**COVER PAGE**

This filing contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notices of Penalty in this filing and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

| Count | Violation ID | Category 1 | Category 2 | Category 3 | Category 4 | Category 5 | Category 6 | Category 7 | Category 8 | Category 9 | Category 10 | Category 11 | Category 12 | CEII PROTECTION (YEARS) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | RFC2017016915 | Yes | | Yes | Yes | | Yes | | | | Yes | | Yes | Category 1: 3 years; Category 2 – 12: 2 years |
| 2 | RFC2016016509 | Yes | | Yes | Yes | | Yes | | Yes | | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 3 | RFC2017016917 | Yes | | Yes | Yes | | Yes | | Yes | | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 4 | RFC2017016918 | Yes | | Yes | Yes | | Yes | | | | Yes | | Yes | Category 1: 3 years; Category 2 – 12: 2 years |
| 5 | RFC2018019980 | Yes | | Yes | Yes | | Yes | | Yes | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 6 | RFC2018019981 | Yes | | Yes | Yes | | Yes | | Yes | | Yes | | Yes | Category 1: 3 years; Category 2 – 12: 2 years |
| 7 | RFC2017016919 | Yes | | Yes | Yes | | Yes | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 8 | RFC2017016924 | Yes | | Yes | Yes | | Yes | | Yes | | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 9 | RFC2017018532 | Yes | | Yes | Yes | Yes | Yes | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 10 | RFC2017016920 | Yes | | Yes | Yes | | Yes | | Yes | | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 11 | RFC2017018530 | Yes | | Yes | Yes | Yes | Yes | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 12 | RFC2017018533 | Yes | | Yes | Yes | Yes | Yes | | Yes | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 13 | RFC2016016473 | Yes | | Yes | Yes | | Yes | | | | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 14 | RFC2017016922 | Yes | | Yes | Yes | | Yes | | Yes | | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 15 | RFC2017016923 | Yes | | Yes | Yes | | Yes | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 16 | RFC2017018534 | Yes | | Yes | Yes | Yes | Yes | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |

Filing Date: March 31, 2020

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016915 | CIP-002-5.1 | R1 | High | Lower | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 1/26/2017 (the date the entity properly classified the virtual server and included it in the Asset Identification list) | Self-Report | 2/15/2017 | 2/1/2018 |

| | |
|---|---|
| **Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)** | On January 31, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-002-5.1 R1. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in this Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.<br><br>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.<br><br>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:<br><br>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;<br>2) decommissioned the relevant virtual server; and<br>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.<br><br>ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2016016509 | CIP-004-3a | R4 | Lower | Moderate | 3/31/2015 (when the entity first failed to include the applications in the quarterly reviews) | 10/5/2016 (the date the entity completed a comprehensive review to ensure that all access information is correct for Critical Cyber Assets/Bulk Electric System Cyber Systems.) | Self-Report | 1/31/2017 | 4/4/2018 |

| | |
|---|---|
| **Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)** | On November 8, 2016, the entity submitted a Self-Report to ReliabilityFirst stating that, as a [redacted], it was in violation of CIP-004-3a R4. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.<br><br>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.<br><br>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.)<br><br>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:<br><br>1) conducted a meeting with the [redacted] team to reinforce the current access management processes;<br>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;<br>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;<br>4) performed and will perform a review of all access transactions each business day. This will ensure the list of users with authorized access to CCAs/BES Cyber Systems remains accurate; |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2016016509 | CIP-004-3a | R4 | Lower | Moderate | 3/31/2015 (when the entity first failed to include the applications in the quarterly reviews) | 10/5/2016 (the date the entity completed a comprehensive review to ensure that all access information is correct for Critical Cyber Assets/Bulk Electric System Cyber Systems.) | Self-Report | 1/31/2017 | 4/4/2018 |

| | |
|---|---|
| | 5) revised the departmental electronic access review procedure to be utilized as a part of the annual and quarterly review process, to include an additional QA step. This additional step will consist of a second [redacted] analyst confirming that the proper action has been performed for each access review response;<br>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;<br>7) performed a comprehensive review in order to ensure that all electronic and informational access was correct for all CCAs/BES Cyber Systems;<br>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<br>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.<br><br>ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016917 | CIP-007-6 | R2 | Medium | High | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 11/28/2016 (the date the entity created and implemented security patch workbooks for each of the applications at issue) | Self-Report | 3/26/2019 | 7/8/2019 |

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

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

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

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

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

**Risk Assessment**

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

**Mitigation**

To mitigate this violation, the entity:

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

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016917 | CIP-007-6 | R2 | Medium | High | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 11/28/2016 (the date the entity created and implemented security patch workbooks for each of the applications at issue) | Self-Report | 3/26/2019 | 7/8/2019 |
| | | | 7) conducted a manual reconciliation of ports and services in [redacted] as compared to [redacted]<br>8) conducted a manual reconciliation of the applications in [redacted] as compared to [redacted]<br>9) conducted a manual reconciliation of installed software patches;<br>10) fully documented the [redacted] environment and provided templates to users to more easily identify differences in test configurations;<br>11) documented a process to document, investigate, and report on unauthorized baseline changes for systems being monitored by [redacted]<br>12) completed whitelist reconfiguration for ports and services, applications, custom applications, operating system/firmware version, and security patches;<br>13) reviewed, revised, and implemented the necessary changes to the Configuration Change Management procedures;<br>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;<br>15) initiated additional Manual Reconciliation of Applications in [redacted] vs. [redacted] to validate;<br>16) initiated additional Manual Reconciliation of Ports and Services in [redacted] vs. [redacted] to validate;<br>17) initiated additional Manual Reconciliation of Patches using Patch workbooks vs. [redacted] to validate;<br>18) completed manual reconciliation of applications, ports and services and patches;<br>19) updated the security patch workbook for the additionally-identified software application and upgraded to most recent version;<br>20) took necessary steps to fully apply operating system patches;<br>21) updated procedures to include an independent annual validation of patching source contact method and details required; and,<br>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.<br><br>ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. | | | | |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016918 | CIP-007-6 | R3 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 2/28/2017 (Mitigation completion) | Self-Report | 2/28/2017 | 2/1/2018 |

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

On January 31, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R3. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.

As part of ongoing proactive compliance reviews in November 2016, the entity discovered that it failed to include in its system security management documentation, and in practice, a process for updating intrusion detection system (IDS) signatures, the immediate notification through malicious code alerts, and the response activities that should be executed when malware is detected. The IDS is used to monitor the [redacted] network traffic for malicious code [redacted] This monitoring has continued to be utilized even though the signatures have not been updated regularly.

The root cause of this violation was the lack of a documented process for updating IDS signatures. This root cause involves the management practice of asset and configuration management, which includes controlling changes to assets and configuration items.

**Risk Assessment**

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the following factors. The risk posed by having outdated IDS signatures is that newer types of malicious code could go undetected. This risk was not minimal because the IDS is used to monitor for malicious code [redacted] and the length of time that the issue persisted. This risk is not serious or substantial based on the following factors. First, the entity identified and corrected the issue through a mock audit within four months of the start date of the noncompliance. Second, the entity designed its network infrastructure in a way that reduces the risk of unauthorized or malicious traffic [redacted]. Specifically, unauthorized or malicious traffic would have to pass through multiple different layers of protection before entering the ESP. First, [redacted] Second, [redacted]. Third, [redacted] Fourth, [redacted] Fifth, [redacted].

**Mitigation**

To mitigate this violation, the entity:

1) updated the IDS signatures per vendor's white paper on the network IDS; and
2) developed and implemented a process to update signatures for the IDS that includes testing, escalation, and language to show the interface to the Cyber Security Incident Response Plan when malicious code is detected.

**Other Factors**

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

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

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016918 | CIP-007-6 | R3 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 2/28/2017 (Mitigation completion) | Self-Report | 2/28/2017 | 2/1/2018 |
| | | | [redacted] ReliabilityFirst considered the latter violation to be a repeat issue because it resulted from the entity's failure to fully mitigate the former violation. For that reason, ReliabilityFirst aggravated the monetary penalty. | | | | | | |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2018019980 | CIP-007-6 | R3 | Medium | Severe | 1/20/2018 (the day after the entity deactivated the account used to run the antivirus instance at the alternate operations center) | 4/12/2018 (the date the entity moved the antivirus task to an active account) | Self-Report | 2/15/2019 | 7/7/2019 |

| | |
|---|---|
| **Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)** | On June 27, 2018, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R3. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.<br><br>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.<br><br>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:<br><br>1) recreated the AV task, and all outstanding definitions were applied to the AOC [redacted] servers and workstations;<br>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;<br>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;<br>4) restricted all accounts except for AV administrative accounts from having the ability to create or modify AV tasks;<br>5) engaged a third-party vendor who performed an active vulnerability assessment;<br>6) completed (third-party vendor) the field work for the active vulnerability assessment;<br>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<br>8) reviewed and finalized the vulnerability assessment report including the plan to address any required mitigation actions. |
| **Other Factors** | ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level. |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2018019980 | CIP-007-6 | R3 | Medium | Severe | 1/20/2018 (the day after the entity deactivated the account used to run the antivirus instance at the alternate operations center) | 4/12/2018 (the date the entity moved the antivirus task to an active account) | Self-Report | 2/15/2019 | 7/7/2019 |
| | | | ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. | | | | | | |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2018019981 | CIP-007-6 | R3 | Medium | Severe | 3/2/2017 (the date the entity first failed to apply updated intrusion detection signatures) | 6/19/2018 (the date the entity applied updated signatures and actually implemented the email notifications in the software tool) | Self-Report | 4/22/2019 | 10/22/2019 |

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

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

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

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

**Risk Assessment**

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

**Mitigation**

To mitigate this violation, the entity:

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

**Other Factors**

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

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2018019981 | CIP-007-6 | R3 | Medium | Severe | 3/2/2017 (the date the entity first failed to apply updated intrusion detection signatures) | 6/19/2018 (the date the entity applied updated signatures and actually implemented the email notifications in the software tool) | Self-Report | 4/22/2019 | 10/22/2019 |

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

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

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016919 | CIP-007-6 | R4 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 1/31/2017 (the date the entity corrected the issue and reviewed all logs to ensure no anomalous activity occurred) | Self-Report | 1/31/2017 | 2/1/2018 |

| | |
|---|---|
| **Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)** | On January 31, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R4. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.<br><br>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.<br><br>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:<br><br>1) redirected any device that was reporting to the AOC [redacted] instance to the primary [redacted] instance;<br>2) configured the [redacted] to also send their logs to an additional syslog server;<br>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;<br>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;<br>5) reconfigured the IP addresses on the [redacted] to send their logs directly to the primary [redacted] and<br>6) reviewed the logs from the impacted switches and no anomalous events were identified. |
| **Other Factors** | ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In doing so, ReliabilityFirst examined data related to the entity's historical compliance performance. Specifically, ReliabilityFirst determined that over 90% of the entity's noncompliance since 2012 were self-reported. However, ReliabilityFirst notes that the entity had noticeable increases in self-reports in [redacted] leading up to its audit, and [redacted] the year of its prior audit. (ReliabilityFirst notes that the timing of the submission of the entity's [redacted] self-reports in relation to its audit was affected by the change in audit schedule in [redacted] ReliabilityFirst also determined that the average number of days from the start of a noncompliance to the date that the entity reports that noncompliance to ReliabilityFirst has decreased significantly since 2012. Additionally, the entity has made several improvements in recent years that have positively impacted the compliance culture in the CIP program, including, but not limited to, the following: (a) significant capital investment in the infrastructure of the CIP program; (b) significant investment in additional personnel to address critical skill deficiencies; (c) organizational changes to embed compliance within operations; and (d) increased oversight from, and engagement with, company leadership both at a program level and at the day-to-day operations level. |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016919 | CIP-007-6 | R4 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 1/31/2017 (the date the entity corrected the issue and reviewed all logs to ensure no anomalous activity occurred) | Self-Report | 1/31/2017 | 2/1/2018 |
| | | | ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. | | | | | | |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016924 | CIP-007-6 | R4 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 4/15/2017 (Mitigating Activities completion) | Self-Report | 4/15/2017 | 2/1/2018 |

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

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

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

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

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

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

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

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

**Risk Assessment**

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

**Mitigation**

To mitigate this violation, the entity:

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

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016924 | CIP-007-6 | R4 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 4/15/2017 (Mitigating Activities completion) | Self-Report | 4/15/2017 | 2/1/2018 |
| | | | 5) updated the system security management process with reference to the new manual review process for devices that are not able to be configured in [redacted]; and<br>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.<br><br>ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. | | | | | | |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017018532 | CIP-007-6 | R4 | Medium | Severe | 4/14/2017 (the date the entity installed the affected components) | 12/15/2017 (Mitigating Activities completion) | Self-Report | 12/15/2017 | 5/3/2018 |

| | |
|---|---|
| **Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)** | On October 18, 2017, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-6 R4. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.<br><br>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.<br><br>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:<br><br>1) worked with vendor support to deploy the functionality that limits [redacted]<br>2) implemented new protocols and functionality to capture security events and authentication attempts;<br>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<br>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.<br><br>ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016920 | CIP-007-6 | R5 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 2/28/2017 (Mitigating Activities completion) | Self-Report | 2/28/2017 | 2/1/2018 |

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

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

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

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

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

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

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

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

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

**Risk Assessment**

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

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016920 | CIP-007-6 | R5 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 2/28/2017 (Mitigating Activities completion) | Self-Report | 2/28/2017 | 2/1/2018 |

| | |
|---|---|
| **Mitigation** | To mitigate this violation, the entity:<br><br>1) configured [redacted] to enforce password complexity on the medium impact field devices and verified that the passwords are complex;<br>2) configured the [redacted] tool to enforce password complexity;<br>3) reset and disabled the two SCADA service account default passwords;<br>4) submitted Technical Feasibility Exceptions for [redacted] for assets not technically feasible to meet the requirements of CIP-007 R5.7;<br>5) developed a documented procedure to manage SCADA vendor services accounts;<br>6) implemented a documented procedure detailing how the entity will procedurally enforce complexity for the two [redacted] shared accounts;<br>7) implemented a documented procedure detailing how the entity will procedurally enforce complexity on the local [redacted] password; and<br>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.<br><br>ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017018530 | CIP-007-6 | R5 | Medium | Severe | 4/14/2017 (the date the entity placed the components into production) | 10/25/2017 (the date the entity submitted the Technical Feasibility Exceptions) | Self-Report | 12/15/2017 | 5/3/2018 |

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

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

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

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

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

**Risk Assessment**

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

**Mitigation**

To mitigate this violation, the entity:

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

**Other Factors**

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

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

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017018533 | CIP-007-6 | R5 | Medium | Severe | 4/14/2017 (the date the entity placed the components into production) | 3/21/2019 (Mitigating Activities completion) | Self-Report | 3/21/2019 | 5/16/2019 |

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

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

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

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

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

**Risk Assessment**

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

**Mitigation**

To mitigate this violation, the entity:

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

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017018533 | CIP-007-6 | R5 | Medium | Severe | 4/14/2017 (the date the entity placed the components into production) | 3/21/2019 (Mitigating Activities completion) | Self-Report | 3/21/2019 | 5/16/2019 |

| | |
|---|---|
| | 6) provided training to subject matter experts about the additions to the CIP change management process for new asset types;<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 aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2016016473 | CIP-007-3a | R6 | Medium | Severe | 4/2/2016 (when the Standard became mandatory and enforceable on the entity) | 12/2/2016 (Mitigating Activities completion) | Self-Report | 12/2/2016 | 7/26/2017 |

| | |
|---|---|
| **Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)** | On October 31, 2016, the entity submitted a Self-Report to ReliabilityFirst stating that, [redacted] it was in violation of CIP-007-3a R6. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.<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 aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. | | | | | | |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016922 | CIP-010-2 | R1 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 3/20/2019 (Mitigating Activities completion) | Self-Report | 3/20/2019 | 7/8/2019 |

| | |
|---|---|
| **Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)** | On January 31, 2017 and March 20, 2019, the entity submitted Self-Reports to ReliabilityFirst stating that, [redacted] it was in violation of CIP-010-2 R1. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.<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; |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016922 | CIP-010-2 | R1 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 3/20/2019 (Mitigating Activities completion) | Self-Report | 3/20/2019 | 7/8/2019 |

| | |
|---|---|
| | 11) provided user training for any changes to the Configuration Change Management Procedure to the subject matter experts who use this program. Training included updates in the processes; proper documentation of evidence; identification of CIP security controls which may be impacted; documentation of test templates to document the differences in [redacted]; and enhancement in the Change ticketing process;<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 aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. |

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016923 | CIP-010-2 | R2 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 10/27/2017 (Mitigating Activities completion) | Self-Report | 10/27/2017 | 4/13/2018 |

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

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

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

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

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

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

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

**Risk Assessment**

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

**Mitigation**

To mitigate this violation, the entity:

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

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017016923 | CIP-010-2 | R2 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 10/27/2017 (Mitigating Activities completion) | Self-Report | 10/27/2017 | 4/13/2018 |

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

**Other Factors**

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

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

[redacted] NOC-2664 $225,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017018534 | CIP-010-2 | R2 | Medium | Severe | 4/14/2017 (the date the entity implemented the components) | 1/25/2018 (Mitigating Activities completion) | Self-Report | 1/25/2018 | 5/3/2018 |

| | |
|---|---|
| **Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)** | On October 18, 2017 and December 21, 2017, the entity submitted Self-Reports to ReliabilityFirst stating that, [redacted] it was in violation of CIP-010-2 R2. This violation is being resolved as part of a package that arises out of the entity's efforts to improve and advance its approach to CIP compliance after identifying several issues related to its transition to CIP Version 5. After identifying prior issues, which were resolved in a prior Settlement Agreement, the entity sought to mature several of its processes and procedures by, among other things, automating multiple tasks through the implementation of new tools. However, in several cases, most notably with respect to the implementation of [redacted] the entity was not adequately prepared to deploy these new tools and processes effectively. Consequently, the violations contained in the Settlement Agreement involve implementation challenges the entity faced in this regard, such as failing to properly configure assets or tools prior to deployment, failing to ensure that responsible staff was appropriately trained and prepared to manage assets and tools prior to deployment, and failing to ensure that sufficient processes were in place to support the implementation and operation of new tools and assets.<br><br>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]<br><br>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.<br><br>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.<br><br>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:<br><br>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;<br>2) implemented the Syslog functionality for the [redacted] to capture security events and authentication attempts that then can be reviewed by [redacted]<br>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;<br>4) provided training to subject matter experts about the additions to the CIP change management process for new asset types;<br>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<br>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.<br><br>ReliabilityFirst considered the entity's relevant compliance history and determined that it should not serve as a basis for aggravating the penalty because while the result of some of the prior issues were arguably similar, they arose from different causes. | | | | | | |

**COVER PAGE**

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notices of Penalty in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

| Count | Violation ID | Category 1 | Category 2 | Category 3 | Category 4 | Category 5 | Category 6 | Category 7 | Category 8 | Category 9 | Category 10 | Category 11 | Category 12 | CEII PROTECTION (YEARS) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | RFC2017017060 | Yes | | Yes | Yes | | | | Yes | Yes | | | | Category 1 – 3 years; Category 2 – 12: 2 years |

Filing Date: January 30, 2020

[redacted] NOC-2653 $50,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017017060 | CIP-010-2 | R2 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 8/1/2017 (the date the entity completed milestones in its Mitigation Plan necessary to correct all instances of non-compliance) | Self-Report | 2/13/2018 | 10/29/2018 |

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

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

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

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

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

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

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

[redacted] NOC-2653 $50,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017017060 | CIP-010-2 | R2 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 8/1/2017 (the date the entity completed milestones in its Mitigation Plan necessary to correct all instances of non-compliance) | Self-Report | 2/13/2018 | 10/29/2018 |

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

[redacted] NOC-2653 $50,000

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017017060 | CIP-010-2 | R2 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable on the entity) | 8/1/2017 (the date the entity completed milestones in its Mitigation Plan necessary to correct all instances of non-compliance) | Self-Report | 2/13/2018 | 10/29/2018 |

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

**Other Factors**

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

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

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

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

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

**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 SNOPs 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 | RFC2017018305 | Yes | | Yes | Yes | Yes | Yes | | Yes | | | | | Category 1: 3 years; Category 2- |
| 2 | RFC2016016353 | Yes | | Yes | Yes | | Yes | | | | Yes | | | 12: 2 years. |
| 3 | RFC2017018475 | Yes | | Yes | Yes | | Yes | | | | | | | Category 1: 3 years; Category 2- |
| 4 | RFC2018019404 | Yes | | Yes | Yes | | Yes | | Yes | Yes | | | | 12: 2 years. |
| 5 | WECC2019021165 | Yes | | Yes | Yes | | | | | | | | Yes | Category 1: 3 years; Category 2- |
| 6 | WECC2017017507 | Yes | | Yes | Yes | | | | | Yes | | | | Category 2 – 12: 2 year |
| 7 | WECC2017017631 | Yes | | Yes | Yes | | | | | Yes | | | | Category 2 – 12: 2 year |
| 8 | WECC2017017632 | Yes | | Yes | Yes | | | | | Yes | | | | Category 2 – 12: 2 year |
| 9 | WECC2017017633 | Yes | | Yes | Yes | | | | Yes | Yes | | | | Category 2 – 12: 2 year |
| 10 | WECC2017017634 | | | Yes | Yes | | | | | Yes | Yes | | | Category 2 – 12: 2 year |
| 11 | WECC2017018364 | Yes | | Yes | Yes | | | | | Yes | Yes | | | Category 2 – 12: 2 year |
| 12 | WECC2017017911 | Yes | | Yes | Yes | | | Yes | | Yes | | | | Category 2 – 12: 2 year |
| 13 | WECC2018018977 | Yes | | Yes | Yes | | | Yes | | Yes | Yes | | | Category 2 – 12: 2 year |
| 14 | WECC2018019483 | Yes | | Yes | Yes | | | Yes | | Yes | | | | Category 2 – 12: 2 year |
| 15 | WECC2017018365 | | | Yes | Yes | | | | | Yes | Yes | | | Category 2 – 12: 2 year |
| 16 | WECC2017017676 | Yes | | Yes | Yes | Yes | | | | Yes | | | | Category 1: 3 years; Category 2- 12: 2 years. |

[redacted] NOC-2648 $115,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017018305 | CIP-005-3a | R2 | Medium | Severe | 9/9/2014 (when the entity failed to implement all CIP-005-3a R2 protections on the [redacted] | 11/3/2017 (when the entity implemented the required controls | Self-Report | 2/9/2018 | 9/11/2018 |

**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 August 30, 2017, the entity submitted a Self-Report stating that, as a [redacted], it was in violation of CIP-005-3a R2.

