and implementation of the devices into the entity CIP environment. This will facilitate comprehensive identification of Technical Feasibility Exceptions, setup and authorization for shared accounts, initiation of security events and configuration monitoring, and other required security controls; and

[redacted] NOC-2664 $225,000

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
RFC2017018533	CIP-007-6	R5	Medium	Severe	4/14/2017 (the date the entity placed the components into production)	3/21/2019 (Mitigating Activities completion)	Self-Report	3/21/2019	5/16/2019

	6) provided training to subject matter experts about the additions to the CIP change management process for new asset types; 7) reviewed all newly identified accounts to confirm whether they are needed; 8) Deleted/disabled unneeded accounts and changed passwords (where applicable) for needed accounts and stored credentials in entity's password management solution; 9) sent email communication to all affected personnel to emphasize the importance of identifying local application accounts when new cyber assets are added to the entity's CIP environment and verifying security controls when making a baseline configuration change; and, 10) updated configuration monitoring system to include monitoring of local accounts – any modification, deletion, or addition of a local account will be reported to and reviewed by the identity [redacted].
Other Factors	ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level. ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.

[redacted] NOC-2664 $225,000

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
RFC2016016473	CIP-007-3a	R6	Medium	Severe	4/2/2016 (when the Standard became mandatory and enforceable on the entity)	12/2/2016 (Mitigating Activities completion)	Self-Report	12/2/2016	7/26/2017

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 31, 2016, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-3a R6. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets. On September 9, 2016, while reviewing available logs, the entity discovered that the logging and alerting functions on [redacted] experienced several intermittent outages during April and June 2016. First, on April 2-4, 2016, the logging function on [redacted] failed due to higher than expected demand for electronic storage that exceeded the available storage capacity. The entity was not immediately notified of this failure because it had not installed an alerting tool, or a system-health monitoring tool, when it implemented [redacted] [redacted] experienced other intermittent outages from April 9-16, 2016, and June 1-6, 2016, due to the fact that [redacted] was generating significant numbers of event logs that affected [redacted] performance. For [redacted], the entity had an established manual process to capture event logs and review them. However, the [redacted] could not be retained locally, so the entity was unable to capture and retain applicable [redacted] event logs during these intermittent outages. Additionally, although the entity was able to recover local logs for the [redacted] devices, the entity failed to review those logs within 15 calendar days due to a corrupted database and the fact that cyber security personnel were heavily engaged in the recovery of those logs. The root cause of the violation was a tuning issue with [redacted] When the entity installed [redacted] it did not configure it to limit the number of generated log events to those that are relevant and needed for compliance and security. This root cause involves the management practice of implementation, because the issue arose at the installation of [redacted] and information management, which includes managing the risk of a particular piece of information.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by not capturing and reviewing security event logs is that it reduces the entity's awareness of potential security issues. Had the entity's system been compromised during this time, the lack of logs would have impeded their investigation and response. This risk was mitigated in this case by the following factors. First, during these intermittent logging outages, alerts were still being sent to the cyber security console and were being reviewed [redacted] to determine if any were unresolved alerts that would need to be escalated. Second, even though [redacted] logs were not being captured during these intermittent outages, the [redacted] themselves were still actively functioning to allow only authorized [redacted] into the CIP environment. Third, other [redacted] functions, including configuration monitoring, continued to function during this time and would have identified any changes to the [redacted] configurations. ReliabilityFirst also notes that the entity's subsequent review of the logs did not identify any unusual events.
Mitigation	To mitigate this violation, the entity: 1) isolated, upon discovery, the corrupted database. Additional storage was added to continue logging events. Manual recovery of event logs from the collection points was initiated where available; 2) added a system health monitoring tool to [redacted] after the first outage to alert systems operations when [redacted] is not actively monitoring or when there is low availability of storage for event log retention; 3) engaged the [redacted] vendor to assist in tuning the application to identify operational efficiencies and filter out logs that were not necessary for compliance or security, but were causing excessive amounts of logs; 4) made projections using the historical volume of event logs being generated, and a significant volume of storage was purchase and added. This would allow [redacted] to reduce or eliminate the need for further interruptions to the event logging and reviews due to storage needs; 5) completed a review of all available logs. The review included spooled and non-spooled syslogs and recovered [redacted] logs. The entity purchased a tool to aid in the evaluation of the logged events from the corrupted database. No cyber event escalation was required from the review; 6) developed and implemented a manual process to monitor logs when there are dropped packets or when there is a planned or unplanned outage; and 7) implemented an alternate means of collecting [redacted] logs in the event that [redacted] were to experience a planned or unplanned outage. This would allow the event logs to be reviewed per the manual process.
Other Factors	ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the

