**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 |
|---|---|---|---|---|---|---|---|---|---|
| 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 applying a 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;<br>7) reviewed all newly identified accounts to confirm whether they are needed;<br>8) Deleted/disabled unneeded accounts and changed passwords (where applicable) for needed accounts and stored credentials in entity's password management solution;<br>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,<br>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.<br><br>ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for applying a 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.<br><br>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]<br><br>[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.<br><br>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.<br><br>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:<br><br>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;<br>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;<br>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;<br>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;<br>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;<br>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<br>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.<br><br>ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for applying a 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.<br><br>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.<br><br>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.<br><br>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:<br><br>1) initiated work with [redacted] Professional Services to assist with [redacted] configurations for monitoring the CIP-010-2 R1 and R2;<br>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;<br>3) created a process for the manual monitoring for any systems where [redacted] cannot be used;<br>4) conducted a manual reconciliation of ports and services in [redacted] as compared to [redacted]<br>5) conducted a manual reconciliation of the applications in [redacted] as compared to [redacted]<br>6) conducted a manual reconciliation of installed software patches;<br>7) fully documented the [redacted] environment and provided templates to users to more easily identify differences in test configurations;<br>8) documented a process to document, investigate, and report on unauthorized baseline changes for systems being monitored by [redacted]<br>9) completed whitelist reconfiguration for ports and services, applications, custom applications, operating system/firmware version, and security patches;<br>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;<br>12) initiated additional manual reconciliations of applications in [redacted] vs. [redacted] to validate;<br>13) initiated additional manual reconciliation of ports and services in [redacted] vs. [redacted] to validate;<br>14) initiated additional manual reconciliation of patches using Patch workbooks vs. [redacted] to validate;<br>15) completed manual reconciliation of applications, ports and services, and patches; and,<br>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.<br><br>ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for applying a 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 applying a 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

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