This violation involves three instances of an application installed on a Bulk Electric System (BES) Cyber Asset (BCA) without the use of certain technical and procedural mechanisms for control of electronic access at all electronic access points. The affected application, known as the [redacted] provides a [redacted]

The entity's [redacted] at the time employed reviews by multiple departments regarding firewall rules that allowed access into the Electronic Security Perimeter (ESP). These departments include [redacted]. When a firewall request was made, these departments reviewed the request for Interactive Remote Access characteristics and proper business justification. However, the procedure was incomplete in that it did not include a check to ensure [redacted] were properly configured on the [redacted] to prevent access in the three instances in question. [redacted]

In the first instance, entity staff identified that, beginning September 9, 2014, a [redacted] was reachable directly from the entity's corporate user network without the required network-level security controls required by CIP-005-3a R2 Parts 2.1 (deny access by default), 2.2 (enable only ports and services required for operations and monitoring), and 2.3 (procedure for securing dial-up access). A user would still have to authenticate to the application prior to gaining access.

Additionally, regarding the second instance, the entity determined that the [redacted] was reachable directly from the corporate user network without the use of an Intermediate System, in violation of CIP-005-5 R2. The application log-on screen was reachable once the user logged into the SSL VPN, which enforced encryption and multi-factor authentication, but it lacked an intermediate device. Thus, this second instance began July 1, 2016, when CIP version 5 went into effect.

Third, during an extent of condition review, the entity identified another instance where the BCAs [redacted] responsible for hosting the [redacted] e were directly accessible via [redacted]. It was determined the access was granted on October 19, 2016. The entity completed remediation of this additional instance on November 3, 2017. [redacted]

The root cause of the violation is that the entity lacked sufficient verification controls to ensure the configuration was correct for the [redacted] and an insufficient process which was missing a step to require verification that [redacted].

The first violation ([redacted]) started on September 9, 2014, when the entity failed to implement all CIP-005-3a R2 protections on the [redacted], and ended on May 9, 2017, when the entity implemented the required protections for the [redacted].

The second violation [redacted]) started on July 1, 2016, when CIP version 5 became effective, and ended on May 9, 2017, when the entity implemented the required controls on the device.

The third violation (relating to BCAs [redacted]) started on October 19, 2016, when the access was granted within an Intermediate System, and ended November 3, 2017, when the entity implemented the required controls.

**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 [redacted] is in-scope for CIP as a BES Cyber System because its functionality is critical to other BES Cyber Systems. However, [redacted]y does not grant access to any critical, real-time application. It only permits authorized users the ability to view or change the [redacted]). Also, users cannot leverage the [redacted]s as a means to jump into other applications on the same subnet. Thus, the application has limited impact to real-time operations. Regarding the BCA in the third instance, the BCAs do not perform any real-time BES functions. Additionally, access to the assets was only available to internal entity users, and access is granted only to authorized administrators after they have authenticated against the entity's access system. The entity was also monitoring for failed authentication attempts, performed annual cyber vulnerability assessments, and scanned the assets quarterly. In addition, as noted above, a user would still need to authenticate to the application in order to gain access; a logon screen would be presented to anyone

[redacted] NOC-2648 $115,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017018305 | CIP-005-3a | R2 | Medium | Severe | 9/9/2014 (when the entity failed to implement all CIP-005-3a R2 protections on the [redacted] | 11/3/2017 (when the entity implemented the required controls | Self-Report | 2/9/2018 | 9/11/2018 |

| | |
|---|---|
| | trying to access this application. The entity also noted that only authorized entity clients were allowed on the network, and that the application servers were not reachable via these means. Regardless, the violation posed moderate risk because the network path available for assets potentially creates a vulnerability that can leveraged for malicious activity. |
| **Mitigation** | For mitigation, generally, as corrective measures, the entity removed the direct access by denying traffic from VPN Networks and User Networks to the [redacted]. As preventive measures, the entity implemented a technical control to prevent any direct access into an ESP (from user or VPN networks) and implemented a procedural control to update the [redacted] to reject any firewall requests from a User or VPN network to [redacted]. The entity also implemented a [redacted] procedure that includes a reminder to add [redacted] and to review [redacted].<br><br>To mitigate this violation, the entity:<br><br>1) created new firewall rules denying direct access from all VPN networks and user networks. This change required all Interactive Remote Access to [redacted] to use an Intermediate System;<br>2) held internal meetings with Subject Matter Experts to determine approaches for preventing a future reoccurrence of this issue;<br>3) reviewed [redacted], tested as needed, and remediated where necessary;<br>4) deployed [redacted] as noted in the root-cause explanation;<br>5) updated [redacted] to include steps to reject any firewall request coming from a user or VPN networks destined for a [redacted]. This will help prevent firewall rules from being added which could accidentally grant direct access ([redacted]); and<br>6) developed and published a procedure that instructs network analysts on configuring [redacted] and provides a reminder to review firewall rules associated with [redacted]. |
| **Other Factors** | ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>ReliabilityFirst considered the entity's cooperation during the Settlement Agreement process and awarded mitigating credit. The entity was proactive in working with ReliabilityFirst once the violations were identified. The entity voluntarily provided ReliabilityFirst with information regarding the violations in a manner that was thorough and timely. The entity has been open with ReliabilityFirst regarding its violations, processes, systems, and organization, and this insight has allowed ReliabilityFirst to better analyze the violations. ReliabilityFirst awarded a mitigating credit to encourage this sort of response in the future.<br><br>Effective oversight of the reliability of the BES depends on robust and timely self-reporting by registered entities. The entity self-identified and reported some of the violations at issue in the Settlement Agreement. As a result, ReliabilityFirst seeks to encourage this type of self-reporting by awarding some mitigating credit.<br><br>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history does not warrant an elevated risk and should not serve as a basis for an aggravated penalty. The prior noncompliances are distinguishable as they involved different circumstances and root causes, in part because the amount of time that has passed since mitigation supports the conclusion that the processes and systems in place at the time of the prior violations evolved such that the instant violations do not involve recurring conduct. |

[redacted] NOC-2648 $115,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| RFC2016016353 | CIP-007-3a | R2 | Medium | Severe | 4/24/2013 ([redacted]) | 9/30/2017 (Mitigation Plan completion) | Compliance Audit | 9/30/2017 | 4/11/2018 |

| | |
|---|---|
| **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 11, 2016, ReliabilityFirst determined that the entity, as a [redacted], was in violation of CIP-007-3a R2. ReliabilityFirst identified the violation during a Compliance Audit conducted [redacted].<br><br>ReliabilityFirst determined that the entity documented overly broad IP address port ranges. The entity did not make a sufficient determination to ensure that only those ports that were necessary were enabled, and therefore its documentation and baselines in its monitoring tool were overly broad in that they authorized an overly broad port range. In many instances, the unnecessary ports that were authorized were applicable to all [redacted] systems, which run the entity's most critical systems, including the energy management system. The entity could not produce justifications for the overly broad port ranges. Additionally, in one instance, the entity did not identify an unauthorized port for a phone system that was deemed necessary because it could not be disabled.<br><br>The root cause was the entity not verifying that the port ranges in the documentation were appropriate and necessary at the time the entity installed software due to insufficient verification controls.<br><br>The violations began on April 24, 2013, [redacted], and ended on September 30, 2017, when the entity completed its Mitigation Plan. |
| **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 of not having sufficient justifications for ports ranges is that an entity will enable unnecessary ports, thus increasing the entity's attack surface for unauthorized access to Bulk Electric System (BES) Cyber Systems. Additionally, the risk of authorizing overly broad port ranges is that it reduces the entity's ability to detect unauthorized access. The risk is somewhat mitigated here based on the following factors. The entity implemented defense-in-depth measures that were in place at the time of the violation, including, for example, the following measures. First, the entity was recently able to show that while it authorized overly broad port ranges, only necessary ports were enabled during the period of noncompliance. Second, the entity required subject matter expert confirmation of any newly detected service running on a CIP-scoped asset. Third, the entity employed all of the CIP-005 protections to the Electronic Security Perimeters (ESPs) containing the assets in question, including the use of two-factor authentication for Interactive Remote Access sessions, and the assets were protected behind a designated Electronic Access Point (EAP). The entity also employed network segmentation to limit the scope of what systems could be reached from any local network, as well as the security monitoring requirements per CIP-007, including the detection of unauthorized login attempts. The network segmentation includes: [redacted] Lastly, the entity employed stringent access management and only authorized a very limited number of users for administration and Interactive Remote Access to the EAPs. While improvements could have been (and now have been) made regarding documenting ports and services on the assets in question, the above-referenced measures collectively would have restricted the ability of an adversary to gain access to an intermediate system and move laterally into one of the assets within an ESP and to evade detection using a service on one of the assets. |
| **Mitigation** | To mitigate this violation, the entity:<br><br>1) developed evidence standards that require vendor, design, or architectural justification for necessary ports, as well as evidence storage and metadata for cataloging necessary ports;<br>2) demonstrated effectiveness of new evidence requirements and validated necessary ports and services for the CIP cyber assets chosen in the [redacted] audit data request. The entity will use the exercise to update the new evidence requirements and catalog metadata;<br>3) integrated the evidence requirements into the entity's ports and services policies and procedures;<br>4) iterated through the remaining [redacted] CIP-scoped cyber assets to ensure compliance with new evidence requirements defined in milestone 2, updated the catalog of necessary ports as necessary, and verified open ports on the assets with approved list; and<br>5) completed iteration of the remaining CIP-scoped cyber assets [redacted] to ensure compliance with new evidence requirements defined in milestone 2, updated the catalog of necessary ports as necessary, and verified open ports on the assets with approved list. |
| **Other Factors** | ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>ReliabilityFirst considered the entity's cooperation during the Settlement Agreement process and awarded mitigating credit. The entity was proactive in working with ReliabilityFirst once the violations were identified. The entity voluntarily provided ReliabilityFirst with information regarding the violations in a manner that was thorough and timely. The entity has been open with ReliabilityFirst regarding its violations, processes, systems, and organization, and this insight has allowed ReliabilityFirst to better analyze the violations. ReliabilityFirst awarded a mitigating credit to encourage this sort of response in the future. |

[redacted] NOC-2648 $115,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| RFC2016016353 | CIP-007-3a | R2 | Medium | Severe | 4/24/2013 ([redacted]) | 9/30/2017 (Mitigation Plan completion) | Compliance Audit | 9/30/2017 | 4/11/2018 |
| | | | Effective oversight of the reliability of the BES depends on robust and timely self-reporting by registered entities. The entity self-identified and reported some of the violations at issue in the Settlement Agreement. As a result, ReliabilityFirst seeks to encourage this type of self-reporting by awarding some mitigating credit.<br><br>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history does not warrant an elevated risk and should not serve as a basis for an aggravated penalty. The prior noncompliances are distinguishable as they involved different circumstances and root causes, in part because the amount of time that has passed since mitigation supports the conclusion that the processes and systems in place at the time of the prior violations evolved such that the instant violations do not involve recurring conduct. | | | | | | |

[redacted] NOC-2648 $115,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017018475 | CIP-010-2 | R1 | Medium | Severe | 4/26/2017 (when the entity user installed the unauthorized application) | 7/18/2017 (when the application was ultimately removed from the server) | Self-Report | 6/21/2018 | 11/29/2018 |

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

On October 5, 2017, the entity submitted a Self-Report stating that, as [redacted], it was in violation of CIP-010-2 R1.

On April 26, 2017, an entity analyst installed an unauthorized application in his personal home directory on an Electronic Access Control or Monitoring System (EACMS) Intermediate System. The application was used by the analyst to [redacted]. The work to install the [redacted] in an individual's home directory did not require escalated privileges, so the analyst did not believe he needed to file a change management request (or test the application). The unauthorized application was not detected by the entity's tool, [redacted] because the software was installed in the analyst's home directory, which is not subject to routine [redacted] scans used to detect software changes.

However, on April 27, 2017, the entity's [redacted] port scans detected the presence of an unauthorized port [redacted] which was attributed to the [redacted]. The entity's IT team investigated the issue, shut down the unauthorized port, and subsequently notified the analyst that the software was not authorized.

On May 3, 2017, the analyst initiated the entity's software approval process, but the request to utilize the application was denied on May 25, 2017. At that time, the entity's security review teams expressed security concerns with the software and offered alternative applications for the analyst to utilize. As part of the review process, the analyst provided further business justification to utilize the application to the entity's security review team, which was considered, and ultimately denied on July 12, 2017. In the meantime, the analyst continued to utilize [redacted]. The entity's [redacted] port scans detected the unauthorized port, and, in each instance, the entity's IT teams shut down the unauthorized port.

On July 11, 2017, the entity performed a review of recent changes to the authorized port "whitelist" and noticed the unauthorized port on a CIP Intermediate System, attributable to the [redacted]. Upon discovery, the entity investigated the issue and discovered that [redacted] was still installed on a CIP Intermediate System.

The application remained in use and actively opened ports from April 26, 2017 to July 18, 2017, when the application was ultimately removed from the server. The application was installed and was in-use on the server for 83 days, therefore exceeding the required time (30 days) the entity had after installation to update the baseline. Additionally, the user did not perform the required change management activities before installing the application.

The root causes were lack of understanding on when change management requests were required, insufficient controls to detect the unauthorized application, and the entity's failure to verify that the analyst removed the application. This violation involves the management practices of workforce management, in that additional training could have helped prevent the violation, and asset and configuration management, in that the entity's controls were insufficient to detect and manage changes to its assets.

This noncompliance started on April 26, 2017, when the entity user installed the unauthorized application, and ended July 18, 2017, when the application was ultimately removed from the server.

**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 potential risk was that the application could have introduced vulnerabilities into the system or could have adversely affected the functionality of the EACMS. This risk was somewhat mitigated by the following factors. The application only accepted connections from clients after the client logged into a VPN with two-factor authentication and authenticated to the Intermediate System through the [redacted]. Thus, there was low likelihood that someone could successfully access the application and potentially compromise the bulk power system. However, the risk is still moderate because the entity failed to test the application prior to installation. Additionally, although the entity quickly identified the unauthorized application, the entity failed to ensure that the application was removed, and the unauthorized application remained installed for 83 days. This slow corrective action extended the period of time that there was an increased risk of compromise on the system.

**Mitigation**

To mitigate this violation, the entity:

1) removed the unauthorized application from the system;
2) counseled the analyst and the department staff on the importance of following the entity's configuration and change management processes and clarified aspects of baselines;
3) scanned for changes to the home directory of the machine at issue. The entity refined detection rules to ensure scripts and software in the home user directories are detected;
4) implemented a tool to scan home directories on CIP-scoped [redacted] systems to look for scripts and locally installed software; and
5) inspected the results of the initial home directory scans on [redacted] assets for additional exceptions, determined if modifications to the approved baselines are needed, and trained individuals on the modifications to the baselines as needed.

**Other Factors**

ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.

[redacted] NOC-2648 $115,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| RFC2017018475 | CIP-010-2 | R1 | Medium | Severe | 4/26/2017 (when the entity user installed the unauthorized application) | 7/18/2017 (when the application was ultimately removed from the server) | Self-Report | 6/21/2018 | 11/29/2018 |

ReliabilityFirst considered the entity's cooperation during the Settlement Agreement process and awarded mitigating credit. The entity was proactive in working with ReliabilityFirst once the violations were identified. The entity voluntarily provided ReliabilityFirst with information regarding the violations in a manner that was thorough and timely. The entity has been open with ReliabilityFirst regarding its violations, processes, systems, and organization and this insight has allowed ReliabilityFirst to better analyze the violations. ReliabilityFirst awarded a mitigating credit to encourage this sort of response in the future.

Effective oversight of the reliability of the BES depends on robust and timely self-reporting by registered entities. The entity self-identified and reported some of the violations at issue in the Settlement Agreement. As a result, ReliabilityFirst seeks to encourage this type of self-reporting by awarding some mitigating credit.

The entity has relevant compliance history. Some of the prior noncompliances resulted from arguably similar contributing causes (i.e. lack of understanding on when change management requests were required). However, RF did not aggravate the penalty based on repeat behavior because the prior noncompliances were all minimal risk and involved high-frequency conduct for which the entity, in the prior noncompliances, quickly identified and corrected noncompliances.

[redacted] NOC-2648 $115,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| RFC2018019404 | CIP-010-2 | R2 | Medium | Severe | 5/24/2017 | 2/20/2018 (when the entity remediated the baseline configuration issue) | Self-Report | 7/31/2018 | 11/19/2018 |

**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 March 13, 2018 and April 17, 2018, the entity submitted Self-Reports stating that, as a [redacted], it was in violation of CIP-010-2 R2.

This violation includes two separate instances. In the first incident, the entity did not monitor a baseline configuration for four CIP-scoped assets at least once every 35 calendar days as required by CIP-10-2 R2.1. On May 24, 2017, four firewalls which are classified as Electronic Access Control or Monitoring Systems (EACMS) were placed into service; however, the firewalls were not added to the entity's baseline monitoring tool [redacted] and were not monitored for baseline changes until November 30, 2017, when an entity analyst detected the violation while seeking evidence for the entity's internal controls testing.

In the second incident, the entity did not monitor two Protected Cyber Assets (PCAs) at least once every 35 days for changes to the baseline configuration as required by CIP-010-2 R2. As background, on July 5, 2017, the entity performed an upgrade on two PCAs which caused some of the baseline elements to return an error in the entity's monitoring tool [redacted] because several elements of the upgrade failed. However, because the entity's monitoring tool was able to reconcile the error with a change ticket for the upgrade, the change was "auto-promoted" meaning it was deemed acceptable and not investigated further. On January 9, 2018, an analyst discovered the issue on one asset and immediately remediated it. On January 10, 2018, the analyst ran a report to see if other assets were affected and discovered the second adversely affected asset.

There were different root causes for the two incidents in this violation. In the first incident, the process for configuration management was not properly documented which made it unclear whose responsibility it was to notify the entity's monitoring tool to monitor the baseline element; and since the process was unclear, it was not followed effectively, resulting in the four EACMS being left outside of configuration monitoring. In the second incident, the file-retrieving software used by [redacted] was older than the version on the entity's other similar devices. Therefore, the older-version of the file-retrieving software had communication issues which resulted in an error communication. However, the error was not caught because the integration between the [redacted] system and the [redacted] change ticketing system was limited. [redacted] These limitations in integration caused [redacted] to erroneously reconcile a baseline change from July 5, 2017, with a change ticket for the affected asset for the same day; however, the actual change was due to an error, rather than the change recorded in the change ticket.

This violation involves the management practice of verification because there was an error in the entity's verification process in that, during the verification process, the error was incorrectly reconciled with the change ticket.

This noncompliance started on May 24, 2017, which is the date the firewalls were placed into service in the first instance and ended on February 20, 2018, when the entity remediated the baseline configuration issue.