[redacted] NOC-2664 $225,000

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
RFC2016016473	CIP-007-3a	R6	Medium	Severe	4/2/2016 (when the Standard became mandatory and enforceable on the entity)	12/2/2016 (Mitigating Activities completion)	Self-Report	12/2/2016	7/26/2017
			entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level. ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.						

[redacted] NOC-2664 $225,000

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
RFC2017016922	CIP-010-2	R1	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	3/20/2019 (Mitigating Activities completion)	Self-Report	3/20/2019	7/8/2019

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On January 31, 2017 and March 20, 2019, the entity submitted Self-Reports to ReliabilityFirst stating that, [redacted] it was in violation of CIP-010-2 R1. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets. As background, as part of its CIP Version 5 transition efforts, the entity implemented two new tools related to change management and baselines. First, the entity implemented the [redacted] system as the system of record for configuration baselines. Additionally, the entity implemented [redacted] to monitor the baselines and report on all changes to the baselines in accordance with CIP-010-2 R2. Prior to implementation of these tools, the entity established configuration baselines in the [redacted] system through system scans and vendor documentation. The entity then had a third-party contract validate the correct configuration baselines prior to go-live. However, upon implementation of [redacted] concerns arose over the validity of these records in [redacted] because of the volume of event records being produced by [redacted] Essentially, subject matter experts were expected to reconcile all of the change records produced by [redacted] with the baselines in [redacted] This situation created concern over the validity of the records contained in [redacted] Accordingly, the entity conducted reviews of the system and identified several insufficiencies. Specifically, the entity identified the following issues: (a) instances of incorrect or missed ports and services and software in the [redacted] system; (b) instances of incomplete documentation of deviations from the existing baseline configurations; and (c) instances of missed baseline updates within 30 days of implementing the change. The root cause of this violation was the immaturity of the entity's CIP Version 5 program and related processes and tools. Specifically, subject matter experts did not have enough time and exercise to properly learn and tune [redacted] prior to implementation. This root cause involves the management practices of implementation, in that the issue was related to the implementation of new tools, and workforce management, which includes providing training, education, and awareness to employees.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to properly perform change and baseline management is that it can impede the entity's ability to know if an unauthorized individual had made any changes to the system, and it may cause issues with future authorized changes if they are assessed and implemented based on outdated information. The risk is not minimal in this case considering the length of time that the issue was present and the broad scope of the issue. The risk is not serious or substantial in this case based on the following factors. First, with respect to the risk of an unauthorized individual making changes to the system, the entity protects its system using a variety of defense-in-depth tools such as [redacted]. Second, with respect to the risk of making future authorized changes based on outdated information, during the time that this issue persisted, the entity employed a change management process that included a [redacted] to review and authorize change requests and to provide general oversight of the change management program. From the go-live date of [redacted] through January 2017, the [redacted] processed over [redacted] change requests. Although this review did not provide complete certainty and accuracy of all changes, it was nevertheless a mitigating factor.
Mitigation	To mitigate this violation, the entity: 1) initiated work with [redacted] Professional Services to assist with [redacted] configurations for monitoring the CIP-010-2 R1 and R2; 2) performed a [redacted] to [redacted] reconciliation to ensure all assets that are capable of being monitored through [redacted] are configured correctly to do so; 3) created a process for the manual monitoring for any systems where [redacted] cannot be used; 4) conducted a manual reconciliation of ports and services in [redacted] as compared to [redacted] 5) conducted a manual reconciliation of the applications in [redacted] as compared to [redacted] 6) conducted a manual reconciliation of installed software patches; 7) fully documented the [redacted] environment and provided templates to users to more easily identify differences in test configurations; 8) documented a process to document, investigate, and report on unauthorized baseline changes for systems being monitored by [redacted] 9) completed whitelist reconfiguration for ports and services, applications, custom applications, operating system/firmware version, and security patches; 10) reviewed, revised, and implemented the necessary changes to the Configuration Change Management procedures;

