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

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.

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;

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.

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] ([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;

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.

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.						

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.						

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

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.

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.						

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;

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.						

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.

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.

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.

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.

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

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.

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.							

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;

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.

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;

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.

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.					