**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 this violation is the potential for an unauthorized user to change the baseline configuration without the entity's knowledge. The risk is partially reduced because in the second incident just 2 of the entity's [redacted] PCAs were affected by the violation. Further reducing the risk, all other CIP controls were in place for the affected assets in the second incident. including logs and anti-virus protection which would alert the entity to a threat caused by the failure to monitor the firewalls. Minimizing the risk in the first incident, in order to reach the firewalls from an administration perspective required two-factor authentication and the use of an Intermediate Device; further all Bulk Electric System (BES) Cyber Asset and PCAs behind the firewalls were also afforded all protections as defined by the NERC CIP Standards. However, the first incident had a duration of more than 7 months before it was discovered by the entity's internal controls. [redacted]

**Mitigation**

To mitigate this violation, the entity:

1) created an "Awareness Only" ticket in the entity change management system to enable daily [redacted] scans on the affected assets. The entity configured [redacted] to scan the affected assets daily;
2) performed a reconciliation to ensure no other assets were affected;
3) reviewed the [redacted] scans for the affected assets per the entity's [redacted]. No actions needed, no changes detected;
4) identified/documented the root cause of the configuration difference for the affected assets. The entity created a ticket with request to resolve issue;
5) performed a reconciliation to discover any other assets affected with older version of a file-retrieving software;
6) held a meeting to determine process improvement steps;
7) updated the two affected assets with current version of a file-retrieving software. The entity ran [redacted] scan successfully to ensure all configuration baseline elements are being monitored;

[redacted] NOC-2648 $115,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| RFC2018019404 | CIP-010-2 | R2 | Medium | Severe | 5/24/2017 | 2/20/2018 (when the entity remediated the baseline configuration issue) | Self-Report | 7/31/2018 | 11/19/2018 |

| | |
|---|---|
| | 8) updated the entity's [redacted] Procedure to add how the entity notifies analysts when to configure [redacted] to monitor CIP baseline elements. The entity communicated this change to the team;<br>9) collected and created an inventory of all error types for content scans within [redacted]. The entity created an inventory based on previously identified error types;<br>10) configured test environment of [redacted] to identify unexpected content so that a scanning error will pick up specific changes like a new version of a file-retrieving software. The entity integrated a configuration solution to determine review frequency and overall process with [redacted];<br>11) validated that implementation was successful and provided expected data that will assist in error identification and baseline reconciliation. The entity documented process for implementation in future content exceptions originating from unknown errors; and<br>12) trained staff on new scanning error parameters and how to adjust for future inclusions. |
| **Other Factors** | ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>ReliabilityFirst considered the entity's cooperation during the Settlement Agreement process and awarded mitigating credit. The entity was proactive in working with ReliabilityFirst once the violations were identified. The entity voluntarily provided ReliabilityFirst with information regarding the violations in a manner that was thorough and timely. The entity has been open with ReliabilityFirst regarding its violations, processes, systems, and organization and this insight has allowed ReliabilityFirst to better analyze the violations. ReliabilityFirst awarded a mitigating credit to encourage this sort of response in the future.<br><br>Effective oversight of the reliability of the BES depends on robust and timely self-reporting by registered entities. The entity self-identified and reported some of the violations at issue in the Settlement Agreement. As a result, ReliabilityFirst seeks to encourage this type of self-reporting by awarding some mitigating credit.<br><br>The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history does not warrant an elevated risk and should not serve as a basis for an aggravated penalty. The prior noncompliances are distinguishable as they involved different circumstances and root causes, in part because the amount of time that has passed since mitigation supports the conclusion that the processes and systems in place at the time of the prior violations evolved such that the instant violations do not involve recurring conduct. |

[redacted] NOC-2652 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2019021165 | CIP-010-2 | R1; P1.4.1; P1.4.2; P1.4.3; P1.5.1; P1.5.2 | Medium | Severe | 2/14/2019 (when the entity changed the configuration by removing the software) | 2/26/2019 (when the entity assessed the security controls according to CIP-010) | Self-Report | 2/26/2019 | 6/11/2019 |

| | |
|---|---|
| **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 March 5, 2019, the entity submitted a Self-Report stating, as a as [redacted], it was in potential noncompliance with CIP-010-2 R1. Specifically, on February 16, 2019, during a review of a daily delta report for baseline configuration changes , the entity identified [redacted] Bulk Electric System (BES) Cyber Assets (BCAs) associated with its High Impact BES Cyber Systems (HIBCS) located at the primary and backup Controls Centers that had software removed on February 14, 2019. The [redacted] BCAs, although connected to the network and in the production environment, had interfaces used to send data from one server to the other, turned off because the BCAs were scheduled to be decommissioned. The software, which was part of the interface, was sending false errors to the software vendor through a different connection than the interface, resulting in the software vendor calling the entity and initiating the software removal to solve the false error reporting. The [redacted] BCAs were then turned on, at which time the software removal occurred without the entity first determining the required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change or verifying that any identified cyber security controls were not adversely affected, once the change had taken place; nor documenting any results as required by CIP-010-2 R1 Part 1.4 sub-parts 1.4.1, 1.4.2, and 1.4.3. Additionally, the entity did not test the changes in a production or test environment prior to implementing the change and did not document such testing as required by CIP-010-2 R1 Part 1.5 sub-parts 1.5.1 and 1.5.2 This issue ended on February 26, 2019, when the security controls in CIP-005 and CIP-007 were determined, verified to not have been adversely affected, the verification results were documented, and the baseline change was documented, for a violation duration of 13 days.<br><br>After reviewing all relevant information, WECC Enforcement determined the entity failed CIP-010-2 R1 Parts 1.4 and Part 1.5 as described above. The root cause of the issue was attributed to senior personnel deciding to not follow the entity's change control and configuration management processes. Specifically, based on the expertise and knowledge of the senior personnel and a contractor performing the work, they determined the removal of the software posed no threat to the BPS and therefore, completed the work without following documented change management processes. |
| **Risk Assessment** | WECC determined this issue posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). In this instance, for a change that deviated from an existing baseline configuration related to [redacted] BCAs, the entity failed to determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; verify those identified controls were not adversely affected; and document the results of the verification as required by CIP-010-2 R1 Part 1.4, as well as failed to test in a production or test environment and document the results prior to implementing the change as required by CIP-010-2 R1 Part 1.5. Such failure could have caused the BCA interfaces to become inoperable and affect traffic that was being sent from one BCA to another, which could potentially affect the reliability of the BPS.<br><br>However, in this instance the interfaces on the BCA were turned off and not capable of sending data between servers; therefore, the potential harm was lessened. The entity had implemented good detective controls in the form of a daily delta report for baseline configuration changes which is how this issue was discovered. Lastly, WECC confirmed the root cause of this violation was an isolated incident and not condoned by the entity's management, which lessens the likelihood of a future issue. No harm is known to have occurred. |
| **Mitigation** | To remediate and mitigate this issue, the entity has:<br>1) verified the security controls of the baseline configuration change and documented the verification;<br>2) updated its baseline configuration for a change that deviated from an existing baseline configuration;<br>3) created awareness of the importance of following the change management procedures by sending a security awareness email to personnel with authority to implement baseline changes; and<br>4) confirmed that the individual responsible for causing the violation is no longer with the entity. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor. The entity exercised due diligence to detect this violation. Additionally, the entity's ICP includes a process for self-auditing and monitoring for noncompliance which is how this violation was discovered.<br><br>WECC considered the entity's history of noncompliance with CIP-010-2 R1 given NERC Violation ID [redacted] and determined it should not serve as a basis for aggravating the penalty because it is one instance of previous noncompliance disposed of as a Compliance Exception with a different root cause.<br><br>WECC considered the entity personnel's choice not to follow the Standard and Requirement to be an aggravating factor in treating this violation in a Settlement Agreement instead of as an FFT. |

[redacted] NOC-2658 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017507 | CIP-005-5 | R1: P1.1 | Medium | Severe | 07/01/2016 | 07/25/2017 | Self-Report | 12/04/2018 | 02/22/2019 |

| | |
|---|---|
| **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 April 28, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in potential noncompliance with CIP-005-5 R1. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one [redacted] within the Electronic Security Perimeter (ESP), [redacted], and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA and submitted four additional Self-Reports.<br><br>After reviewing all relevant information, WECC determined the entity failed to place the BCA connected to a network via a routable protocol, within a defined ESP as required by CIP-005-5 R1 Part 1.1. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on July 25, 2017, when the BCA was added to the ESP, for a total of 390 days of noncompliance.<br><br>The root cause of the BCA violations was attributed to a lack of knowledge of the capabilities and functions of the BCA. |
| **Risk Assessment** | WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633 and WECC2017017634) individually and collectively posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-005-5 R1, CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to EACMS and PACS [redacted]escribed here[redacted]<br><br>Failing to locate this BCA within an ESP and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a [redacted] which could affect [redacted] at the entity; thereby potentially affecting the reliability of the BPS. Failing to create a baseline for configuration results in the entity not being able to compare the current configuration to that which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets.<br><br>However, as compensation, the entity had implemented managed policy rules for monitoring the BCA, and it was in a network segment that limited permissions to communicate with other parts of the entity's network, preventing the BCA from being accessed from other network segments unless a specific rule was created to allow that communication path. To control physical access, it was located within a PSP. The BCA was used as a [redacted], but there were two backup sources [redacted]. If the primary [redacted] (the BCA) were to fail, the system would automatically switch to one of the backup sources within 30 seconds. If [redacted], the System Operator would have received an alarm and could have utilized his capability to quickly switch the [redacted] to one of the backup devices, in the event they needed to manually bypass the BCA. Additionally, the entity implemented periodic internal audits which is how the instances with the EACMS and PACS were discovered. [redacted] |
| ***Mitigation*** | To mitigate this violation, the entity has:<br>1) placed the BCA inside the ESP; and<br>2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices. |
| **Other Factors** | These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty.<br><br>WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2658 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017631 | CIP-007-6 | R1: P1.1 | Medium | High | 07/01/2016 | 05/17/2017 | Self-Report | 09/07/2017 | 10/08/2019 |

| | |
|---|---|
| **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 May 22, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in potential noncompliance with CIP-007-6 R1. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one [redacted] within the Electronic Security Perimeter (ESP), [redacted], and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA.<br><br>After reviewing all relevant information, WECC determined the entity failed to enable only logical network accessible ports on the BCA that have been determined to be needed by the entity as required by CIP-007-6 R1 Part 1.1. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on May 17, 2017, when the BCA's open logical ports were documented in a baseline configuration, for a total of 321 days of noncompliance.<br><br>The root cause of the violation was attributed to a lack of knowledge of the capabilities and functions of the BCA. |
| **Risk Assessment** | WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633 and WECC2017017634) individually and collectively posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-005-5 R1, CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to [redacted] EACMS and [redacted] PACS as described herein.<br><br>Failing to locate this BCA within an ESP and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a [redacted] which could affect [redacted] at the entity; thereby potentially affecting the reliability of the BPS. Failing to create a baseline for configuration results in the entity not being able to compare the current configuration to that which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets.<br><br>However, as compensation, the entity had implemented managed policy rules for monitoring the BCA and it was in a network segment that limited permissions to communicate with other parts of the entity's network, preventing the BCA from being accessed from other network segments unless a specific rule was created to allow that communication path. To control physical access, it was located within a PSP. The BCA was used as a [redacted], but there were two backup sources [redacted]. If the primary [redacted] (the BCA) were to fail, the system would automatically switch to one of the backup sources within 30 seconds. If [redacted], the System Operator would have received an alarm and could have utilized his capability to quickly switch the [redacted] to one of the backup devices, in the event they needed to manually bypass the BCA. Additionally, the entity implemented periodic internal audits which is how the instances with the EACMS and PACS were discovered. [redacted]. No harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the entity has:<br>1) documented all enabled logical network accessible ports; and<br>2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices. |
| **Other Factors** | These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty.<br><br>WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2658 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017632 | CIP-007-6 | R2: P2.1 | Medium | Moderate | 07/01/2016 | 05/09/2017 | Self-Report | 08/24/2018 | 10/23/2019 |

| | |
|---|---|
| **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 May 22, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in potential noncompliance with CIP-007-6 R2. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one [redacted] within the Electronic Security Perimeter (ESP), used as the [redacted], and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA.<br><br>After reviewing all relevant information, WECC determined the entity failed to identify a source or sources that the entity tracks for the release of cyber security firmware patches applicable to the BCA, as required by CIP-007-6 R2 Part 2.1. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on May 9, 2017, when the BCA was added to the patch source tracking spreadsheet, for a total of 313 days of noncompliance.<br><br>The root cause of this violation was attributed to a lack of knowledge of the capabilities and functions of the BCA. |
| **Risk Assessment** | WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633 and WECC2017017634) individually and collectively posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-005-5 R1, CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to [redacted] EACMS and [redacted] PACS as described herein.<br><br>Failing to locate this BCA within an ESP and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a [redacted] which could affect [redacted] at the entity; thereby potentially affecting the reliability of the BPS. Failing to create a baseline for configuration results in the entity not being able to compare the current configuration to that which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets.<br><br>However, as compensation, the entity had implemented managed policy rules for monitoring the BCA and it was in a network segment that limited permissions to communicate with other parts of the entity's network, preventing the BCA from being accessed from other network segments unless a specific rule was created to allow that communication path. To control physical access, it was located within a PSP. The BCA was used as a [redacted], but there were two backup sources [redacted]. If the primary [redacted] (the BCA) were to fail, the system would automatically switch to one of the backup sources within 30 seconds. If [redacted], the System Operator would have received an alarm and could have utilized his capability to quickly switch the [redacted] to one of the backup devices, in the event they needed to manually bypass the BCA. Additionally, the entity implemented periodic internal audits which is how the instances with the EACMS and PACS were discovered. [redacted]. No harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the entity has:<br>1) added the BCA to the patch source tracking spreadsheet;<br>2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices; and<br>3) updated its process to require all new Cyber Assets to go through a documented commissioning process before being connected to the operations network or deployed into an ESP to include adding Cyber Assets to the patch tracking spreadsheet and documenting baseline configurations. |
| **Other Factors** | ECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant history was an issue in 2014 that posed minimal risk and not indicative of broader compliance issues. |

[redacted] NOC-2658 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017633 | CIP-007-6 | R5: P5.1-P5.7 | Medium | Severe | 07/01/2016 | 02/15/2019 | Self-Report | 02/15/2019 | TBD |

**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 May 22, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in potential noncompliance with CIP-007-6 R5. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one [redacted] within the Electronic Security Perimeter (ESP), used as the [redacted], and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA.

After reviewing all relevant information, WECC determined the entity failed to have method(s) to enforce authentication of interactive user access, identify and inventory all known enabled default or other generic account types, identify individuals who have authorized access to shared accounts, change known default passwords, enforce the required password length and complexity, enforce password changes at least once every 15 calendar months; and limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts where technically feasible on the BCA, as required by CIP-007-6 R5 Parts 5.1 through 5.7. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on February 15, 2019, when the protective measures as required by CIP-007-6 R5 Parts 5.1 through 5.6 were implemented and for Part 5.7 when the entity submitted a Technical Feasibility Exception, for a total of 960 days of noncompliance.

The root cause of the BCA violations was attributed to a lack of knowledge of the capabilities and functions of the BCA.

**Risk Assessment**

WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, and WECC2017017634) individually and collectively posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-005-5 R1, CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to EACMS and [redacted]CS as descri[redacted]erein.

Failing to locate this BCA within an ESP and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a primary [redacted] which could affect [redacted] at the entity; thereby potentially affecting the reliability of the BPS. Failing to create a baseline for configuration results in the entity not being able to compare the current configuration to that which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets.

However, as compensation, the entity had implemented managed policy rules for monitoring the BCA and it was in a network segment that limited permissions to communicate with other parts of the entity's network, preventing the BCA from being accessed from other network segments unless a specific rule was created to allow that communication path. To control physical access, it was located within a PSP. The BCA was used as a [redacted], but there were two backup sources for [redacted]. If the primary [redacted] (the BCA) were to fail, the system would automatically switch to one of the backup sources within 30 seconds. If [redacted], the System Operator would have received an alarm and could have utilized his capability to quickly switch the [redacted] to one of the backup devices, in the event they needed to manually bypass the BCA. Additionally, the entity implemented periodic internal audits which is how the instances with the EACMS and PACS were discovered. [redacted]. No harm is known to have occurred.

**Mitigation**

To mitigate this violation, the entity has:

1) enforced authentication of interactive user access by changing the default passwords;
2) identified and inventoried all default accounts;
3) added new passwords to password safe and only allowed access to technicians with authorization to shared accounts in the password safe;
4) changed the default passwords for all accounts;
5) procedurally enforced password requirements;
6) tracked password changes in account database to be changed at least every 15 calendar months;
7) submitted to WECC a Technical Feasibility Exception for the Cyber Assets in scope not capable of limiting the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts;
8) trained technicians to increase their knowledge of legacy devices and the functionality of those devices; and
9) implemented a bi-weekly or monthly CIP collaboration meeting between technical personnel, the CIP subject matter experts, the [redacted] management to discuss such details as review of default accounts, passwords, account access logging, and asset name/role tags during the annual cyber vulnerability assessments.

[redacted] NOC-2658 $0

| | |
|---|---|
| **Other Factors** | These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty.<br><br>WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant history consisted of an issue in 2011 and one in 2014 that posed minimal risk and are not indicative of a broader issue. |

[redacted] NOC-2658 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017634 | CIP-010-2 | R1: P1.1; P1.2; P1.3 | Medium | Moderate | 07/01/2016 | 05/18/2017 | Self-Report | 11/16/2018 | 08/13/2019 |

**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 May 22, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in potential noncompliance with CIP-010-2 R1. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one [redacted] within the Electronic Security Perimeter (ESP), used as the [redacted], and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA.

The Self-Report submitted for CIP-010-2 R1 also included noncompliance related to three EACMS that did not have logical port information in the baseline configuration as required by Part 1.1 sub-part 1.1.4; for [redacted] EACMS and [redacted] PACS, the entity failed to authorize and document changes that deviated from the existing baseline configuration as required by Part 1.2; and for [redacted] EACMS and the same [redacted] PACS, made changes that deviated from the existing baseline configuration without updating the baseline configuration within 30 calendar days from completing the change as required by Part 1.3.

After reviewing all relevant information, WECC determined the entity failed to develop baseline configurations for the BCA firmware and a port as required by CIP-010-2 R1 Part 1.1 sub-parts 1.1.1 and 1.1.4; develop a baseline configuration for [redacted] EACMS that included any logical network accessible ports as required by CIP-010-2 R1 Part 1.4 sub-part 1.1.4; authorize and document changes that deviated from the existing baseline configuration for [redacted] EACMS and [redacted] PACS as required by Part 1.2; and update the baseline configuration for [redacted] EACMS and [redacted] PACS as necessary within 30 calendar days of completing a change that deviated from the existing baseline configuration as required by CIP-010-2 R1 Part 1.3. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on May 18, 2017, when a port scan was completed, and the BCAs baseline configuration was updated, for a total of 322 days of noncompliance. The CIP-010-2 R1 instances related to the EACMS and PACS ended on June 7, 2017, when baseline configurations were authorized and updated, for a total of 342 days of noncompliance.

The root cause of the BCA violations was attributed to a lack of knowledge of the capabilities and functions of the BCA. The root cause of the violations related to the EACMS and PACS was attributed to less than adequate training and miscommunications. Specifically, steps were overlooked or not performed correctly because they were being performed infrequently.

**Risk Assessment**

WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, and WECC2017017634) individually and collectively posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-005-5 R1, CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to two EACMS and three PACS as described herein.

Failing to locate this BCA within an ESP and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a [redacted] which could affect [redacted] at the entity; thereby potentially affecting the reliability of the BPS. Failing to create a baseline for configuration results in the entity not being able to compare the current configuration to that which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets.

However, as compensation, the entity had implemented managed policy rules for monitoring the BCA and it was in a network segment that limited permissions to communicate with other parts of the entity's network, preventing the BCA from being accessed from other network segments unless a specific rule was created to allow that communication path. To control physical access, it was located within a PSP. The BCA was used as a [redacted], but there were two backup sources [redacted]. If the primary [redacted] (the BCA) were to fail, the system would automatically switch to one of the backup sources within 30 seconds. If [redacted], the System Operator would have received an alarm and could have utilized his capability to quickly switch the [redacted] to one of the backup devices, in the event they needed to manually bypass the BCA. Additionally, the entity implemented periodic internal audits which is how the instances with the EACMS and PACS were discovered. [redacted] No harm is known to have occurred.