[redacted] NOC-2664 $225,000

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
RFC2017016922	CIP-010-2	R1	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	3/20/2019 (Mitigating Activities completion)	Self-Report	3/20/2019	7/8/2019

	11) provided user training for any changes to the Configuration Change Management Procedure to the subject matter experts who use this program. Training included updates in the processes; proper documentation of evidence; identification of CIP security controls which may be impacted; documentation of test templates to document the differences in [redacted]; and enhancement in the Change ticketing process; 12) initiated additional manual reconciliations of applications in [redacted] vs. [redacted] to validate; 13) initiated additional manual reconciliation of ports and services in [redacted] vs. [redacted] to validate; 14) initiated additional manual reconciliation of patches using Patch workbooks vs. [redacted] to validate; 15) completed manual reconciliation of applications, ports and services, and patches; and, 16) sent an email communication to affected personnel emphasizing the importance of determining and providing all applicable baseline configuration attributes associated with any new cyber asset for inclusion in [redacted]
Other Factors	ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level. ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.

[redacted] NOC-2664 $225,000

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
RFC2017016923	CIP-010-2	R2	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	10/27/2017 (Mitigating Activities completion)	Self-Report	10/27/2017	4/13/2018

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

On January 31, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-010-2 R2. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.

As background, as part of its CIP Version 5 transition efforts, the entity implemented two new tools related to change management and baselines. First, the entity implemented the [redacted] system as the system of record for configuration baselines. Additionally, the entity implemented [redacted] to monitor the baselines and report on all changes to the baselines in accordance with CIP-010-2 R2.

However, through a proactive spot check and mock audit in November 2016, the entity discovered that it failed to load [redacted] software agents on certain devices and that it lacked documentation to demonstrate whether the devices were capable of hosting the [redacted] agent. The entity also discovered that it did not have a detailed process in place to consistently monitor the devices without a [redacted] software agent.

Specifically, the entity determined that the following assets could not host the [redacted] software agent, but could have their baselines monitored by [redacted] through an automatic process without an agent: [redacted]. Moreover, the entity determined the following assets could not host the [redacted] software agent and required a manual process to monitor the baseline configurations: [redacted]

Additionally, the entity further expanded the scope of this noncompliance by noting that during the same process review, it discovered tuning issues with [redacted] that impeded the entity's ability to monitor and document unauthorized changes at least every 35 days. (The entity identified this issue in a self-report submitted on August 30, 2018.) The problem was that [redacted] was generating voluminous records every day and cybersecurity personnel could not review them within the required timeframe. The volume of records generated by [redacted] was due to the fact that the [redacted] reports included a significant amount of unnecessary information not relevant to the CIP configuration baselines.

The root cause of this violation was the improper implementation of the [redacted] tool. The entity failed to install [redacted] software agents on devices and did not spend enough time learning the tool and understanding how to apply it in its environment before implementation. This root cause involves the management practice of implementation.

Risk Assessment

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by failing to monitor devices for unauthorized changes is that the entity could be unaware of adverse changes occurring on its system. This risk is not minimal in this case considering the length of time that the issue was present and the broad scope of the issue. The risk is not serious or substantial in this case based on the following factors. First, for assets enrolled in [redacted] the tuning issues impeded, but did not prevent, the entity's ability to perform the reconciliations within 35 days. In fact, the entity did complete all of the reconciliations for enrolled assets and identified no anomalous or unapproved changes during the time that this issue persisted. Second, the entity protects its system using a variety of defense-in-depth tools such as [redacted]. Furthermore, the entity also deploys several detective controls such as [redacted]

Mitigation

To mitigate this violation, the entity:

1) initiated work with [redacted] Professional Services to assist with [redacted] configurations for monitoring of CIP-010-2 R1 and R2;
2) performed a [redacted] to [redacted] reconciliation to ensure all assets that are capable of being monitored through [redacted] are configured correctly to do so;
3) created a process for the manual monitoring for any systems where [redacted] cannot be used;
4) conducted a manual reconciliation of ports and services in [redacted] as compared to [redacted]
5) conducted a manual reconciliation of the applications in [redacted] as compared to [redacted]
6) conducted a manual reconciliation of installed software patches;
7) fully documented the [redacted] environment and provided templates to users to more easily identify differences in test configurations;

[redacted] NOC-2664 $225,000

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
RFC2017016923	CIP-010-2	R2	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	10/27/2017 (Mitigating Activities completion)	Self-Report	10/27/2017	4/13/2018

8) documented a process to document, investigate, and report on unauthorized baseline changes for systems being monitored by [redacted]
9) completed whitelist reconfiguration for ports and services, applications, custom applications, operating system/firmware version and security patches;
10) reviewed, revised, and implemented the necessary changes to the Configuration Change Management procedures;
11) provided user training for any changes to the Configuration Change Management Procedure to the subject matter experts who use this program. Training included updates in the processes; proper documentation of evidence; identification of CIP security controls which may be impacted; documentation of test templates to document the differences in [redacted] and enhancement in the Change ticketing process;
12) initiated additional manual reconciliations of applications in [redacted] vs. [redacted] to validate;
13) initiated additional manual reconciliation of ports and services in [redacted] vs. [redacted] to validate;
14) initiated additional manual reconciliation of patches using Patch workbooks vs. [redacted] to validate; and
15) completed manual reconciliation of applications, ports and services, and patches.

Other Factors

ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level.

ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.

[redacted] NOC-2664 $225,000

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
RFC2017018534	CIP-010-2	R2	Medium	Severe	4/14/2017 (the date the entity implemented the components)	1/25/2018 (Mitigating Activities completion)	Self-Report	1/25/2018	5/3/2018

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	On October 18, 2017 and December 21, 2017, the entity submitted Self-Reports to ReliabilityFirst stating that, [redacted] it was in violation of CIP-010-2 R2. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets. In July 2017, while responding to a 35-day baseline configuration review notice for a different CIP asset, the entity discovered that it failed to monitor the baseline configurations every 35 calendar days for several components of the [redacted] which the entity implemented on [redacted]. Moreover, the entity also discovered that these components were implemented without the required cyber security controls being completed. The affected components, which were all considered Bulk Electric System Cyber Systems, included: [redacted] Subsequently, in November 2017, the entity discovered that it failed to collect all of the required configuration information items on [redacted] devices at the [redacted] for one 35-day interval. The entity's November review did not include custom software. Once the entity obtained the custom software configuration for the [redacted] devices, it discovered no deviations from the previous baseline review. The root cause of the failure to monitor baseline configurations was the lack of knowledge of personnel responsible for implementing the components. The root cause of the failure to perform the required cyber security controls testing prior to implementation was a lack of internal controls in the change management process. These root causes involve the management practices of implementation, because these issues arose during the implementation process, and workforce management, because the responsible personnel lacked the knowledge required to successfully perform the implementation. The root cause of the failure to include custom software in the configuration baselines for [redacted] devices was the fact that the entity did not begin the data collection early enough to address any issues that arose prior to the due date. This root cause involves the management practice of work management.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) based on the following factors. This violation involves two discrete risks. The risk posed by failing to monitor devices for unauthorized changes is that the entity could be unaware of adverse changes occurring on its system. The risk posed by failing to conduct the required cyber security controls testing prior to implementation is that the new devices could have adverse impacts on the entity's system. These risks were mitigated in this case by the following factors. First, an individual would first need either physical or electronic access to these assets in order to make an unauthorized change. The entity controls physical access to these assets through a Physical Security Perimeter that requires [redacted]. The entity controls electronic access to these assets through its Electronic Security Perimeter and a [redacted]. Second, the [redacted] equipment does not have a 15-minute impact on the BPS.
Mitigation	To mitigate this violation, the entity: 1) worked with vendor support to resolve the issues with the tool used to collect configurations so the [redacted] configurations can be captured for review of baseline configuration; 2) implemented the Syslog functionality for the [redacted] to capture security events and authentication attempts that then can be reviewed by [redacted]; 3) augmented the CIP change management process to include a review of any new asset type to validate that the security capabilities are understood and documented before the installation and implementation of the devices into the entity CIP environment. This will facilitate comprehensive identification of Technical Feasibility Exceptions, setup and authorization for shared accounts, initiation of security events and configuration monitoring, and other required security controls; 4) provided training to subject matter experts about the additions to the CIP change management process for new asset types; 5) pursued the collection of the configuration information for the custom application and validated that there were no unauthorized baseline configuration changes since the last collection in October 2017; and 6) developed and implemented an alternative notification and tracking process that will accommodate a rolling 35-day calendar based on the prior task being completed, and provided director level escalation when the task has not been completed within five business days prior to the due date.
Other Factors	ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the