**Mitigation**

To mitigate this violation, the entity has:

1) updated and authorized baseline configurations on the Cyber Assets in scope of these violations;
2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices;

[redacted] NOC-2658 $0

| | |
|---|---|
| | 3) updated its process to require all new Cyber Assets to go through a documented commissioning process before being connected to the operations network or deployed into an ESP to include documenting baseline configurations; and<br>4) updated the change management software to require:<br>a. a documented baseline configuration be completed as part of the commissioning process before deploying into an ESP; and<br>b. employees to update the baseline configuration on Cyber Assets before they can close the request for change. |
| **Other Factors** | These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty.<br><br>WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2658 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017018364 | CIP-006-6 | R1: P1.5 | Medium | Severe | 07/01/2016 | [redacted] | Compliance Audit | 11/6/2018 | 08/19/2019 |

| | |
|---|---|
| **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.)** | During a Compliance Audit conducted [redacted], WECC determined the entity, as a [redacted], had a potential noncompliance with CIP-006-6 R1 Parts 1.4 and 1.5. Specifically, for three PSPs controlling access to MIBCSs, the entity was unable to demonstrate that it was monitoring for unauthorized access through a physical access point into each PSP as required by CIP-006-6 R1 Part 1.4, and alarms or alerts in response to detected unauthorized access through a physical access point into each PSP were issued to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection as required by CIP-006-6 R1 Part 1.5.<br><br>The root cause of the violation was attributed to a misinterpretation of the Requirement Parts. Specifically, the entity believed if the PSPs were manned, no monitoring or automated alarming or alerting was needed, as such, the entity suppressed the alarms during business hours. This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable, and ended on [redacted] when the entity turned on the forced entry and door held open alarms during business hours, for a total of [redacted] days of noncompliance. |
| **Risk Assessment** | WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to monitor for unauthorized access through a physical access point into three PSPs and issue an alarm or alert in response to detected unauthorized access through a physical access point into said PSPs to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection, as required by CIP-006-6 R1 Parts 1.4 and 1.5.<br><br>Such failure could potentially result in an attacker gaining access to critical systems without the entity's knowledge, prolonging the time the attacker could use for nefarious purposes and possibly allow them to escape undetected. An attacker could also monitor, manipulate, or disable Cyber Assets without entity knowledge. However, as compensation the PSPs were manned [redacted] and one of the PSPs was equipped with a camera to observe the interior of the room. [redacted] |
| **Mitigation** | To mitigate this violation, the entity has:<br>1) activated alarms for existing forced entry and door held open alarms during business hours;<br>2) updated its technician procedure for testing physical security mechanisms to include language from the Standard as a reminder of the requirements for compliance which includes verifying that door forced open and held open alarms are always communicated to the System Operators; and<br>3) provided training to its technical personnel on what is required for compliance with CIP-006-6 R1 and the updated procedure. |
| **Other Factors** | These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty.<br><br>WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2658 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017911 | CIP-007-6 | R2: P2.3 | Medium | Severe | 10/01/2016 | 05/09/2017 | Self-Report | 09/21/2018 | 10/08/2019 |

| | |
|---|---|
| **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 July 7, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in potential noncompliance with CIP-007-6 R2. The Cyber Assets in scope were associated with the entity's MIBCS located [redacted]<br><br>Specifically, on August 26, 2016, the entity evaluated a security patch as applicable to [redacted] EACMS which it planned to install by September 30, 2016. Due to installation issues during the entity's conversion of its network from switching to routing, it was unable to install the security patch on the EACMS without interrupting service to its distribution Supervisory Control and Data Acquisition system. However, the entity did not create a dated mitigation plan within 35 calendar days of the evaluation completion as required by Part 2.3. On May 9, 2017, the entity was able to install the security patch without incident, for a total of 221 days of noncompliance.<br><br>The causes of this violation were attributed to: 1) a lack of controls to escalate security patch reminder emails that were not acted upon, 2) less than adequate patch management procedure in that it was not clear who was responsible for creating a mitigation plan or how the mitigation plan would be tracked to ensure completion by the stated date, and 3) software being used to track patches experiencing a server hardware failure which required the software to be installed on different hardware delaying the evaluation of security patches for applicability. |
| **Risk Assessment** | WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to create a dated mitigation plan within 35 calendar days of the evaluation completion for one security patch identified as applicable to [redacted] EACMS and failed to apply one applicable security patch to [redacted] BCAs within 35 calendars days of the evaluation completion, as required by CIP-007-6 R2 Part 2.3.<br><br>Such failures could have prolonged the presence of software vulnerabilities, which if exploited, could allow unauthorized access to or misuse of Cyber Assets that impact the reliability of the BPS. . However, as a corrective control for the BCAs and EACMS in scope, the entity ensured that the Control Systems engineer was in constant communication with the technicians, giving them verbal guidance on the issue during the noncompliance. Additionally, the PACS resided within an ESP and PSP with restricted electronic and physical access. The entity did not implement controls to prevent or detect these violations. [redacted] |
| **Mitigation** | To mitigate this violation, the entity has:<br>1) evaluated security patches released since the previous evaluation;<br>2) installed the applicable security patch.<br>3) provided additional training to technical staff on security patching activities;<br>4) implemented an internal control to daily back-up the server and provide an alert to technical staff with the status of the back-up;<br>5) updated its patch management program to clearly define the process for creating a mitigation plan when a security patch cannot be installed;<br>6) trained technicians on the new process;<br>7) created an annual task to review the patch management program with technicians to reinforce the entire patch management program;<br>8) updated its patch management program with language stating that upon determination of the applicability of a patch, a change request shall be created that same day with a due date one calendar month from the day of applicability determination;<br>9) changed the email task reminders from being sent to just the technicians but also to management staff and the [redacted], who will escalate past-due tasks to supervisors and follow-up to ensure the task is completed; and<br>10) implemented emailing reports of due or past due change request tickets to assignees and management as an additional control. |
| **Other Factors** | WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant history was an issue in 2014 that posed minimal risk and not indicative of broader compliance issues. |

[redacted] NOC-2658 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2018018977 | CIP-007-6 | R2: P2.3 | Medium | Severe | 09/29/2017 | 01/02/2018 | Self-Report | 10/05/2018 | 10/10/2019 |

| | |
|---|---|
| **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 12, 2018, the entity submitted a Self-Report stating, as a [redacted] it was in potential noncompliance with CIP-007-6 R2. The Cyber Assets in scope were associated with the entity's MIBCS located [redacted]<br><br>Specifically, for the first instance, on August 24, 2017, the entity evaluated a security patch as applicable to [redacted] EACMS which it planned to install by September 28, 2017. However, [redacted] and performing cyber vulnerability assessments, the installation of the security patch was overlooked, and no timely action was taken as required by Part 2.3. The security patch was installed on [redacted] of the EACMS on December 20, 2017, and a mitigation plan was created for the [redacted] remaining EACMS on December 21, 2017, for a duration of 84 days of noncompliance. For the second instance, on August 16, 2017, the entity evaluated a security patch as applicable to [redacted] BCAs which was outside of the 35 calendar day window from the previous evaluation which occurred on June 24, 2017, and again, [redacted], the entity was delayed in applying the security patch and went beyond the 35 calendar days since the evaluation completion, as required by Part 2.3. However, the entity applied the security patch on January 2, 2018, for a total of 96 days of noncompliance.<br><br>The causes of this violation were attributed to: 1) a lack of controls to escalate security patch reminder emails that were not acted upon, 2) less than adequate patch management procedure in that it was not clear who was responsible for creating a mitigation plan or how the mitigation plan would be tracked to ensure completion by the stated date, and 3) software being used to track patches experiencing a server hardware failure, which required the software to be installed on different hardware delaying the evaluation of security patches for applicability. |
| **Risk Assessment** | WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In these instances, the entity failed to create a dated mitigation plan within 35 calendar days of the evaluation completion for one security patch identified as applicable to [redacted] EACMS and failed to apply one applicable security patch to [redacted] BCAs within 35 calendars days of the evaluation completion, as required by CIP-007-6 R2 Part 2.3.<br><br>Such failures could have prolonged the presence of software vulnerabilities, which if exploited could allow unauthorized access to or misuse of Cyber Assets that impact the reliability of the BPS. . However, as a corrective control for the BCAs and EACMS in scope, the entity ensured that the Control Systems engineer was in constant communication with the technicians, giving them verbal guidance on the issue during the noncompliance. Additionally, the PACS resided within an ESP and PSP with restricted electronic and physical access. The entity did not implement controls to prevent or detect these violations. [redacted] |
| **Mitigation** | To mitigate this violation, the entity has:<br>1) evaluated security patches released since the previous evaluation;<br>2) installed the applicable security patch.<br>3) provided additional training to technical staff on security patching activities;<br>4) implemented an internal control to daily back-up the server and provide an alert to technical staff with the status of the back-up;<br>5) updated its patch management program to clearly define the process for creating a mitigation plan when a security patch cannot be installed;<br>6) trained technicians on the new process;<br>7) created an annual task to review the patch management program with technicians to reinforce the entire patch management program;<br>8) updated its patch management program with language stating that upon determination of the applicability of a patch, a change request shall be created that same day with a due date one calendar month from the day of applicability determination;<br>9) changed the email task reminders from being sent to just the technicians but also to management staff and the [redacted], who will escalate past-due tasks to supervisors and follow-up to ensure the task is completed; and<br>10) implemented emailing reports of due or past due change request tickets to assignees and management as an additional control. |
| **Other Factors** | These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty.<br><br>WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant history was an issue in 2014 that posed minimal risk and not indicative of broader compliance issues. |

[redacted] NOC-2658 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2018019483 | CIP-007-6 | R2: P2.2 | Medium | Lower | 01/31/2018 | 02/01/2018 | Self-Report | 05/21/2019 | 10/09/2019 |

| | |
|---|---|
| **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 April 5, 2018, the entity submitted a Self-Report stating that as a [redacted], it was in potential noncompliance with CIP-007-6 R2. The Cyber Assets in scope were associated with the entity's MIBCS located [redacted]<br><br>Specifically, on December 26, 2017, the entity evaluated security patches for [redacted] PACS. The next evaluation did not occur until February 1, 2018, which was beyond the requirement to evaluate at least once every 35 calendar days, per Part 2.2, which should have been January 31, 2018, for a total of two days of noncompliance.<br><br>The causes of this violation were attributed to, 1) a lack of controls to escalate security patch reminder emails that were not acted upon, 2) less than adequate patch management procedure in that it was not clear who was responsible for creating a mitigation plan or how the mitigation plan would be tracked to ensure completion by the stated date, and 3) software being used to track patches experiencing a server hardware failure which required the software to be installed on different hardware delaying the evaluation of security patches for applicability, respectively. |
| **Risk Assessment** | WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In these instances, the entity failed to at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1 for [redacted] PACS , as required by CIP-007-6 R2 Part 2.2.<br><br>Such failures could have prolonged the presence of software vulnerabilities, which if exploited could allow unauthorized access to or misuse of Cyber Assets that impact the reliability of the BPS. If an attacker gained access to a PACS, they could deny PSP access to authorized personnel or allow entry to unauthorized persons. The PSP controlled access to the MIBCS that if compromised could allow an attacker to manipulate, disable, or destroy Cyber Assets critical to the BPS. However, as a corrective control for the BCAs and EACMS in scope, the entity ensured that the Control Systems engineer was in constant communication with the technicians, giving them verbal guidance on the issue during the noncompliance. Additionally, the PACS resided within an ESP and PSP with restricted electronic and physical access. The entity did not implement controls to prevent or detect these violations. [redacted] |
| **Mitigation** | To mitigate this violation, the entity has:<br>1) evaluated security patches released since the previous evaluation;<br>2) installed the applicable security patch.<br>3) provided additional training to technical staff on security patching activities;<br>4) implemented an internal control to daily back-up the server and provide an alert to technical staff with the status of the back-up;<br>5) updated its patch management program to clearly define the process for creating a mitigation plan when a security patch cannot be installed;<br>6) trained technicians on the new process;<br>7) created an annual task to review the patch management program with technicians to reinforce the entire patch management program;<br>8) updated its patch management program with language stating that upon determination of the applicability of a patch, a change request shall be created that same day with a due date one calendar month from the day of applicability determination;<br>9) changed the email task reminders from being sent to just the technicians but also to management staff and the [redacted], who will escalate past-due tasks to supervisors and follow-up to ensure the task is completed; and<br>10) implemented emailing reports of due or past due change request tickets to assignees and management as an additional control. |
| **Other Factors** | These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty.<br><br>WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant history consisted of an issue in 2014 that posed minimal risk and not indicative of broader compliance issues. |

[redacted] NOC-2658 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017018365 | CIP-007-6 | R4: P4.2; Sub-part 4.2.2 | Medium | High | 07/01/2016 | [redacted] | Compliance Audit | 11/07/2018 | 10/09/2019 |

| | |
|---|---|
| **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.)** | During a Compliance Audit conducted [redacted], WECC determined the entity, as a [redacted], was in potential noncompliance with CIP-007-6 R4 Part 4.2 sub-part 4.2.2. Specifically, the entity failed to generate alerts for the detected failure of event logging on [redacted] BCAs, [redacted] EACMS, and [redacted] PACS associated with the MIBCS located at [redacted]<br><br>After reviewing all relevant information, WECC Enforcement concurs with the audit finding as stated above. The root cause was attributed to a design failure in that one of the rule building blocks designed to weed out false positives was in fact suppressing alerts for failed logins not associated with two-factor authentication. This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on August 29, 2017, when logging of detected failures was enabled on six of the Cyber Assets, and one Cyber Asset was decommissioned, for a total of 425 days of noncompliance. |
| **Risk Assessment** | WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to generate alerts for security events that included detected failure of event logging for [redacted] BCAs, [redacted] EACMS, and [redacted] PACS associated with the MIBCS located at [redacted] as required by CIP-007-6 R4 Part 4.1 sub-part 4.2.2.<br><br>The entity did not implement controls to detect or prevent this violation. However, as compensation the entity was able to collect logs locally even though alerting was not enabled. Additionally, as a corrective control for the BCAs and EACMS in scope, the entity ensured that the Control Systems engineer was in constant communication with the technicians, giving them verbal guidance on the issue during the noncompliance. The PACS resided within an ESP and PSP with restricted electronic and physical access. [redacted] |
| **Mitigation** | To remediate and mitigate this violation, the entity has:<br>1) updated the Windows auditing configuration and the SIEM alert rule which enabled alerting for detected failure of event logging for [redacted] Cyber Assets, and decommissioned one Cyber Asset;<br>2) updated its technician procedure to include more detail on configuring the Windows auditing section; and<br>3) completed initial and annual testing to ensure the SIEM is receiving and alerting on login attempts for the Cyber Assets in scope. |
| **Other Factors** | These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty.<br><br>WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant history consisted of an issue in 2014 that posed minimal risk and not indicative of broader compliance issues. |

[redacted] NOC-2654 $65,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017676 | CIP-002-5.1 | R1, P1.1, P1.2 | High | Lower | 7/1/2016 (when the Standard and Requirement became mandatory and enforceable on the entity) | 3/15/2019 (when the entity completed mitigating activities) | Self-Report | 3/15/2019 | 4/2/2019 |

**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 May 30, 2017, the entity submitted a Self-Report stating that, as a [redacted], it was in violation of CIP-002-5.1 R1.

Specifically, on March 8, 2017 during the planning and engineering activities associated with upgrading tone telemetry equipment at the [redacted] Control Center [redacted] the entity discovered that [redacted] Remote Terminal Unit (RTU) was not considered per CIP-002-5.1 R1; therefore, the RTU was not identified as a High Impact BES Cyber System (HIBCS) per CIP-002-5.1 R1 Part 1.1. The RTU was subsequently evaluated, through the entity's established BES Cyber Asset identification process, as being a Cyber Asset. The RTU was classified as a BES Cyber Asset (BCA) associated with a HIBCS, since the RTU resided in a facility containing HIBCS. [redacted] The entity determined that the RTU should be classified as a BES Cyber Asset, due to its role in the [redacted]. Subsequently, the RTU, due to its unique functionality, was recognized as a new class of BES Cyber System, which had not previously existed at the entity. In addition, the entity had an increase in scope from what it originally Self-Reported. During mitigation of the violation, the entity discovered [redacted] more RTUs that it failed to correctly identify as part of its Medium Impact BES Cyber Systems (MIBCS) located at several of its substations. Regarding the scope increase of [redacted] RTUs; the entity had incorrectly identified [redacted] of the RTUs as non-CIP devices; [redacted] of the RTUs were assessed as having the incorrect impact rating; and [redacted] of the RTUs were missing in the initial inventory and therefore were never identified. WECC determined that because these devices were BCAs within a HIBCS and MIBCS, the entire suite of CIP Standards and Requirements should be applied to these [redacted] devices, as applicable.

WECC determined that the entity failed to appropriately identify each BES Cyber System as required by CIP-002-5.1 R1 Part 1.1 and 1.2. Specifically, the entity did not identify and protect [redacted] RTUs as part of its HIBCS and MIBCS.

The root cause of the noncompliance was less than adequate process for properly considering each of its assets for purposes of identify the impact rating of BES Cyber Systems at each asset. Specifically, since the RTUs were utilized as [redacted], the entity believed they were non-BES assets, and therefore did not include them in the initial 15-minute impact analysis.

This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable on the entity, and ended on March 15, 2019, when the entity completed mitigating activities, for a total of 988 days of noncompliance.

**Risk Assessment**

WECC determined this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system BPS. In this instance, the entity failed to appropriately identify and protect [redacted] RTUs associated with its HIBCS and MIBCS, as required by CIP-002-5 R1 Part 1.1 and 1.2.

Such failure could have resulted in the compromise of the RTUs, any adjacent Cyber Assets, and the associated HIBCS or MIBCS; to include gaining complete control of the BCAs which could have led to misconfigurations, invalid data being sent, introduction of malicious firmware or lock-out of the BCAs; thereby potentially affecting the reliability and security of the BPS. However, as compensation, the RTUs were serially connected and as such had no routable network connectivity; baseline configuration information was maintained on the RTUs; the [redacted] RTU that should have been classified and protected as a HIBCS did not provide control functions and was configured to only transmit, not receive, data; and the other [redacted] RTUs that should have been classified and protected as MIBCS did not have control capabilities. All [redacted] RTUs had the protective measures of CIP-007-6 applied, as verified by WECC.

**Mitigation**

To remediate and mitigate this violation, the entity has:

1) correctly identified and documented the [redacted] RTUs in scope;
2) verified whether the RTUs were compliant with applicable CIP Standards and Requirements, and where they were not, applied the necessary protective measures of the CIP Standards and Requirements,
3) identified eight gaps in its control design and control operations;
4) worked with stakeholders to address the identified gaps;

[redacted] NOC-2654 $65,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017676 | CIP-002-5.1 | R1, P1.1, P1.2 | High | Lower | 7/1/2016 (when the Standard and Requirement became mandatory and enforceable on the entity) | 3/15/2019 (when the entity completed mitigating activities) | Self-Report | 3/15/2019 | 4/2/2019 |
| | | | 5) updated its process, procedures, and controls;<br>6) communicated changes to its Change Advisory Board; and<br><br>7) provided awareness and training to applicable individuals within its organization. | | | | | | |
| **Other Factors** | | | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>WECC considered the entity's CIP-002-5.1 R1 compliance history to be an aggravating factor in the penalty determination. | | | | | | |

**COVER PAGE**

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Compliance Exceptions in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

| Count | Violation ID | Category 1 | Category 2 | Category 3 | Category 4 | Category 5 | Category 6 | Category 7 | Category 8 | Category 9 | Category 10 | Category 11 | Category 12 | CEII PROTECTION (YEARS) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | NPCC2018019849 | Yes | | Yes | Yes | | | | | | Yes | | | Categories 3 – 4, 10: 2 years<br>Category 1: 3 years |
| 2 | NPCC2018019848 | Yes | | Yes | Yes | | | | | | Yes | | | Categories 3– 4, 10: 2 years<br>Category 1: 3 years |
| 3 | NPCC2018019847 | Yes | | Yes | Yes | | | | | | Yes | | | Categories 3– 4, 10: 2 years<br>Category 1: 3 years |
| 4 | NPCC2018019846 | Yes | | Yes | Yes | | | | | | Yes | | | Categories 3– 4, 10: 2 years<br>Category 1: 3 years |
| 5 | NPCC2018019845 | Yes | | Yes | Yes | | | | | | Yes | | | Categories 3– 4, 10: 2 years<br>Category 1: 3 years |
| 6 | | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | | |
| 11 | | | | | | | | | | | | | | |
| 12 | | | | | | | | | | | | | | |
| 13 | | | | | | | | | | | | | | |
| 14 | | | | | | | | | | | | | | |
| 15 | | | | | | | | | | | | | | |
| 16 | | | | | | | | | | | | | | |
| 17 | | | | | | | | | | | | | | |
| 18 | | | | | | | | | | | | | | |
| 19 | | | | | | | | | | | | | | |
| 20 | | | | | | | | | | | | | | |
| 21 | | | | | | | | | | | | | | |
| 22 | | | | | | | | | | | | | | |
| 23 | | | | | | | | | | | | | | |
| 24 | | | | | | | | | | | | | | |
| 25 | | | | | | | | | | | | | | |
| 26 | | | | | | | | | | | | | | |
| 27 | | | | | | | | | | | | | | |
| 28 | | | | | | | | | | | | | | |
| 29 | | | | | | | | | | | | | | |
| 30 | | | | | | | | | | | | | | |
| 31 | | | | | | | | | | | | | | |
| 32 | | | | | | | | | | | | | | |
| 33 | | | | | | | | | | | | | | |
| 34 | | | | | | | | | | | | | | |