[redacted] NOC-2664 $225,000

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
RFC2017018534	CIP-010-2	R2	Medium	Severe	4/14/2017 (the date the entity implemented the components)	1/25/2018 (Mitigating Activities completion)	Self-Report	1/25/2018	5/3/2018
			entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level. ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes.					

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 Spreadsheet Notices of Penalty 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	RFC2017017060	Yes		Yes	Yes				Yes	Yes				Category 1 – 3 years; Category 2 – 12: 2 years

Filing Date: January 30, 2020

[redacted] NOC-2653 $50,000

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
RFC2017017060	CIP-010-2	R2	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	8/1/2017 (the date the entity completed milestones in its Mitigation Plan necessary to correct all instances of non-compliance)	Self-Report	2/13/2018	10/29/2018

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

On February 16, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [redacted], it was in violation of CIP-010-2 R2.

On November 30, 2016, as part of compliance governance enhancements, the entity's IT [redacted] Team identified device types that were not being properly monitored for baseline configuration changes in accordance with the entity's documented program. This program permitted the use of baseline configurations by device type or group for purposes of the configuration change management activities required by CIP-010-2 R1. While this is permissible under CIP-010-2 R1, the group baseline must accurately reflect the baselines for every individual device within that group.

However, personnel improperly assumed that this same approach could be used for monitoring baselines changes under CIP-010-2 R2. In other words, they incorrectly assumed that monitoring one device within a device type or group would be representative of all devices within that type or group. This is not permitted by CIP-010-2 R2. As a direct result of this error, as changes were made to individual devices within a group, the entity did not identify or update the baseline to reflect these changes across all devices within a device type. Thus, there were discrepancies between individual device baselines and the documented group baselines required by CIP-010-2 R1. (The entity identified this issue in the original self-report. It stemmed from the same errors the entity made in its baseline monitoring program. The entity did not submit a separate self-report because these additional issues were the direct result of the overarching problems with its baseline monitoring program.) Recognizing the error in approach to monitoring individual devices within a device type, the entity's IT [redacted] Team reviewed the baseline monitoring program by performing a full extent of condition review of the entity's configuration monitoring practices, including checking for individual differences in device baseline configurations. Specifically, the entity identified [redacted] device types for which individual device baselines did not match actual device configurations, including:

(a.) [redacted] This device type included multiple devices with the same Operating System, but different functions. Consequently, different software and services were observed.
(b.) [redacted] A list of baseline processes and software was not complete for this device type. As a result, there were instances where a single process or software component was not accounted for.
(c.) [redacted] A list of baseline processes and software was not properly maintained for this device type. In addition, baselines should have been updated after planned baseline impacting changes were performed to the device type.
(d.) [redacted] A list of baseline processes and software was not complete for this device type.
(e.) [redacted] Firmware variances were unique to this device type. Issues were due to the manner in which firmware was documented in the official baseline document.
(f.) [redacted] Software versions were not consistent between baselines and actuals. Additionally, this analysis led to the conclusion that this device type should be separated into another device type.
(g.) [redacted] A list of baseline processes and software was not complete for this device type.
(h.) [redacted] The variances in this device type were primarily due to common software components and processes not being documented in the original baseline. However, there was only one device within this device type, and it has since been retired and is no longer in the NERC CIP environment.
(i.) [redacted]: the entity was performing a major upgrade to the [redacted]. Changes had not been completely implemented across the platform. These changes were all part of the planned upgrade.
(j.) [redacted]: A list of baseline processes and software was not complete for this device type.
(k.) [redacted]: A list of baseline processes and software was not complete for this device type.
(l.) [redacted] The servers were installed at the same point in time. Initial baselines were developed before the system went live. However, the documented baselines were not updated after system hardening activities were performed prior to go live.