Filing Date: October 31, 2019

[redacted] $84,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018019849 | CIP-005-5 | R1. | Medium | VSL - Severe | 7/1/2016 | 6/6/2018 | On-site Audit | 9/6/2018 | 7/31/2019 |

| | |
|---|---|
| **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.)** | During a Compliance Audit conducted from [redacted] NPCC determined that [redacted] (the entity), as a [redacted] was in noncompliance with CIP-005-5 R1 (1.3).<br><br>This violation started on July 1, 2016, when the entity failed to identify the reason for granting inbound and outbound access permissions on Electronic Access Points for one Medium Impact BES Cyber System [redacted] The violation ended on June 6, 2018, when the entity identified the reason for granting inbound and outbound access permissions and updated its firewall rules.<br><br>Specifically, several firewall rules within two (2) Medium Impact EACMS that provide Electronic Access Points to Medium Impact BES Cyber Systems did not have valid reasons for granting the access permission. There were rules with an "unknown" reason as well as rules that were no longer necessary.<br><br>The root cause of this violation was the lack of regular review and an undue reliance on a single person. Previous to the NERC CIP Audit, the review of firewall rules was the responsibility of one person who was unable to spend the necessary time on this type of review. The entity is now reviewing the firewall rules as a team and completing the reviews at least quarterly. |
| **Risk Assessment** | The violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Unnecessary EAP rules and active firewall rules where the reason for granting access is unknown can provide paths into the Electronic Security Perimeter (ESP) that can be exploited to gain unauthorized entry.<br><br>The entity has several systems in place to detect and prevent a potential incident. While some of the entity's firewall rules had been marked as unknown business reason or marked as to be removed, the firewall did have rules enabled to restrict access to and from the ESP. The entity also [redacted]<br><br>No harm is known to have occurred as a result of this violation. |
| **Mitigation** | To mitigate this violation, the entity<br>1) Reviewed and updated its Firewall rules; and<br>2) Initiated a process to review vulnerability assessment action plans quarterly that includes additional staffing |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2649 $84,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018019848 | CIP-005-5 | R2. | Medium | VSL - Moderate | 11/18/2016 | 6/7/2018 | On-site Audit | 12/10/2018 | 7/31/2019 |

| | |
|---|---|
| **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.)** | During a Compliance Audit conducted from [redacted] NPCC determined that [redacted] (the entity), as a [redacted], was in noncompliance with CIP-005-5 R2 (2.1.).<br><br>This violation started on November 18, 2016, when the entity failed to utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access the entity's Medium Impact BES Cyber Assets. The violation ended on June 7, 2018, when the entity disabled the interactive remote access. However, the [redacted]<br><br>The root cause of this violation was misinterpretation of both the standard and the recommended solutions provided by NERC. |
| **Risk Assessment** | The violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, failure to utilize an Intermediate System can provide attackers with additional vectors to attack the entity's Medium Impact BES Cyber Systems and gain unauthorized access.<br><br>The entity reduced the risk of an individual gaining unauthorized access [redacted]<br><br>While the entity is mitigating the violation, [redacted]<br><br>No harm is known to have occurred as a result of this violation. |
| **Mitigation** | To mitigate this violation, the entity:<br>1) Disabled VPN connections<br>2) Designed, along with a third-party vendor, a new Interactive Remote Access Solution as an alternate system to meet the requirements, and<br>3) Implemented the new Interactive Remote Access Solution. |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2649 $84,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018019847 | CIP-007-6 | R2. | Medium | VSL - Severe | 7/1/2016 | 7/19/2018 | On-site Audit | 11/28/2018 | 7/31/2019 |

| | |
|---|---|
| **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.)** | During a Compliance Audit conducted from [redacted] NPCC determined that [redacted] (the entity), as a [redacted] was in noncompliance with CIP-007-6 R2. (2.1.).<br><br>This violation started on July 1, 2016, when the entity failed to include three (3) Medium Impact BES Cyber Systems in its patch management process. The violation ended on July 19, 2018, when the entity added the three (3) Medium Impact BES Cyber Systems to its patch tracking spreadsheet and reviewed software updates for applicability.<br><br>Specifically, the entity had three unmanaged switches that are classified as Medium Impact BES Cyber Systems that it was not tracking or evaluating security patches for. The switches in scope provide [redacted]<br><br>The root cause of this violation was misunderstanding the applicability of the requirements. [redacted], which led to the exclusion of the switches from patch evaluations. |
| **Risk Assessment** | The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, not evaluating applicable systems for cyber security patches could leave the devices vulnerable to known exploits and could provide a bad actor the ability to gain unauthorized access to the Electronic Security Perimeter. If the switches in scope were taken offline, the entity's operators would lose the ability to remotely control the SCADA system. The entity in this instance reduced the risk of an attacker identifying a known unpatched exploit on the switches in scope by not configuring these switches to use a routable protocol.<br><br>[redacted]<br><br>If an attacker or expoit were to take the devices offline, the entity [redacted]. After the issue was discovered, the entity evaluated the patches that had been released for the switches in scope and determined they were not applicable.<br><br>No harm is known to have occurred as a result of this violation. |
| **Mitigation** | To mitigate this violation, the entity:<br>1) Updated its patch checklist to include a check for firmware;<br>2) Reviewed Firmware; and<br>3) Reviewed the CIP-007-6 Standard and its [redacted] process Documentation. |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2649 $84,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018019846 | CIP-007-6 | R5. | Medium | VSL - Severe | 7/1/2016 | 9/28/2018 | On-site Audit | 10/17/2018 | 7/31/2019 |

| | |
|---|---|
| **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.)** | During a Compliance Audit conducted from [redacted], NPCC determined that [redacted] (the entity), as a [redacted] was in noncompliance with CIP-007-6 R5. (5.4).<br><br>This violation started on July 1, 2016, when the entity failed to change known default passwords on 45 Medium Impact Cyber Assets. The violation ended on September 28, 2018, when the entity changed the known default password on applicable cyber assets that are capable of having a password set.<br><br>The root cause of this violation was failure to implement CIP Standard Requirements based on mitigating factors.<br><br>Specifically, the entity chose not to change passwords on the 45 applicable systems due to the following mitigating factors: substations do not have External Routable Connectivity. [redacted] |
| **Risk Assessment** | The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, unchanged known default passwords can provide attackers with unauthorized access to applicable Cyber Assets.<br><br>The entity reduced the risk of an unauthorized individual leveraging a known default password to access the 45 substation relays in scope by implementing a multi-layered security approach. [redacted]<br><br>No harm is known to have occurred as a result of this violation. |
| **Mitigation** | To mitigate this violation, the entity:<br>1) Changed passwords for the assets in scope; and<br>2) Updated its NERC CIP Training Program to include a reminder that all BCAs must have their default/manufacturer password changed before a BCA is put into service. |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2649 $84,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018019845 | CIP-010-2 | R3. | Medium | VSL - Severe | 7/1/2016 | 6/6/2018 | On-site Audit | 9/6/2018 | 7/31/2019 |

| | |
|---|---|
| **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.)** | During a Compliance Audit conducted from [redacted], NPCC determined that [redacted] (the entity), as a [redacted] was in noncompliance with CIP-010-2 R3 (3.4).<br><br>This violation started on July 1, 2016, when the entity failed to document the planned date of completion of the action plan and/or the execution status of the mitigation plans it created to mitigate vulnerabilities identified in its CIP-010-2 R3 vulnerability assessments. The violation ended on June 6, 2018, when the entity documented the completion date of the action plans and/or execution status of the mitigation plans.<br><br>Specifically, the entity completed its 2018 Cyber Vulnerability Assessment (CVA), but did not document the planned completion date and/or status of each of the CVA findings. Additionally, for many items, the subject matter experts were unsure of the status/planned completion date.<br><br>The root cause of this violation was lack of regular review by the entity and an undue reliance on a single person. Previous to the NERC CIP Audit, the maintenance of Vulnerability Assessments was the responsibility of one person who was unable to spend the necessary time on this responsibility. The oversight of vulnerability assessments is now the responsibility of a team and completing the review and updates occurs at least quarterly. |
| **Risk Assessment** | The violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, allowing vulnerabilites to go unmitigated could provide a potential attacker a vector to take advantage of technical flaws and configuration errors, which could allow an attacker to gain control of one Medium Impact BES Cyber System.<br><br>There were 40 items open on the entity's mitigation plan, some of the items were out of scope of NERC CIP, and many items were security improvements versus vulnerabilities. Five (5) of the forty (40) items did not have a documented status and action. The items impacted one Medium Impact BES Cyber System that is associated with System Operations [redacted]. Some of the vulnerabilties to be mitigated included: [redacted]<br><br>The entity reduced the risk of having systems with known vulnerabilities within its Electronic Security Perimeter (ESP) by [redacted]<br><br>No harm is known to have occurred as a result of this violation. |
| **Mitigation** | To mitigate this violation, the entity:<br>1) Updated its mitigation plans before the audit was complete; and<br>2) Initiated a process to review vulnerability assessment action plans quarterly that included additional staffing. |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

**COVER PAGE**

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notice of Penalty in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

| Count | Violation ID | Category 1 | Category 2 | Category 3 | Category 4 | Category 5 | Category 6 | Category 7 | Category 8 | Category 9 | Category 10 | Category 11 | Category 12 | CEII PROTECTION (YEARS) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | TRE2016016184 | Yes | | Yes | Yes | Yes | | | | Yes | | | | Category 1: 3 years; Category 2 – 12: 2 year |

Filing Date: September 26, 2019

[redacted] NOC-2646 No 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 |
|---|---|---|---|---|---|---|---|---|---|
| TRE2016016184 | CIP-002-5.1 | R1 | High | Lower | 7/1/2016 (when the Standard became mandatory and enforceable) | Present | Self-Certification | 11/7/2019 (approved completion date) | TBD |

| | |
|---|---|
| **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 [redacted], the Entity submitted a Self-Certification stating that, as a [redacted], it was in noncompliance with CIP-002-5.1 R1. Specifically, the Entity did not have or implement a process that considers [redacted] for the purposes of CIP-002-5.1 R1, Parts 1.1 through 1.3. As a result, the Entity did not identify each asset that contains a BES Cyber System. This issue began when CIP-002-5.1 became enforceable and continued after CIP-002-5.1a R1 became enforceable.<br><br>The root cause of this issue is that the Entity did not have any documented process for compliance with CIP-002-5.1 during the period leading up to CIP-002-5.1 becoming enforceable. As a result, the Entity did not document or implement processes necessary for compliance with CIP-002-5.1.<br><br>This noncompliance started on July 1, 2016, when CIP-002-5.1 R1 became enforceable and is currently ongoing. |
| **Risk Assessment** | This issue posed a moderate risk and did not pose a serious or substantial risk to the bulk power system based on the following factors. The failure to properly identify and classify a BES Cyber System increases the potential that the BES Cyber System will not receive the appropriate cyber security protections. The duration of this issue was approximately three years, lasting from July 1, 2016, when CIP-002-5.1 became enforceable, until the present. In addition, during the noncompliance, the Entity's [redacted] In addition, the Entity's initial review of its assets indicates that the Entity [redacted] BES Cyber Systems. |
| **Mitigation** | To mitigate the noncompliance, the Entity:<br><br>1) created a draft process for compliance with CIP-002-5.1a, which includes a preliminary draft of the identifications required by CIP-002-5.1a R1;<br>2) approved a documented internal compliance program, which includes a process for identifying applicable current and new Reliability Standards;<br>3) established a compliance committee, as described in the documented internal compliance program, which determines upcoming deadlines at regular meetings and implements the Entity's process for identifying applicable Reliability Standards; and<br>4) conducted training regarding the Entity's process for compliance with CIP-002-5.1a and regarding the Entity's overall compliance program.<br><br>Furthermore, the Entity submitted a Mitigation Plan to address the following actions that will be completed by November 7, 2019:<br><br>1) finalize and have CIP Senior Manager approve the draft identifications required by CIP-002-5.1a R1.<br><br>The Entity requires [redacted] and intends to complete this change before finalizing its process for compliance with CIP-002-5.1a R1. |
| **Other Factors** | [redacted]<br><br>Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance. |

**COVER PAGE**

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notice of Penalty in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

| Count | Violation ID | Category 1 | Category 2 | Category 3 | Category 4 | Category 5 | Category 6 | Category 7 | Category 8 | Category 9 | Category 10 | Category 11 | Category 12 | CEII PROTECTION (YEARS) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | MRO2017018152 | Yes | | Yes | Yes | | | | | | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 2 | MRO2017018150 | Yes | | Yes | Yes | | | | | | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |

Filing Date: August 29, 2019

[redacted] ("the Entity") NOC-2645 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| MRO2017018152 | CIP-007-6 | R5.7 | Medium | Severe | 7/1/2016 (when the Standard became mandatory and enforceable) | 10/31/2018 (when all applicable Cyber Assets were configured to either lockout or send a real-time alert) | Compliance Audit | 2/25/2019 | 2/25/2019 |

| | |
|---|---|
| **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.)** | During a Compliance Audit conducted from [redacted], MRO determined that the Entity, as a [redacted] was in violation of CIP-007-6 R5. Sampling conducted during the Compliance Audit and a subsequent extent of condition analysis uncovered multiple Cyber Assets that were not configured to either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, as required by P5.7.<br><br>The cause of the noncompliance was the Entity's failure to understand the full scope of the Standard and Requirement. The Entity believed that it was not required to file a Technical Feasibility Exception (TFE) if the device could not meet the requirements. Additionally, the Entity only considered whether a device had the capability to limit the number of unsuccessful authentication attempts, and failed to consider a device's event forwarding capability in conjunction with a collection system(s) that can generate an alert as a method for complying with P5.7. |
| **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). Two of the devices were granted a TFE that resolved the noncompliance. One of the devices had a low inherent risk to the BPS as it was a terminal server that transferred redundant information to map boards. The majority of remaining devices were receiving some level of protection at the time of the Compliance Audit. Prior to the audit, event forwarding had been turned on for these devices, which were configured to alert through an hourly report (MRO does not consider an alert from an hourly report to be compliant with P5.7). Finally, the Entity's [redacted] No harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the Entity:<br><br>1) submitted a TFE for two devices;<br>2) conducted an extent of condition review;<br>3) configured all applicable devices to either lockout or send a real-time alert;<br>4) augmented the account implementation form to add additional steps and permit the elevation of concerns for peer or supervisory review; and<br>5) validated updated process and provided training to SMEs through a table top exercise of actual assessment of applicable Cyber Asset(s). |
| **Other Factors** | MRO considered the scope of the noncompliance and the discovery method to be an aggravating factor in the disposition. Noncompliance that impacts a high population of applicable devices should be self-detected through internal controls. However, MRO determined that even though the noncompliance should not be eligible for Compliance Exception treatment, the noncompliance does not warrant a financial penalty given the minimal impact of the noncompliance upon the BPS.<br><br>MRO considered the Entity's CIP-007-6 R5 compliance history in determining the penalty. MRO determined that the Entity's compliance history should not serve as a basis for aggravating the penalty because the prior instances of noncompliance did not involve noncompliance with P5.7 and the current noncompliance was not caused by a failure to mitigate the prior noncompliance. |

[redacted] ("the Entity") NOC-2645 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| MRO2017018150 | CIP-010-2 | R1.1.2 | Medium | Lower | 7/1/2016 (when the Standard became mandatory and enforceable) | 5/11/2018 (updated the existing baselines to include all intentionally installed software) | Compliance Audit | 2/25/2019 | 2/25/2019 |

| | |
|---|---|
| **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.)** | During a Compliance Audit conducted from [redacted], MRO determined that the Entity, [redacted], was in violation of CIP-010-2 R1. Sampling conducted during the Compliance Audit and a subsequent extent of condition analysis uncovered multiple Cyber Assets that did not have baselines that included all installed commercially available software as required by P1.1. The Entity did not include the [redacted] software on the documented baseline for two devices and the Entity did not sufficiently identify the [redacted] software for numerous devices. The Entity would typically document its baselines in either its baseline tool or its patch management system (an alternate tracking system used to track patches and software items that cannot be tracked by its baseline tool). Both of these software applications could not be tracked in its baseline tool. The [redacted] software was included in its patch management system, but the reference was not specific enough to identify the unique or incremental software version that was installed on each Cyber Asset. The Entity did not detect the noncompliance during its vulnerability assessment because that process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible discrepancies.<br><br>The cause of the noncompliance was the Entity's deficient process for developing baselines and detecting errors or omissions. |
| **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). For all affected Cyber Assets, with the exception of two, the noncompliance was limited to not including sufficient detail regarding the software version as opposed to an omission. Further, the Entity had a software change process and change form specifically for the [redacted] software, reducing the risk of an inadvertent or unapproved change. The [redacted] software was also well managed by the Entity's SMEs, reducing the risk of an unexpected change to the [redacted] software. Finally, the Entity's [redacted]. No harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the Entity:<br><br>1) conducted an extent of condition analysis;<br>2) corrected the baselines for the impacted Cyber Assets;<br>3) improved the process to identify any commercially available software; and<br>4) validated the new process of identifying any commercially available or intentionally installed software. |
| **Other Factors** | MRO considered the scope of the noncompliance and the discovery method to be an aggravating factor in the disposition. Noncompliance that impacts a high population of applicable devices should be self-detected through internal controls. However, MRO determined that even though the noncompliance should not be eligible for Compliance Exception treatment, the noncompliance does not warrant a financial penalty given the minimal impact of the noncompliance upon the BPS.<br><br>MRO considered the Entity's compliance history and determined there were no relevant instances of noncompliance. |

**COVER PAGE**

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notice of Penalty in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

| Count | Violation ID | Category 1 | Category 2 | Category 3 | Category 4 | Category 5 | Category 6 | Category 7 | Category 8 | Category 9 | Category 10 | Category 11 | Category 12 | CEII PROTECTION (YEARS) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | NPCC2018020347 | Yes | | Yes | Yes | | | | | Yes | | | | Categories 3 – 4: 2 years Categories 1, 9: 3 years |
| 2 | NPCC2018020348 | Yes | | Yes | Yes | | | | | Yes | | | | Categories 3 – 4, 2 years Categories 1, 9: 3 years |
| 3 | NPCC2018020350 | Yes | | Yes | Yes | | | | | Yes | | | | Categories 3 – 4, 2 years Categories 1, 9: 3 years |
| 4 | NPCC2018020346 | Yes | | Yes | Yes | | | | | Yes | | | | Categories 3 – 4, 2 years Categories 1, 9: 3 years |
| 5 | NPCC2018020351 | Yes | | Yes | Yes | | | | | Yes | | | | Categories 3 – 4, 2 years Categories 1, 9: 3 years |
| 6 | WECC2018020039 | | | Yes | Yes | | | | Yes | | | | | Category 2 – 12: 2 year |
| 7 | WECC2018020282 | | | Yes | Yes | | | | | | | | | Category 2 – 12: 2 year |
| 8 | WECC2016015862 | | | Yes | Yes | | | | | | | Yes | Yes | Category 2 – 12: 2 year |
| 9 | WECC2017018174 | Yes | | Yes | Yes | | | | | | | | | Category 1: 3 years; Category 2 – 12: 2 year |
| 10 | WECC2017017885 | Yes | | Yes | Yes | | | | | | | | | Category 1: 3 years; Category 2 – 12: 2 year |
| 11 | WECC2018019006 | | | Yes | Yes | | | | | Yes | | | | Category 1: 3 years; Category 2 – 12: 2 year |
| 12 | WECC2017016941 | Yes | | Yes | Yes | | | | | Yes | | | | Category 1: 3 years; Category 2 – 12: 2 year |
| 13 | WECC2017016928 | Yes | Yes | Yes | Yes | | | | | Yes | | | | Category 1: 3 years; Category 2 – 12: 2 year |
| 14 | WECC2017016939 | Yes | | Yes | Yes | | | | | Yes | | | | Category 1: 3 years; Category 2 – 12: 2 year |
| 15 | WECC2017016938 | | | Yes | Yes | | | | | Yes | | | | Category 1: 3 years; Category 2 – 12: 2 year |
| 16 | WECC2017016940 | Yes | | Yes | Yes | | | | Yes | Yes | | | | Category 1: 3 years; Category 2 – 12: 2 year |
| 17 | WECC2017016926 | Yes | | Yes | Yes | | | | Yes | Yes | Yes | Yes | | Category 1: 3 years; Category 2 – 12: 2 year |
| 18 | WECC2017016929 | | | Yes | Yes | | | | Yes | Yes | | | | Category 1: 3 years; Category 2 – 12: 2 year |
| 19 | | | | | | | | | | | | | | |
| 20 | | | | | | | | | | | | | | |
| 21 | | | | | | | | | | | | | | |
| 22 | | | | | | | | | | | | | | |
| 23 | | | | | | | | | | | | | | |
| 24 | | | | | | | | | | | | | | |
| 25 | | | | | | | | | | | | | | |
| 26 | | | | | | | | | | | | | | |
| 27 | | | | | | | | | | | | | | |
| 28 | | | | | | | | | | | | | | |
| 29 | | | | | | | | | | | | | | |
| 30 | | | | | | | | | | | | | | |

[redacted] NOC-2636 $10,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020347 | CIP-002-5.1a | R1.1, R1.2, R1.3 | High | Lower | 3/29/2017 | 9/4/2018 | Self-Report | 9/4/2018 | 12/12/2018 |

| | |
|---|---|
| **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 September 5, 2018, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered in June of 2017 it was in noncompliance with CIP-002-5.1a R1. The entity discovered the noncompliance through a third-party company it contracted with to evaluate its compliance program.<br><br>This violation started on March 29, 2017 when the entity failed to implement a process to identify its BES Cyber Systems. The violation ended on September 4, 2018 when the entity developed a process for identifying and rating its BES Cyber Systems.<br><br>Specifically, the facility in scope [redacted] the entity discovered there was a new version of the CIP standards and that it was not in compliance. The entity then hired a third-party company to help them evaluate and implement a compliance program.<br><br>The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations [redacted]. In particular, the entity did not incorporate amendments to the NERC Reliability Standards into its compliance program. Therefore, certain requirements were not reviewed, assessed, or implemented when the entity [redacted]. |
| **Risk Assessment** | The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. Specifically, by failing to identify the impact level of its assets, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope has been classified as a Low Impact Asset that runs a few times a year. The entity has a Process Information (PI) system that is used for real-time performance monitoring and diagnostics. This system sends information to [redacted]; if this connection were interrupted, the entity would provide data to [redacted] via phone.<br><br>The entity reduced the risk of its system becoming compromised by [redacted]. The Low Impact system is further protected from unauthorized physical access. [redacted]. |
| **Mitigation** | To mitigate this violation, the entity:<br>1. contracted third-party company to create compliance program; and<br>2. developed and implement process for identifying the impact level of assets in accordance with CIP-002-5.1 Attachment 1.<br><br>To prevent recurrence, the entity:<br>1. implemented automated system/tasks to ensure NERC activities are tracked and completed. |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.<br><br>Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility. |

[redacted] NOC-2636 $10,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020348 | CIP-002-5.1a | R2.1, R2.2 | Lower | High | 3/29/2017 | 9/4/2018 | Self-Report | 9/4/2018 | 12/12/2018 |

| | |
|---|---|
| **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 September 5, 2018, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered on June of 2017 it was in noncompliance with CIP-002-5.1a R2. The entity discovered the noncompliance through a third-party company it contracted with to evaluate its compliance program.<br><br>This violation started on March 29, 2017 when the entity failed to implement a process to identify its BES Cyber Systems, and therefore did not review or have CIP Senior Manager Approval of the identified impact levels. The violation ended on September 4, 2018 when the entity developed a process for identifying and rating its BES Cyber Systems, designated a CIP Senior Manager and reviewed and approved its identified impact level.<br><br>Specifically, the facility in scope [redacted] the entity discovered there was a new version of the CIP standards and that it was not in compliance. The entity then hired a third-party company to help them evaluate and implement a compliance program.<br><br>The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations [redacted]. In particular, the entity did not incorporate amendments to the NERC Reliability Standards into its compliance program. Therefore, certain requirements were not reviewed, assessed, or implemented when the entity [redacted]. |
| **Risk Assessment** | The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify the impact level of its assets, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope has been classified as a Low Impact Asset that runs a few times a year. The entity has a PI system that sends information to [redacted], if this connection were interrupted the entity would provide data to [redacted] via phone.<br><br>The entity reduced the risk of its system becoming compromised by [redacted]. The Low Impact system is further protected from unauthorized physical access. [redacted]. |
| **Mitigation** | To mitigate this violation, the entity:<br>1. contracted third-party company to create compliance program;<br>2. developed and implement process for identifying the impact level of assets in accordance with CIP-002-5.1 Attachment 1;<br>3. designated a CIP Senior Manager; and<br>4. reviewed and obtained CIP Senior Manager Approval of the identified impact level.<br><br>To prevent recurrence, the entity:<br>1. implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.<br><br>Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility. |

[redacted] NOC-2636 $10,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020350 | CIP-003-6 | R1.1, R1.2 | Medium | High | 4/1/2017 | 9/4/2018 | Self-Report | 9/18/2018 | 5/24/2019 |

| | |
|---|---|
| **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 September 5, 2018, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered in June of 2017 it was in noncompliance with CIP-003-6 R1. The entity discovered the noncompliance through a third-party company it contracted with to evaluate its compliance program.<br><br>This violation started on April 1, 2017 when the entity failed to implement documented cyber security policies that address Cyber Security Awareness and Cyber Security Incident Response for its low impact BES Cyber System. The violation ended on September 4, 2018 when the entity's CIP Senior Manager reviewed and approved its CIP-003-6 Cyber Security – Security Management Controls policy.<br><br>Specifically, the facility in scope [redacted] the entity discovered there was a new version of the CIP standards and that it was not in compliance. The entity then hired a third-party company to help them evaluate and implement a compliance program.<br><br>The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations [redacted]. In particular, the entity did not incorporate amendments to the NERC Reliability Standards into its compliance program. Therefore, certain requirements were not reviewed, assessed, or implemented when the entity [redacted]. |
| **Risk Assessment** | The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify the impact level of its assets and create and review one or more documented cyber security policies, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope has been classified as a Low Impact Asset that runs a few times a year. The entity has a PI system that sends information to [redacted], if this connection were interrupted the entity would provide data to [redacted] via phone.<br><br>The entity reduced the risk of its system becoming compromised by [redacted]. The Low Impact system is further protected from unauthorized physical access. [redacted]. |
| **Mitigation** | To mitigate this violation, the entity:<br>1. contracted third-party to create compliance program;<br>2. implemented Cyber Security Awareness training;<br>3. implemented Cyber Security Incident Response Plan;<br>4. performed tabletop exercise of Cyber Security Incident Response Plan; and<br>5. created a facility specific CIP-003-6 procedure.<br><br>To prevent recurrence, the entity:<br>1. implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed. |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.<br><br>Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility. |

[redacted] NOC-2636 $10,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020346 | CIP-003-6 | R2. | Lower | Severe | 4/1/2017 | 9/4/2018 | Self-Report | 9/6/2018 | 5/24/2019 |

| | |
|---|---|
| **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 September 5, 2018, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered in June of 2017 it was in noncompliance with CIP-003-6 R2. The entity discovered the noncompliance through a third-party company it contracted with to evaluate its compliance program.<br><br>This violation started on April 1, 2017 when the entity failed to implement documented cyber security policies that address Cyber Security Awareness and Cyber Security Incident Response for its low impact BES Cyber System. The violation ended on September 4, 2018 when the entity implemented its approved CIP-003-6 Cyber Security – Security Management Controls policy. .<br><br>Specifically, the facility in scope [redacted] the entity discovered there was a new version of the CIP standards and that it was not in compliance. [redacted] did not have in place documented cyber security plans that addressed the sections in CIP-003-6 Attachment 1. The entity then hired a third-party company to help them evaluate and implement a compliance program.<br><br>The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations [redacted]. In particular, the entity did not incorporate amendments to the NERC Reliability Standards into its compliance program. Therefore, certain requirements were not reviewed, assessed, or implemented when the entity [redacted]. |
| **Risk Assessment** | The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify the impact level of its assets and create and review one or more documented cyber security policies, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope has been classified as a Low Impact Asset that runs a few times a year. The entity has a PI system that sends information to [redacted], if this connection were interrupted the entity would provide data to [redacted] via phone.<br><br>The entity reduced the risk of its system becoming compromised by [redacted]. The Low Impact system is further protected from unauthorized physical access. [redacted]. |
| **Mitigation** | To mitigate this violation, the entity:<br>1. Contracted third-party to create compliance program;<br>2. Implemented Cyber Security Awareness training;<br>3. Implemented Cyber Security Incident Response Plan;<br>4. Performed tabletop exercise of Cyber Security Incident Response Plan; and<br>5. Created a facility specific CIP-003-6 procedure.<br><br>To prevent recurrence, the entity:<br>1. implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.<br><br>Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility. |

[redacted] NOC-2636 $10,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020351 | CIP-003-6 | R3. | Medium | Severe | 4/1/2017 | 9/4/2018 | Self-Report | 9/4/2018 | 12/12/2018 |

| | |
|---|---|
| **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 September 5, 2018, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered in June of 2017 it was in noncompliance with CIP-003-6 R3. The entity discovered the noncompliance through a third-party company it contracted with to evaluate its compliance program.<br><br>This violation started on April 1, 2017 when the entity failed to identify a CIP Senior Manager by name. The violation ended on September 4, 2018 when the entity designated a CIP Senior Manager.<br><br>Specifically, the facility in scope [redacted] the entity discovered there was a new version of the CIP standards and that it was not in compliance. The entity then hired a third-party company to help them evaluate and implement a compliance program.<br><br>The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations [redacted]. In particular, the entity did not incorporate amendments to the NERC Reliability Standards into its compliance program. Therefore, certain requirements were not reviewed, assessed, or implemented when the entity [redacted]. |
| **Risk Assessment** | The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify a CIP Senior Manager the entity didn't have an individual responsible for ensuring compliance. As a result the entity failed to identify the impact level of its assets and failed to create and review one or more documented cyber security policies. By failing to implement these controls to ensure compliance, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope has been classified as a Low Impact Asset that runs a few times a year. The entity has a PI system that sends information to [redacted], if this connection were interrupted the entity would provide data to [redacted] via phone.<br><br>The entity reduced the risk of its system becoming compromised by [redacted]. The Low Impact system is further protected from unauthorized physical access. [redacted]. |
| **Mitigation** | To mitigate this violation, the entity:<br>1. identified and documented by name the CIP Senior Manager;<br>2. contracted third-party to create compliance program; and<br>3. created a facility specific CIP-003-6 procedure.<br><br>To prevent recurrence, the entity:<br>1. implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed. |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.<br><br>Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility. |

[redacted]

No 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2018020039 | CIP-004-3a | R3 | Medium | High | 8/6/2015 (when electronic access was provisioned without a PRA) | 5/3/2018 (when a PRA was performed) | Self-Report | 5/3/2018 | 4/3/2019 |

| | |
|---|---|
| **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 July 18, 2018, the entity submitted a Self-Report stating that, as a [redacted], it was in violation of CIP-004-3a R3.<br><br>The entity conducted an internal audit beginning in October 2017, as part of mitigation related to two previous violations for the same Standard and Requirement and realized a gap in adherence to its procedures for ensuring that a Personnel Risk Assessment (PRA) was conducted for individuals authorized for electronic access to Critical Cyber Assets (CCAs). In January of 2018, the affected departments that utilize those access management procedures met to discuss and address the gap in adherence, with internal controls. While implementing one of the controls, the entity identified one employee who was authorized and granted electronic access on August 6, 2015 to software on a CCA, used for outage coordination, without first having a completed PRA for the person. Because the entity did not perform a PRA on the employee, they were not in the PRA tracking database, which the entity used to help reconcile employees with CIP electronic and physical access.<br><br>The entity did not have any other controls in place within its processes to identify the issue sooner. On May 3, 2018, the entity performed the missing PRA for the one employee, for a total of 1,002 days of noncompliance.<br><br>The root cause of this violation was the entity's personnel not following documented procedures, which required processing of CIP electronic access requests through the department that performed the PRAs, prior to the access being granted.<br><br>After reviewing all relevant information, WECC determined the entity failed to conduct a PRA for one employee prior to granting electronic access to CCAs, as required by CIP-004-3a R3. |
| **Risk Assessment** | This violation posed a moderate risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to conduct a PRA for one employee prior to granting electronic access to CCAs, as required by CIP-004-3a R3.<br><br>The entity had no internal controls implemented to detect or prevent this violation for nearly three years. Given the extent of the employee's access within the outage scheduling software, had they had malicious intent, they could have caused significant harm. However, the employee was authorized to have the electronic access and was sufficiently trained to use the software to perform their job. Additionally, the internal control, that was implemented in place as part of the mitigation of previous violations, identified the single individual that did not have the PRA in the tracking database. If there were any other individuals missing the PRA, this control would have identified it. |
| **Mitigation** | To mitigate this violation, the entity:<br><br>1) completed a PRA for the one employee in scope;<br>2) re-circulated its PRA verification procedure to applicable personnel; and<br>3) held a meeting with applicable personnel to discuss and train for the procedures and processes that need to be followed for compliance. During this meeting the attendees agreed that the [redacted] will verify PRAs with [redacted] if the personnel requesting access is new to their system. If the personnel is requesting additional access to an area, the [redacted] will verify access by checking the name against the PRA Audit SharePoint list maintained by [redacted] |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor The entity identified this violation utilizing an internal control it had implemented as part of the mitigation of a previous violation.<br>[redacted]<br><br>WECC considered the entity's CIP-004-3a R3 compliance history in determining the disposition track. WECC considered the entity's CIP-004-3a R3 compliance history to be an aggravating factor in the disposition determination. |

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2018020282 | CIP-006-3c | R4 | Medium | Severe | [redacted] (when the first employee entered the PSP using a hard key) | 8/30/2016 (when the ability to access the PSP utilizing a hard key was removed) | Self-Report | 5/15/2017 | 10/4/2018 |

**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 [redacted], WECC created a violation record for the entity, as a [redacted], for a violation of CIP-006-3c R4. The entity had increased the scope of an existing violation of CIP-006-6 R1, given NERC Violation ID [redacted], to include CIP-006-3c R4. WECC created the new violation record because the increase in scope had a start date of [redacted], which was before July 1, 2016, the mandatory and enforceable date of CIP Version 5.

Specifically, on [redacted], during a scheduled substation service power outage, which affected availability of the electronic access controls, the entity's employee was able to use a hard key to enter the control house Physical Security Perimeter (PSP) at a substation containing a Medium Impact BES Cyber System (MIBCS) with External Routable Connectivity (ERC). The door that was accessed had been designated to require the use of an alternate access key for entry to the PSP when electronic access controls failed or were out of service. Use of the alternate access key was intended to invoke the entity's procedure which required the Alarm Monitoring Station (AMS) to authenticate the person requesting access to the alternate access key, thus enforcing two-factor authentication per the entity's physical security plan. However, the door's key core had not been changed out to the alternate access key core required for MIBCS with ERC, per the established entity security standards, during the entity's NERC CIP V5 implementation efforts. Additionally, on August 9, 2016, another employee utilized an issued hard key to enter a control house PSP containing MIBCS with ERC. Similar to the issue mentioned above, the key core at this PSP door should have been switched out to comply with the entity's Alternate Access Key procedure which required two-factor authentication before access was permitted.

After reviewing all relevant information, WECC determined the entity failed to appropriately implement its documented operational and procedural controls to manage physical access at all access points to the PSP twenty-four hours a day, seven days a week as required by CIP-006-3c R4.

The root cause of the violation was less than adequate internal controls. Specifically, the entity's CIP Version 5 project documentation did not incorporate a procedure to confirm all PSP door lock cores were replaced to comply with the entity's physical security plan.

This violation began on [redacted], when the first employee entered the PSP using a hard key, and ended on August 30, 2016, when the entity removed the ability to access the PSP through the alternate access door with the hard key, for a total of [redacted] days of noncompliance.

**Risk Assessment**

WECC determined this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to appropriately implement its documented operational and procedural controls to manage physical access at all access points to the PSP twenty-four hours a day, seven days a week as required by CIP-006-3c R4.

However, as compensation, the entity had a very limited the number of individuals with access to its PSPs and were only those who have a legitimate business need and who had completed Personnel Risk Assessments (PRAs) and CIP training. At the time of the violation the employees who accessed the PSPs were authorized to be there and had valid PRAs. No harm is known to have occurred.

**Mitigation**

To mitigate this violation, the entity:

1) changed the energized access key cores to the alternate access key cores at the two PSPs doors in scope;

2) conducted an audit on all alternate access key PSP doors containing MIBCS to ensure the core locks were appropriate. The entity identified six sites with key cores that were not set for utilization of alternate access keys. The entity mitigated by either installing the alternate access key cores or by inserting a non-key core lock and door handle to prohibit the door from being opened from the outside; and

| | |
|---|---|
| | 3) updated its physical security plans to include a test checklist as an internal control. The checklist requires that the tester attempt to use a specific key in all PSP door key cores and confirm that all other PSP doors have blank key cores. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor.<br><br>[redacted]<br><br>WECC considered the entity's CIP-006 -3c R4 compliance history in determining the disposition track and considered two previous violations to be an aggravating factor in the disposition determination.<br><br>Additional compliance history related to CIP-006-6 R4 were not relevant because the associated violations were related to failing to maintain logs for physical access to PSPs; the entity's visitor control program; and its personnel risk assessment program, respectively, which involved different conduct than the violations in this disposition. |

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2016015862 | CIP-006-6 | R1 P1.1,1.2, 1.3, and 1.4 | Medium | Severe | [redacted] | 7/19/2017 (when all issues were remediated) | Self-Report | 11/14/2017 | 7/26/2018 |

**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 [redacted], the entity submitted a Self-Report stating that, as [redacted], it was in violation of CIP-006-6 R1. This noncompliance was identified by WECC auditors during the entity's CIP Version 3 to CIP Version 5 transitional audit on [redacted]. [redacted] WECC auditors provided the entity with an Area of Concern in accordance with guidance provided by NERC for CIP Version 5 transition audits. The entity then self-reported the noncompliance after receiving the audit report, knowing that the noncompliance was still occurring.

Specifically, several issues were identified with the implementation of CIP-006-6 R1 Parts 1.1, 1.2, 1.3, and 1.4.

a. Regarding issue one (R1), the entity had a conference room located in its main building that was identified as a dual-purpose conference room that at times also functioned as a PSP. When not in use as a PSP, the entity did not ensure that all of the protective measures required in the Standards were applied.

b. Regarding issue two (R1 Part 1.1), the entity's Physical Access Control Systems (PACS) were protected by a PSP; however, the entity utilized mechanical locks and keys that were not managed with operational or procedural controls defined in its physical security plan.

c. Regarding issue three (R1 Part 1.2), the entity's employee identified [redacted] substations with an access door in the control house basement connected to a tunnel, designated as part of the PSP, that were found to have an emergency release (Safety) handle that did not require authentication for access into the PSP. The other end of the tunnel led to the outside. Entry by this manner was treated as an intrusion and would generate a response by security but did not require any type of authentication to gain access. The entity implemented this alternate path to comply with the National Fire Protection Association requirements for egress from the confined areas of the tunnel because the PSP space was concluded to be a necessary evacuation route.

d. Regarding issue four (R1 Part 1.3), the entity did not ensure a minimum of two-factor authentication to a PSP access point at the primary Control Center containing High Impact BES Cyber Systems (HIBCS). The management of the hard keys was not well documented and did not follow a two-factor authentication for use and distribution.

e. Regarding issue 5 (R1 Part 1.4), the entity did not implement continuous monitoring of windows, glass, and hatches for intrusion detection when PSP motion sensors were disabled, per its procedure, throughout the workday if one or more persons entered the PSP at six substations containing MIBCS. The disabling of the motion sensors also disabled intrusion monitoring through windows, glass, and some hatches at those substations. Specifically, on July 21, 2016, the entity received a loss of communication alarm from a PSP at a substation containing MIBCS with ERC. The entity's AMS operators notified Dispatch at the 15- and 30-minute marks concerning the loss of communications with the site; however, Dispatch did not direct and authorize human observation per the established procedures.

After reviewing all relevant information, WECC Enforcement determined the entity; 1) failed to define operation or procedural controls to restrict physical access; 2) failed to utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access; where technically feasible; 3) failed to utilize two or more different physical access controls to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access; and 4) failed to monitor for unauthorized access through a physical access point into a PSP, as required by CIP-006-6 R1 Parts 1.1, 1.2, 1.3, and 1.4, respectively.

The root cause of these violations was the lack of open and coordinated communication. Specifically, the different departments within the entity were not communicating or collaborating effectively during its implementation of Version 5 of the CIP Standards and Requirements.

| | |
|---|---|
| | This violation began on [redacted] and ended on July 19, 2017, when the entity remediated all the issues, for a total of [redacted] days of noncompliance. |
| **Risk Assessment** | WECC determined these violations posed a moderate risk and did not pose a serious and substantial risk to the reliability of the BPS. In these instances, the entity, 1) failed to define operation or procedural controls to restrict physical access; 2) failed to utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access; 3) where technically feasible, failed to utilize two or more different physical access controls to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access; and 4) failed to monitor for unauthorized access through a physical access point into a PSP, as required by CIP-006-6 R1 Parts 1.1, 1.2, 1.3, and 1.4, respectively.<br><br>However, the entity implemented good controls. All its PACS devices were within a designated PSP; the number of people with access to the PSPs was limited to those who had a legitimate need to access the area, and they all had PRAs. The PACS servers were monitored for unauthorized access. Additionally, the cabinets which housed the PACS control panels included tamper alarms, which would alert security officers if a cabinet were inappropriately accessed. The access tunnels were monitored around the clock, the use of the handle would have set off an alarm, and the tunnels are not accessible from the outside. Authentication, logging, and monitoring of physical access was captured for all individuals that entered the tunnel, which was the only way into the PSPs. |
| **Mitigation** | To mitigate CIP-006-6 R1 Part 1.1, the entity has:<br>1) developed a key control program for alternate access to PACS servers;<br>2) changed the field site location from a designated PSP to a secure area and updated documentation;<br>3) provided test results after the PACS system was moved to its new secure areas; and<br>4) provided guidance for applicable personnel for identifying the required security controls for a PACS system that resides within a PSP or outside of a PSP.<br><br>To mitigate CIP-006-6 R1 Part 1.2, the entity has:<br>1) identified all sites containing MIBCS that utilize the pull handle safety device;<br>2) reviewed each site's tunnels and hatches for conformance to its physical security standards;<br>3) developed plans for sites that deviated from the physical security standard to bring the tunnels and hatches into compliance with its physical security standards;<br>4) reviewed all hatches and service doors to tunnels that are not a PSP access point to ensure they are locked down and cannot be opened from the exterior of the tunnel space;<br>5) ensured all tunnel doors into the PSP with the pull handle are monitored 24/7, and the use of the pull handle immediately generates a forced door event to the AMS;<br>6) tested that the alarms were working; and<br>7) updated the response procedure that the AMS operators use to investigate "Forced Door" alarms. The pull handles are documented on all PSP drawings, and AMS operators are trained to respond to all forced door events.<br><br>To mitigate CIP-006-6 R1 Part 1.3, the entity has:<br>1) collected and inventoried all assigned keys to the primary Control Center;<br>2) developed and implemented a procedure for primary Control Center key control. The referenced operations bulletin was sent to AMS for their action, and the process was made available to employees;<br>3) updated the Physical Security Plan to change security responsibilities to security personnel and posted an operations bulletin that describes the processes to the Control Center employees;<br>4) assigned the PSP keys for the primary Control Center to Physical Security organization and stored them within a secure key box residing in the security AMS;<br>5) moved the key management program to the Physical Security organization; and<br>6) audited the updated procedure for effectiveness.<br><br>To mitigate CIP-006-6 R1 Part 1.4, the entity has:<br>1) enhanced the training program and procedures between AMS and Dispatch to deploy resources for physical observation within the 30 minutes required by its Loss of Security System procedure; and |

| | |
|---|---|
| | 2) implemented a script for contractors to read as part of their enhanced procedures between AMS and Dispatch. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor.<br><br>[redacted]<br><br>WECC considered the entity's CIP-006-6 R1 compliance history and determined there were no relevant instances of noncompliance. |

[redacted] $80,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017018174 | CIP-006-3c | R1; R1.1 | Medium | Severe | 1/13/2012 (when the substation became a Critical Asset) | 12/9/2016 (when the relays were disconnected from the ESP) | Self-Report | 6/13/2018 | 11/1/2018 |

**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 August 14, 2017, the entity submitted a Self-Report stating that, as a [redacted], it was in violation with CIP-006-3c R1.