Additionally, the entity's errors in its baseline monitoring program also led to additional errors within port setting justifications under CIP-007 R1 and within change authorization under CIP-010 R1. (The entity identified these additional issues in its Self-Report, as they stemmed from the same errors the entity made in its baseline monitoring program. The entity did not submit separate Self-Reports because these additional issues were the direct result of the overarching problems with its baseline monitoring program.) For the port setting issue, the entity identified 11 device types that had missing logical ports documentation, including ports justifications, in systems of record for baseline documentation. For the change authorization issue, the entity identified 10 potential missed change authorization instances where the change management ticket for the planned work was not fully approved before the change was promoted to the production environment.

The root cause of this violation was the lack of clear documentation in the entity's procedure for baseline configuration and management, and a lack of consistent implementation of the entity program that resulted from the lack of clear procedural documentation. This unclear process documentation led employees to make incorrect assumptions regarding configuration baseline monitoring implementation and to create steps contrary to the intent of the procedure. This incorrect monitoring directly led to the additional issues with baseline discrepancies, port justifications, and change authorization. This

[redacted] NOC-2653 $50,000

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
RFC2017017060	CIP-010-2	R2	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	8/1/2017 (the date the entity completed milestones in its Mitigation Plan necessary to correct all instances of non-compliance)	Self-Report	2/13/2018	10/29/2018

	major contributing factor involves the management practices of asset and configuration management, which includes establishing assets and configuration items inventory and controlling changes, implementation, which includes establishing implementation processes, and workforce management, which includes providing training, education, and awareness to employees.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Not monitoring baselines has the potential to affect the reliability of the Bulk Power System (BPS) by reducing the entity's ability to identify unauthorized activity, changes, or vulnerabilities and by introducing system instability when making changes to assets. The entity's inadequate monitoring resulted in issues with maintaining adequate baselines, authorizing changes, and not having justifications for open ports. There are distinct risks associated with each of these issues. First, the risk associated with not maintaining accurate baselines is that the entity may make decisions or take action based on incorrect or outdated information, which could have an adverse impact on the affected devices. Second, the risk associated with executing changes on CIP assets without properly executing change management controls and test procedures could impact the security profile of the system given the way that baselines were managed. [redacted], protecting against potential impacts to the BPS.) Lastly, the entity's failure to document justifications for ports and services required for normal and emergency operations could create decreased awareness in monitoring for and detecting unauthorized changes to necessary ports, but did not introduce an opportunity for unauthorized access through an open communication channel (i.e. there were no unnecessary open ports). However, the risk is not serious and substantial based on several factors. First, the entity detected these issues less than four months after the effective date of the CIP version 5 Standards as part of a pre-planned project to review entity change management processes and device baselines. This relatively prompt detection permitted the entity to conduct a full and exhaustive review to understand the scope and extent of the issue. Second, with respect to the other effective security controls, at the time the entity identified the issue, it had stringent defense-in-depth measures in place to control access and communications and otherwise protect and secure the devices at issue. These defense-in-depth measures include physical security controls, electronic security controls, logical access controls, malicious code prevention, and patching. Third, although the entity discovered some discrepancies in its baselines, it was performing limited baseline management, which reduced the risk that it would make decisions or take action based on incorrect or outdated information. Additionally, the entity was performing reliability testing and security event monitoring on all of these devices during the time period in question, which included logging and alerting events. In short, these security controls reduced the likelihood that any of the affected devices could be compromised as a result of the problem with baseline monitoring.
Mitigation	To mitigate this violation, the entity: 1) changed Management Training of change management tool and compliance change management requirements to entity IT [redacted] including acquiring baseline change approvals in the tool prior to work; 2) created [redacted] cross-business unit (BU) Job Aid(s) with the following criteria: (i) Update with sufficient detail including having IT [redacted] perform the monitoring to ensure a separation of duties; (ii) Include detail for using the NERC CIP asset directory as the source of determining devices in scope for each cycle of baseline monitoring; (iii) Include requirements for documentation of devices within a device type where groupings are used; (iv) Include monitoring all devices within a device type; and (v) The new Job Aid will include the process for change management of revisions, acceptance of the revisions, approvals, and promotion to the proper evidence location; 3) investigated and documented port ranges in baseline documentation and systems for all entity IT devices requiring baselines or Port and Service justification; 4) completed analysis of actual software vs. required software and inventory potential removals. Reviewed the list of potential removals with vendor and obtained approval or rejection for any proposed changes; 5) trained employees on new cross BU Job Aid(s) [redacted]; 6) performed an entity NERC CIP change management meeting reiterating the change management requirements and the importance of adhering to the entity and NERC CIP requirements; including details of what IT changes are required in change management including levels of approval required prior to work being performed; 7) performed new baseline monitoring steps for entity IT based on new Job Aid(s) and created baseline monitoring report and evidence for a cycle. Completed a schedule for subsequent baseline monitoring cycles through the end of the year. Documented lessons learned improvement opportunities and baseline updates required to support subsequent baseline monitoring cycles; 8) replaced documentation that describes the promotion of [redacted] baselines as it relates to change management and to maintain consistency with the NERC CIP asset directory; 9) for any software or services lockdown changes approved by the vendor, performed change management to test, obtained approvals, implemented the change, and updated baselines documentation