Specifically, the entity reported that on June 4, 2015, it discovered that [redacted] that were part of an Electronic Security Perimeter (ESP) were located outside the designated Physical Security Perimeter (PSP) of a substation. The [redacted] were located in a [redacted], which was protected by the perimeter fence but outside the documented PSP. [redacted] of the [redacted] were used for Supervisory Control and Data Acquisition (SCADA) control between [redacted], and the other [redacted] were used for protection of [redacted] Although the entity identified the issue in 2015, it mistakenly marked the issue as remediated. On October 10, 2016, while performing a site validation assessment for CIP Version 5, the entity discovered that the [redacted] remained connected to the ESP and were still located outside the PSP.

After reviewing all relevant information, WECC Enforcement determined that the entity failed to ensure that all Cyber Assets within an ESP resided within an identified PSP, as required by CIP-006-3c R1.1.

The root cause of the violation was a less than adequate process. Specifically, the entity did not evaluate the ESP and PSP at the substation for compliance before or after it was energized.

WECC determined that this violation began on January 13, 2012, when the substation became a Critical Asset for CIP Version 3, and ended on December 9, 2016, when the [redacted] were disconnected from the ESP, for a total of 1,793 days of noncompliance.

**Risk Assessment**

WECC determined that this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to ensure that [redacted] Cyber Assets within an ESP resided within an identified PSP, as required by CIP-006-3c R1.1.

The entity implemented no preventive or detective controls as this violation was not discovered within a timely manner and only because the entity was implementing a newer version of the CIP Standards. Additionally, the entity had weak corrective controls as the violation was originally discovered in 2015, but marked as resolved and was not re-discovered until October of 2016. However, as compensation, [redacted]

**Mitigation**

To remediate and mitigate this violation, the entity:

1) removed the [redacted] from the ESP;
2) enhanced both of its work management ticketing systems to identify and track work at BES sites or with BES Cyber Systems;
3) updated its procedure to include instructions on what steps should be followed to add a new ESP, including which Cyber Assets should be included within the PSP;
4) updated its procedure to address its assessments for ESPs and PSPs; and
5) created and provided training for its updated processes and procedures to applicable personnel.

**Other Factors**

WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.

The entity did not receive mitigating credit for cooperation. The entity did not quickly address the violations, determine the facts, and report mitigation. This is evident by the duration between the Self-Report date and the Mitigation Plan submittal dates which was 403 days.

The entity did not receive mitigating credit for self-reporting because the Self-Report was submitted 362 days after the entity discovered the noncompliance.

WECC considered the entity's CIP-006-3c R1 compliance history in determining the penalty. WECC determined the entity's CIP-006-3c R1 compliance history to be an aggravating factor in the penalty determination.

[redacted] $80,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017885 | CIP-005-5 | R2; P2.3 | Medium | Moderate | 7/1/2016 (when the Standard and Requirement became enforceable) | 4/4/2017 (when the entity modified the firewall access rules to the legacy device) | Self-Report | 1/18/2019 | TBD |

**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 30, 2017, the entity submitted a Self-Report stating that, as a [redacted], it was in violation with CIP-005-5 R2.

Specifically, the entity reported that while performing an internal controls assessment in February 2017, it discovered that [redacted] Information Technology (IT) cybersecurity personnel were using a legacy intermediate device (ID) for Interactive Remote Access (IRA), which did not require multi-factor authentication, to remotely access Protected Cyber Assets (PCAs) within various ESPs for [redacted] High Impact BES Cyber Systems (HIBCS) and [redacted] Medium Impact BES Cyber Systems (MIBCS). The entity had replaced this legacy ID with a new IRA system which did require multi-factor authentication. IT cybersecurity personnel had been instructed to utilize the new IRA system and stop using the legacy ID. However, because the entity had not removed the firewall rules that allowed remote access to the various ESPs through the use of the legacy ID, IT cybersecurity personnel continued to use the legacy ID Internet Protocol (IP) to connect to the various ESPs.

After reviewing all relevant information, WECC Enforcement determined the entity failed to require multi-factor authentication for all IRA sessions, as required by CIP-005-5 R2 Part 2.3.

The root cause of the violation was less than adequate internal controls and follow up. Specifically, the entity did not have controls in place to ensure that personnel were using the appropriate and authorized IRA system, and that firewall rules were such that they prevented access to the legacy device.

WECC determined that this violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on April 4, 2017, when the entity removed the firewall access rules from the source IP that allowed connection to the various ESPs, for a total of 278 days of noncompliance.

**Risk Assessment**

WECC determined that this violation posed a moderate risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to require multi-factor authentication for all IRA sessions to access [redacted] HIBCS and [redacted] MIBCS, as required by CIP-005-5 R2 Part 2.3.

However, the entity implemented strong internal controls. Specifically, the entity [redacted]. These controls lowered the likelihood of a malicious actor gaining access.

**Mitigation**

To remediated and mitigate this violation, the entity:

1) removed user access to the ESPs from the unauthorized ID;
2) [redacted]
4) developed new rules to improve firewall management and tracking;
5) validated connectivity and created a process to ensure that when changing rules, they are correct;
6) verified successful explicit deny rule(s) for all admin traffic destined to ESP networks are working; and
7) implemented training of the new processes to all firewall administrators.

**Other Factors**

WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.

The entity did not receive mitigating credit for cooperation. The entity did not quickly address the violations, determine the facts, and report mitigation. This is evident by the duration between the Self-Report date and the Mitigation Plan submittal date, which was 441 days.

[redacted] $80,000

| | |
|---|---|
| | The entity did not receive mitigating credit for self-reporting because the Self-Report was submitted 362 days after the entity discovered the noncompliance.<br><br>WECC considered the entity's CIP-005-5 R2 compliance history in determining the penalty. WECC determined the entity's CIP-005-5 R2 compliance history to be an aggravating factor in the penalty determination. |

[redacted] $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2018019006 | CIP-005-5 | R1; P1.3 | Medium | Severe | 7/1/2016 (when the Standard and Requirement became mandatory and enforceable on the entity) | 4/3/2017 (when the reason for granting access was properly documented) | Self-Report | 4/4/2018 | 5/11/2018 |

| | |
|---|---|
| **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 19, 2018, the entity submitted a Self-Report stating that, as a [redacted] it was in violation of CIP-005-5 R1.<br><br>Specifically, on April 3, 2017, while working on Transient Cyber Asset Access Control Lists (ACLs), the entity discovered that the reasons for granting access for five access rules were missing in the ACLs for [redacted] Electronic Access Points (EAPs) to the Electronic Security Perimeters (ESPs) of [redacted] different Medium Impact BES Cyber Systems (MIBCS) at [redacted] switching stations. Upon discovery, the entity added the appropriate reasons for granting access to the ACLs on the [redacted] EAPs and saved the [redacted] EAP configurations, therefore remediating the possible violation on the same day it was discovered.<br><br>After reviewing all relevant information, WECC determined the entity failed to include the reason for granting access for inbound and outbound access permissions, for [redacted] EAPs as required by CIP-005-5 R1, Part 1.3.<br><br>The root cause of the violation was a lack of written communication. Specifically, the task to review all ACLs and ensure the reason for granting access was properly documented; however, it was not part of the entity's CIP Version 5 transition project plan.<br><br>This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable on the entity, and ended on April 3, 2017, when the entity properly documented the reason for granting access within each ACL rule on the [redacted] EAPs in scope, for a total of 276 days of noncompliance. |
| **Risk Assessment** | This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to include the reason for granting access for inbound and outbound access permissions, for two EAPs as required by CIP-005-5 R1, Part 1.3.<br><br>This violation was a documentation issue rather than technical in nature. The entity implemented strong controls. Specifically, its network was implemented with "hub and spoke" technology in that another Cyber Asset was in place between the EAPs in scope and the external network, which had its ACL rules set to block traffic not permitted, with access comments for granting other permitted access. This setup increased the security posture and provided defense in depth. The [redacted] EAPs in scope were also configured to block all traffic. |
| **Mitigation** | To mitigate this violation, the entity has:<br><br>1) added reasons to each of the ACLs on [redacted] the EAPs and saved the two EAP configurations;<br>2) created a Security Information and Event Management (SIEM) policy test that will run daily, verify that all ACLs have a comment, and send results weekly to applicable personnel;<br>3) updated the CIP-005-5 procedure document to include peer review of ACLs and to ensure that comments are added to all ACLs when a new ACL is added, updated, or changed; and<br>4) sent an email to the applicable personnel to notify them of the new peer review process. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity's ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS.<br><br>The entity received mitigating credit for admitting to the violation.<br><br>The entity did not receive mitigating credit for self-reporting due to the length of time between the discovery date and the Self-Report date.<br><br>WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because it involved conduct distinct from this violation.<br><br>WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program. |

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016941 | CIP-005-5 | R1; P1.5 | Medium | High | 7/1/2016 (when the Standard and Requirement became enforceable) | 7/14/2016 (when malicious communication detection was reestablished) | Self-Report | 5/23/2018 | 8/22/2018 |

| | |
|---|---|
| **Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)** | On February 6, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-005-5 R1.<br><br>On July 7, 2016, the entity discovered, via an automated alert from the management console, that there was a configuration issue with [redacted] Cyber Asset pairs ([redacted] devices) configured in high availability fail-over configuration mode. These Cyber Assets were classified as EAPs to the ESP protecting the High Impact BES Cyber Systems (HIBCS). Upon further investigation, the entity determined that during its transition to CIP Version 5, a critical configuration setting was missed in the Intrusion Detection System (IDS) module for each of the [redacted] EAPs pairs. All configuration for the IDS modules had been completed as of July 1, 2016 except for a single configuration setting. Because of the missing IDS module configuration setting, the EAPs did not have a method for detecting known or suspected malicious communications for both inbound and outbound communications from July 1, 2016 to July 14, 2016, when the entity added the configuration settings.<br><br>After reviewing all relevant information, WECC determined that the entity failed to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications, as required by CIP-005-5 R1 Part 1.5.<br><br>The root cause of the violation was less than adequate controls for verifying configuration settings on the three EAP pairs during the NERC CIP Version 3 to Version 5 transition.<br><br>This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on July 14, 2016, when malicious communication detection was reestablished, for a total of 14 days of noncompliance. |
| **Risk Assessment** | This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications, as required by CIP-005-5 R1 Part 1.5.<br><br>However, the entity implemented strong controls. Specifically, the entity utilized a SIEM to detect changes in the configuration of devices and included commands to ensure raw data was analyzed and alerted on actionable information. [redacted]. The entity discovered this noncompliance as a result of investigating the alerts. Furthermore, multiple monitoring systems and methods were employed to log, detect, and alert on the overall health of the affected Cyber Assets, resulting in several layers of defenses protecting the Cyber Assets. [redacted] |
| **Mitigation** | To mitigate this violation the entity:<br><br>1) added the missing IDS module configuration to the [redacted] EAP pairs;<br>2) reseated the cable into the sensor port;<br>3) created a SIEM policy test to monitor and detect for changes;<br>4) provided training for the EAP with sensor port services;<br>5) upgraded the software level on the [redacted] affected EAPs active/standby pairs; and<br>6) held a mitigation closure meeting with applicable personnel related to all compliance elements of CIP-005-5 R1. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity's ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS.<br><br>The entity received mitigating credit for admitting to the violation.<br><br>The entity did not receive mitigating credit for self-reporting due to the length of time between the discovery date and the Self-Report date.<br><br>WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because it involved conduct distinct from this violation. |

[redacted] NOC-2635 $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016941 | CIP-005-5 | R1; P1.5 | Medium | High | 7/1/2016 (when the Standard and Requirement became enforceable) | 7/14/2016 (when malicious communication detection was reestablished) | Self-Report | 5/23/2018 | 8/22/2018 |
| | | | WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program. | | | | | | |

[redacted] NOC-2635 $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016928 | CIP-007-6 | R2; P2.1, 2.2, 2.3 | Medium | Severe | 7/1/2016 (when the Standard and Requirement became enforceable) | 12/19/2018 (Mitigation Plan completion) | Self-Report | 12/19/2018 | TBD |

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

On February 3, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-007-6 R2.

Specifically, for the entity's patch management process for tracking, evaluating, and installing cyber security patches pursuant to CIP-007-6 R2 Part 2.1, it utilized a configuration management application to maintain a comprehensive software whitelist. The whitelist was intended to track all software and the associated security patch sources installed on all [redacted] HIBCS and MIBCS BCAs, and the associated Electronic Access Control and Monitoring System (EACMS), Physical Access Control System (PACS), and Protected Cyber Assets (PCAs). The software whitelist was utilized as the starting point to execute CIP-007-6 R2 Part 2.1 through Part 2.4. On November 3, 2016, during the entity's efforts to true-up its software whitelist to the actual installed software on all its HIBCS and MIBCS BCAs and associated EACMS, PACS, and PCAs, it was discovered that several software applications on [redacted] HIBCS BCA, [redacted] EACMS associated with the HIBCS and [redacted] PCAs associated with [redacted] separate MIBCS, were not originally captured in the software whitelist during the CIP Version 5 implementation effort. Additionally, on December 13, 2016, and February 2, 2017, during continued efforts to true-up its software whitelist, the entity discovered another software application installed on [redacted] HIBCS BCAs, [redacted] PCAs and [redacted] EACMS associated with the HIBCS, as well as [redacted] HIBCS BCAs, respectively, where the software and the associated patch sources were missing from the software whitelist. None of this software was being tracked for cyber security patches, therefore the patches were not being evaluated, applied, or had mitigation plans created. This issue affected [redacted] BCAs ([redacted] in HIBCS and [redacted] in MIBCS), [redacted] EACMS, [redacted] PCAs and [redacted] PACS associated with the HIBCS, as well as [redacted] EACMS and [redacted] PCAs associated with the MIBCS, for a total of [redacted] Cyber Assets.

After reviewing all relevant information, WECC determined the entity failed to identify a source or sources to track for the release of cyber security patches for applicable Cyber Assets that were updateable and for which a patching source exists, for [redacted] applicable Cyber Assets, as required by CIP-007-6 R2 Part 2.1. As a result, the entity also failed to evaluate security patches for applicability for the software applications installed on those [redacted] devices, as required by CIP-007-6 R2 Part 2.2; as well as failed to take action for [redacted] patches to either apply the patches, or create a dated mitigation plan, or revise an existing mitigation plan, as required by CIP-007-6 R2 Part 2.3.

The root cause of the violation was management policy guidance or expectations not being well-defined, understood, or enforced. Specifically, the entity had no project plans in place to address this requirement, the scope of the tasks was unknown, and available resources were constrained. Additionally, there was a misalignment of the operations team's skill sets and resource assignment.

This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity and ended when the entity completed its mitigation plan on December 19, 2018, for a total of 902 days of noncompliance.

**Risk Assessment**

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to identify a source or sources to track for the release of cyber security patches for applicable Cyber Assets that were updateable and for which a patching source exists, as required by CIP-007-6 R2 Part 2.1. As a result, the entity also failed to evaluate security patches for applicability for the software applications installed on those Cyber Assets, as required by CIP-007-6 R2 Part 2.2; as well as failed to take action for applicable patches to either apply the patches, or create a dated mitigation plan, or revise an existing mitigation plan, as required by CIP-007-6 R2 Part 2.3.

However, the entity had implemented strong controls. None of the affected Cyber Assets were internet-facing. Furthermore, multiple monitoring systems and methods were employed to log, detect, and alert on the overall health of the affected Cyber Assets, resulting in several layers of defenses protecting the Cyber Assets. [redacted]

**Mitigation**

To mitigate this violation, the entity:

1) inventoried all installed software applications utilizing its SIEM reporting tool, and added any missing installed software applications to asset management tool software;
2) used a whitelist to ensure that all installed software applications are added to and being tracked in the vulnerability management service where possible;
3) inventoried all installed firmware and added to the vulnerability management service for tracking and evaluation of firmware in its environment;
4) uninstalled software applications that are no longer needed and removed them from the software whitelist;

[redacted] $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016928 | CIP-007-6 | R2; P2.1, 2.2, 2.3 | Medium | Severe | 7/1/2016 (when the Standard and Requirement became enforceable) | 12/19/2018 (Mitigation Plan completion) | Self-Report | 12/19/2018 | TBD |

| | |
|---|---|
| | 5) updated the SIEM [redacted] functions to ensure use of the best reporting tools available from the SIEM;<br>6) inspected the software whitelist entries for inclusion and exclusion errors that could cause software to be excluded from the evaluation work flow;<br>7) added functionality to its asset management tool to make it apparent to a user that an entry is either including or excluding software from the whitelist;<br>8) developed and documented a process for the evaluation of software and firmware entries in the software whitelist that are not able to be tracked by vulnerability management service; and<br>9) held training for subject matter experts (SMEs) responsible for evaluating software and firmware patches. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS.<br><br>The entity received mitigating credit for admitting to the violation.<br><br>WECC considered the entity's CIP-007-6 R2 compliance history in determining the penalty. WECC determined the entity's CIP-007-6 R2 compliance history to be an aggravating factor in the penalty determination.<br><br>WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program. |

[redacted] $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016939 | CIP-007-6 | R3; P3.1 | Medium | Severe | 7/1/2016 (when the Standard and Requirement became enforceable) | 5/19/2017 (when the physical ports were locked and added antivirus to the PCA) | Self-Report | 4/10/2018 | 10/11/2018 |

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

On February 6, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-007-6 R3.

Specifically, the entity utilized physical port locking as one of the methods to deter, detect, or prevent malicious code on it CIP applicable Cyber Assets. However, on January 19, 2017, the entity identified that [redacted] ports on [redacted] MIBCS BCAs without External Routable Connectivity (ERC) had not been port locked as of July 1, 2016. The employee responsible for this task mistakenly applied the CIP-007-6 R1, Part 1.1 methodology of leaving the physical ports instead of the logical ports open. Upon identification of the missing port locks, the entity began the process of physically port locking [redacted] ports on [redacted] of the BCAs, which was completed on February 10, 2017. The entity did not physically port lock one port each on the [redacted] remaining BCAs because it was in the process of decommissioning those devices, which it completed on December 13, 2016. Additionally, [redacted] PCA did not have antivirus installed as required by CIP-007-6 R3 Part R3.1.

After reviewing all relevant information, WECC determined the entity failed to deploy methods to deter, detect, or prevent malicious code on [redacted] MIBCS BCAs without ERC and [redacted] PCA, as required by CIP-007-6 R3 Part 3.1.

The root cause of the violation was not understanding the documented processes. Specifically, an employee mistakenly applied the CIP-007-6 R1, Part 1.1 methodology of leaving the physical ports instead of logical ports open on the BCAs in scope.

This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on May 19, 2017, when the entity physically port locked the remaining BCAs in scope and added antivirus to the PCA, for a total of 322 days of noncompliance.

**Risk Assessment**

This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. The entity failed to deploy methods to deter, detect, or prevent malicious code on [redacted] MIBCS BCAs without ERC, as required by CIP-007-6 R3 Part 3.1.