[redacted] NOC-2653 $50,000

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
RFC2017017060	CIP-010-2	R2	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable on the entity)	8/1/2017 (the date the entity completed milestones in its Mitigation Plan necessary to correct all instances of non-compliance)	Self-Report	2/13/2018	10/29/2018

with the changes; and
10) conducted quality review and sampling of changes and ongoing performance (baseline updates, authorizations, baseline monitoring).

Other Factors

ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. [redacted] Specifically, ReliabilityFirst determined that over 90% of the [redacted] noncompliance since [redacted] were self-reported. ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the [redacted] report that noncompliance to ReliabilityFirst has decreased significantly since [redacted]

Additionally, ReliabilityFirst recognized the fact that the [redacted] discovered this issue as a result of its effective internal compliance program. Specifically, in preparation for CIP Version 5 implementation, the [redacted] sought to consolidate the individual configuration monitoring processes of each business unit. During that consolidation effort, the [redacted] discovered the current issue at [redacted] only. Moreover, while they do not constitute above and beyond actions, the entity implemented several organizational and procedural enhancements, [redacted], in response to the present issue which are indicative of the entity's strong culture. Specifically, the entity's IT [redacted] engaged the software vendor to address installed software differences to determine whether software could be removed for system hardening. This work was included in the Mitigation Plan and was aimed at reducing the entity's risk profile during mitigation of the issues. During this time, a test cycle of the new configuration monitoring process was deployed. After determining that the new configuration monitoring test cycle was successful, [redacted] deployed the same configuration monitoring program in place at the other business units [redacted], sixty (60) days before its committed completion date in the Mitigation Plan.

Following the completion of the mitigation, the entity also took additional significant steps to further improve compliance oversight in its corporate CIP [redacted] Program. These efforts include resource enhancements to provide dedicated compliance oversight staff assigned to review the work performed by the IT [redacted] team. The additional actions represent an important investment in compliance assurance benefiting the entity. Under the entity's prior structure, [redacted] dedicated Full Time Equivalent personnel (FTEs) were within IT [redacted] and charged with compliance oversight for all CIP standard requirements applicable, including CIP-010. Under the revised [redacted] compliance oversight organization, the entity benefits from an additional five [redacted]

Taken together, these facts are indicative of a strong internal control program focused on preventing, detecting, and correcting noncompliance. Accordingly, ReliabilityFirst awarded mitigating credit for the entity's ICP.

ReliabilityFirst considered the entity's CIP-010-2 R2 compliance history in determining the penalty. ReliabilityFirst determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the prior noncompliance was the result of a different root cause.