However, the entity implemented an extensive SIEM architecture that continually monitors changes on HIBCS and MIBCS Cyber Assets and alerts the operations group of unauthorized changes. The SIEM also monitors network switch configurations to ensure enabled ports have a description entered. [redacted] This protection is provided for all devices on the network segment, including those without the anti-malware software installed. [redacted]

**Mitigation**

To mitigate this violation, the entity:

1) placed tamper tape on open ports on [redacted] of the BCAs in scope;
2) implemented a mandatory escort checklist to ensure the responsibilities of authorized escorts are met and to identify any potential incidents, including physical disturbances such as broken tamper tape or missing port locks. The checklist will also outline the proper response steps to be taken in the event an incident/disturbance is discovered;
3) documented a process to capture cyber security controls for all new cyber assets and/or new device types at transmission facilities to prevent introducing any device types that could create a CIP or Reliability risk;
4) decommissioned the remaining [redacted] BCAs in scope;
5) installed antivirus on applicable devices;
6) removed legacy non-ERC device types associated with its MIBCS which were classified as BCA and replaced them with devices capable of ERC;
7) communicated to applicable personnel new process changes;
8) reviewed and/or edited procedure to ensure full understanding of the documented controls to prevent malicious code on non-ERC devices; and
9) ensured that reports from the antivirus software were created, scheduled, and being sent to appropriate personnel for their review and verification that antivirus was installed on all applicable devices.

**Other Factors**

WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS.

[redacted] NOC-2635 $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016939 | CIP-007-6 | R3; P3.1 | Medium | Severe | 7/1/2016 (when the Standard and Requirement became enforceable) | 5/19/2017 (when the physical ports were locked and added antivirus to the PCA) | Self-Report | 4/10/2018 | 10/11/2018 |
| | | | The entity received mitigating credit for admitting to the violation.<br>WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because it was distinct, separate, and not relevant to this violation.<br><br>WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program. | | | | | | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016938 | CIP-007-6 | R4; P4.2.2 | Medium | High | 11/8/2016 (when the SIEM stopped functioning correctly) | 12/26/2016 (when the SIEM began logging and alerting for events) | Self-Report | 5/17/2018 | 10/11/2018 |

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

On February 6, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-007-6 R4.

Specifically, on December 7, 2016 during a log review, the entity identified a potential logging issue with its SIEM, the event logging and alerting tool utilized to perform CIP-007-6 R4 for its HIBCS and MIBCS and the associated EACMS, PCAs, and PACS, as applicable, for technically capable devices. As a result, the entity worked with the SIEM vendor to determine that the SIEM database had been corrupted since November 8, 2016. Subsequently, the entity rebuilt the indexes in the database and brought the SIEM back to a normal operating state by December 26, 2016. During the 48-day span while the SIEM database was not operating correctly, [redacted] Cyber Assets were not reporting to the SIEM: [redacted] BCAs, [redacted] EACMS devices, [redacted] PCAs, and [redacted] PACS Cyber Asset, all associated with the HIBCS, and [redacted] PCAs associated with the MIBCS. The identified Cyber Assets were still logging locally, therefore once the SIEM database was repaired, all data was able to be restored and captured for the 48-day timeframe. Furthermore, the antivirus continued to function as expected during this timeframe and could send its logs to the antivirus policy administrator console, which was capable of alerting on malicious code. However, during the 48-day span, the [redacted] Cyber Assets were not able to send logs to the SIEM in order for the SIEM to generate alerts for a detected failure of Part 4.1 event logging. Because all logs were cached on the local devices, when the SIEM became operational again, all logs were forwarded on, normalized, and correlated. Any logs that would have caused an alert from the SIEM would have been sent when the SIEM was repaired.

Additionally, the entity reported that as a result of the issue with the SIEM, the [redacted] Cyber Assets associated with its HIBCS were not included in the 15-calendar day log review during the 48 days in which the SIEM database was not operating correctly.

After reviewing all relevant information, WECC determined the entity failed to generate alerts for detected failure of Part 4.1 event logging, as required by CIP-007-6 R4 Part 4.2 Sub-Part 4.2.2. WECC also determined that the entity did not violate CIP-007-6 R4 Part 4.4 because logs were being reviewed at a summary level as required.

The root cause of the violation was an equipment malfunction. Specifically, the entity's SIEM, which is its event logging and alerting tool, experienced a corruption of its database.

This violation began on November 8, 2016, when the SIEM stopped functioning correctly, and ended on December 26, 2016, when the SIEM began logging and alerting for events, for a total of 48 days of noncompliance.

**Risk Assessment**

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to generate alerts for detected failure of Part 4.1 event logging, as required by CIP-007-6 R4 Part 4.2 Sub-Part 4.2.2.

However, the entity implemented strong controls. The risk of malicious code was mitigated by the entity's implementation of antivirus since it has the ability to log and alert. The risk of loss of logs on the Cyber Assets was mitigated, as the information was cached and sent to the SIEM upon re-indexing of the database. All Cyber Assets in question were protected within Physical Security Perimeters (PSPs) which was verified at audit. The antivirus continued to function as expected during this timeframe and could send its logs to the antivirus policy administrator console, which was capable of alerting on malicious code. Additionally, the entity implemented task reminders to remind employees to review logs which included escalations up to senior management if the task is not completed prior to the due date. While performing the manual review of those logs, this noncompliance was identified.

**Mitigation**

To mitigate this violation the entity:

1) corrected the SIEM database corruption;
2) verified that the SIEM database was operational and ensured that all logs were normalized and reporting--no database corruption errors were displayed in the console manager log;
3) updated the CIP-007-6 R4 procedure regarding log review;
4) created a SIEM Normal Operations Dashboard that will exhibit the health and normal operations of the SIEM by utilizing dynamic insights of critical components of the SIEM;
5) conducted a summary review of logs from July 1, 2016 to the date the database indexes were rebuilt to ensure no potential Cyber Security Incidents went undetected. The logs were restored, and a representative sample was used for the review;
6) updated the CIP-007-6 R4 procedure to include all the new processes; and
7) provided training to applicable personnel on the updated CIP-007-6 R4 procedures.

[redacted] NOC-2635 $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016938 | CIP-007-6 | R4; P4.2.2 | Medium | High | 11/8/2016 (when the SIEM stopped functioning correctly) | 12/26/2016 (when the SIEM began logging and alerting for events) | Self-Report | 5/17/2018 | 10/11/2018 |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS.<br><br>The entity received mitigating credit for admitting to the violation.<br>WECC considered the entity's CIP-007-6 R4 compliance history in determining the penalty. WECC determined the entity's CIP-007-6 R4 compliance history to be an aggravating factor in the penalty determination.<br><br>WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program. | | | | | | | | |

[redacted] $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016940 | CIP-007-6 | R5; P5.5.1, P5.5.2 | Medium | Severe | 7/1/2016 (when the Standard and Requirement became enforceable) | 1/25/2017 (when password parameters were set for the accounts) | Self-Report | 10/19/2018 | TBD |

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

On February 6, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-007-6 R5.

Specifically, on December 9, 2016, while the entity's engineers were executing its change management process to install new MIBCS BCAs at a switching station, the entity's Operations SMEs provided temporary passwords for the BCAs to be functionally tested prior to their deployment into the ESP where the BCA password length and complexity would be automatically enforced via a substation remote access system. Upon the Operations SMEs providing the temporary passwords, the [redacted] SMEs identified that both the temporary passwords and the enforcement of password length and complexity in the substation remote access system for these particular BCAs did not meet the minimum password parameters as required by Part 5 Sub-Part 5.5.1 (length) and Part 5 Sub-Part 5.5.2 (complexity), even though the substation remote access system and the BCAs could support such parameters. Upon discovery, it was determined that the Operations SMEs would enforce password length and complexity procedurally until the scope of the potential issue could be determined and corrected in the substation remote access system.

Upon further investigation, the entity determined that [redacted] BCAs and [redacted] EACMS Cyber Assets associated with the MIBCSs at [redacted] switching stations did not have the appropriate CIP-007-6 R5.5 password parameters in place. The [redacted] Cyber Assets were identified as not meeting either one or two of the Sub-Parts of CIP-007-6 R5 Part 5.5, which equated to [redacted] accounts with passwords that needed to be changed, out of a total population of [redacted] accounts with passwords managed by the substation remote access system. As of January 25, 2017, all [redacted] passwords for the [redacted] Cyber Assets had been updated to meet length and complexity requirements, and all password settings within the substation remote access system had been corrected to meet CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2.

After reviewing all relevant information, WECC determined the entity failed to implement a process for password-only authentication for interactive user access, either technically or procedurally, and to enforce password parameters as required by CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2.

The root cause of the violation was a lack of internal controls during the entity's transition from Version 3 to Version 5. Specifically, there was insufficient run time in the entity's project plan to validate the configuration prior to the effective date of Version 5. During this time, the entity was implementing a new change management system and did not allow configuration changes, other than for emergencies, to CIP Cyber Assets. Had the entity's change management been in place at the time, it would have likely caught the misconfiguration.

This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on January 25, 2017, when password parameters were set for the accounts to the devices in scope, for a total of 209 days of noncompliance.

**Risk Assessment**

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to implement a process for password-only authentication for interactive user access, either technically or procedurally, and to enforce password parameters, as required by CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2.

However, the entity implemented strong controls. [redacted]

Therefore, while password length and complexity did not meet the CIP-007-6 R 5 Part 5.5 length and complexity requirements between July 1, 2016 and January 25, 2017, password enforcement was still set to a minimum length of five characters or more (depending on the device type) and a minimum complexity of two different character types during the violation duration.

**Mitigation**

To mitigate this violation, the entity:

1) updated the passwords associated with the identified Cyber Assets to meet length and complexity requirements;
2) update the SIEM policy test to ensure it shows that the passwords for devices in scope meet the parameters of CIP-007 R5 Part 5.5;
3) created a tool to assist in identifying CIP requirements, if any, that apply to new devices prior to approval of any final design that is planned to go through the entity's commissioning process;
4) documented a process to capture Cyber Security controls for all new Cyber Assets prior to any commissioning of a Cyber Asset;
5) ensured business unit procedures align to support password length and complexity for any new devices coming online; and

[redacted] $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016940 | CIP-007-6 | R5; P5.5.1, P5.5.2 | Medium | Severe | 7/1/2016 (when the Standard and Requirement became enforceable) | 1/25/2017 (when password parameters were set for the accounts) | Self-Report | 10/19/2018 | TBD |
| | | | 6) held a mitigation closure meeting with all mitigation SME team members, as well a representative from [redacted] management, applicable Operations SMEs, and its [redacted] Completed remediation and mitigation tasks and procedures will be discussed, reviewed, and verified. | | | | | | |
| **Other Factors** | | | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS.<br><br>The entity received mitigating credit for admitting to the violation.<br><br>WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because it was distinct, separate, and not relevant to this violation.<br><br>WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program. | | | | | | |

[redacted] $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016926 | CIP-010-2 | R1; P1.1.1, P1.1.2, P1.1.4, P1.1.5 | Medium | High | 7/1/2016 (when the Standard and Requirement became enforceable) | 5/1/2017 (when baseline configurations were developed and captured) | Self-Report | 3/29/2019 | TBD |

**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 [redacted] the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-010-2 R1.

Specifically, on August 4, 2016, during its first performance of a bookend review of CIP-010-2 R2 Part 2.1 baseline configurations, the entity's [redacted] SMEs became concerned that some baseline elements might be missing from some Cyber Asset baseline configuration details. At the time, the entity believed that it may not have complete baseline configurations captured for only a few Cyber Assets since port scanning could not be accomplished due to connectivity problems between its configuration monitoring tool and the Cyber Assets. However, to examine the scope of the issue, and to perform the necessary due diligence, [redacted] began an effort on August 25, 2016 to review each Cyber Asset in its Cyber Asset inventory to ensure that all required and applicable CIP-010-2 R1 Part 1.1 Sub-Parts 1.1.1 through 1.1.5 baseline elements were captured for each applicable Cyber Asset. The entity concluded that the scope of this violation included [redacted] Cyber Assets ([redacted] BCAs, [redacted] EACMS, and [redacted] PCAs) at the HIBCS and MIBCS. During the entity's [redacted] audit, WECC auditors confirmed an additional [redacted] Cyber Assets ([redacted] BCAs, [redacted] EACMS, and [redacted] PCAs) as being in scope of this violation, for a total of [redacted] Cyber Assets, along with the baseline element that was missing from the Cyber Assets baseline configuration. [redacted] of the [redacted] Cyber Assets were in violation of sub-part 1.1.1; [redacted] were in violation of sub-part 1.1.2; [redacted] were in violation of sub-part 1.1.4; and [redacted] was in violation of sub-part 1.1.5.

After reviewing all relevant information, WECC determined the entity failed to develop a baseline configuration individually or by a group, as required by CIP-010-2 R1 Part 1.1 Sub-Parts 1.1.1, 1.1.2, 1.1.4, and 1.1.5.

The root cause of the violation was less than adequate procedures. Specifically, the entity had a procedure in place to meet objectives of the Requirements; however, the procedure did not contain complete and accurate information to meet those objectives. Additionally, the entity had no procedure in place to address configuration and communication issues with the SIEM.

This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on May 1, 2017, when baseline configurations were developed and captured for the Cyber Assets in scope, for a total of 305 days of noncompliance.

**Risk Assessment**

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to develop a baseline configuration individually or by a group, as required by CIP-010-2 R1 Part 1.1 Sub-Parts 1.1.1, 1.1.2, 1.1.4 and 1.1.5.

However, the entity implemented strong detective controls. [redacted] The entity did not implement controls to prevent this violation from occurring but did employ detective controls which identified the violation. Furthermore, multiple monitoring systems and methods were employed to log, detect, and alert on the overall health of the affected Cyber Assets, resulting in several layers of defenses protecting the Cyber Assets.

**Mitigation**

To mitigate this violation, the entity has:

1) collected the number and names of devices missing baseline elements and completed baseline configurations on the Cyber Assets in scope;
2) documented a process to capture cyber security controls for all new Cyber Assets and/or new device types at Transmission facilities to prevent introducing any device type that could create a CIP or Reliability risk;
3) upgraded applicable configuration monitoring tool device profilers to compatible firmware versions to ensure automated port scan capability;
4) provided training to SMEs on SIEM admin, security, and compliance;
5) for any baselines that are being tracked manually (e.g. in spreadsheets), converted to Offline Device Type in its asset management system in order for the baseline element to be documented within the configuration monitoring tool. An alternative is to track the baseline element through configuration monitoring tool scanning if possible. The desired end result is that all baseline documentation resides within the configuration monitoring tool;
6) promoted all 'unpromoted changes', which will set the as-is device state to be the current baseline;
7) updated baseline reports to include only the required information to help SMEs more easily see if/when information is missing;

[redacted] $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016926 | CIP-010-2 | R1; P1.1.1, P1.1.2, P1.1.4, P1.1.5 | Medium | High | 7/1/2016 (when the Standard and Requirement became enforceable) | 5/1/2017 (when baseline configurations were developed and captured) | Self-Report | 3/29/2019 | TBD |

| | |
|---|---|
| | 8) updated the CIP-010-2 R1 procedure to reflect the changes to processes, documentation, and reporting that have been made, to include updating procedures for how to commission offline devices that includes a process for adding manual baseline configurations into its asset management system; and<br>9) trained applicable personnel on commissioning new CIP devices to ensure clarity on the procedure of collecting and documenting baseline data. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS.<br><br>The entity received mitigating credit for admitting to the violation.<br><br>The entity did not receive mitigating credit for self-reporting due to the length of time between the discovery date and the Self-Report date.<br><br>WECC considered the entity's CIP-010-2 R1 compliance history in determining the penalty. WECC determined the entity's CIP-010-2 R1 compliance history to be an aggravating factor in the penalty determination.<br><br>WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program. |

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016929 | CIP-010-2 | R2; P2.1 | Medium | Severe | 8/6/2016 (when baseline changes were not monitored) | 11/11/2017 (when baseline changes commenced) | Self-Report | 6/5/2018 | 10/11/2018 |

| | |
|---|---|
| **Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)** | On February 3, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-010-2 R2.<br><br>Specifically, on November 1, 2016, the entity's [redacted] SMEs discovered a misconfiguration within its configuration monitoring tool used to monitor the entity's Cyber Asset baseline configurations, which caused an EACMS associated with the HIBCS not to have its baseline configuration monitored from August 6, 2016 to November 1, 2016, as required by CIP-010-2 R2 Part 2.1. During the entity's investigation, to ensure other Cyber Assets did not have similar issues, it discovered [redacted] additional Cyber Assets where baseline configurations were not being monitored at least once every 35 calendar days for changes, from August 6, 2016 to January 26, 2017. The [redacted] Cyber Assets included [redacted] BCAs, in addition to [redacted] EACMS and [redacted] PCAs associated with the HIBCS.<br><br>After reviewing all relevant information, WECC determined the entity failed to monitor at least once every 35 calendar days for changes to the baseline configuration, as well as document and investigate detected unauthorized changes, as required by CIP-010-2 R2 Part 2.1.<br><br>The root cause of the violation was less than adequate procedures. Specifically, the entity had a procedure in place to meet objectives of the Requirements; however, the procedure did not contain complete and accurate information to meet those objectives. Additionally, the entity had no procedure in place to address the configuration and communication issues with the SEIM.<br><br>This violation began on August 6, 2016, when changes to baseline configurations were not being monitored, and ended on May 11, 2017, when monitoring of changes to baseline configurations commenced on the Cyber Assets in scope, for a total of 279 days of noncompliance. |
| **Risk Assessment** | This violation posed a moderate risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to monitor at least once every 35 calendar days for changes to the baseline configuration, as well as document and investigate detected unauthorized changes, as required by CIP-010-2 R2 Part 2.1.<br><br>However, the entity implemented strong controls. Specifically, the entity implemented an asset management system, which is used for off-line device management to facilitate a method to collect configuration information for Cyber Assets when it is difficult to implement technical or other controls. The information is gathered manually from the Cyber Assets in question and entered into the asset management system. Additionally, the risk specific to [redacted] of the BCAs in scope of this noncompliance was further reduced because changes to their baseline configurations could only be made through a physical hardware change, and not remotely. |
| **Mitigation** | To mitigate this violation, the entity:<br><br>1) worked with its SIEM vendor to develop and implement a solution that tracks the number of days since an asset was last monitored by the SIEM to verify successful baseline monitoring of Cyber Assets for a 35-day rolling window;<br>2) implemented new configuration monitoring tool rules, policy tests, and reports;<br>3) monitored the 20 Cyber Assets for baseline configuration changes;<br>4) created a daily automated test to run for Cyber Assets which do not directly connect to the SIEM to ensure that manual baseline checks are performed at least once every 35 calendar days. For those Cyber Assets that exceed a 35-day baseline monitoring check, a policy test will fail and the failure will be reflected on a daily email report sent to [redacted]<br>5) upgraded applicable configuration monitoring tool device profilers to compatible firmware versions to ensure automated port scan capability;<br>6) established an interface with the asset management functionality and collected the date the offline device type was last checked and used the new rules to calculate how long since the last check;<br>7) added the offline device type assets to the new configuration monitoring tool reports to report on failing assets;<br>8) updated the CIP-010-2 R2 procedure to reflect the changes to processes, documentation, and reporting that have been made as a result of the new reporting evidence; and<br>9) provided training to applicable personnel on the updated procedure. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS.<br><br>The entity received mitigating credit for admitting to the violation.<br>The entity did not receive mitigating credit for self-reporting due to the length of time between the discovery date and the Self-Report date.<br><br>WECC considered the entity's CIP-010-2 R2 compliance history in determining the penalty. WECC determined the entity's CIP-010-2 R2 compliance history to be an aggravating factor in the penalty determination. |

[redacted] NOC-2635 $74,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016929 | CIP-010-2 | R2; P2.1 | Medium | Severe | 8/6/2016 (when baseline changes were not monitored) | 11/11/2017 (when baseline changes commenced) | Self-Report | 6/5/2018 | 10/11/2018 |
| | | | WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program. | | | | | | |

**COVER PAGE**

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notice of Penalty in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

| Count | Violation ID | Category 1 | Category 2 | Category 3 | Category 4 | Category 5 | Category 6 | Category 7 | Category 8 | Category 9 | Category 10 | Category 11 | Category 12 | CEII PROTECTION (YEARS) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | NPCC2018020059 | Yes | | Yes | Yes | | | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 2 | NPCC2018020060 | Yes | | Yes | Yes | | | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 3 | NPCC2018020061 | Yes | | Yes | Yes | | | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 4 | NPCC2018020063 | Yes | | Yes | Yes | | | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 5 | NPCC2018020064 | Yes | | Yes | Yes | | | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 6 | NPCC2018020062 | Yes | | Yes | Yes | | | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 7 | WECC2017018752 | Yes | | Yes | Yes | | | | Yes | | | | | Category 1: 3 years; Category 2 – 12: 2 year |
| 8 | WECC2018019340 | Yes | | Yes | Yes | | | | | | | | | Category 1: 3 years; Category 2 – 12: 2 year |
| 9 | WECC2017018489 | Yes | | Yes | Yes | | | | Yes | | | | Yes | Category 1: 3 years; Category 2 – 12: 2 year |
| 10 | WECC2017018732 | Yes | | Yes | Yes | | | | Yes | | | | | |
| 11 | WECC2017017229 | Yes | | Yes | Yes | Yes | Yes | | Yes | | | | | |
| 12 | WECC2018020044 | Yes | | Yes | Yes | | | | Yes | | | | | |
| 13 | WECC2018020045 | Yes | | Yes | Yes | Yes | Yes | | Yes | | | | | |
| 14 | | | | | | | | | | | | | | |
| 15 | | | | | | | | | | | | | | |
| 16 | | | | | | | | | | | | | | |
| 17 | | | | | | | | | | | | | | |
| 18 | | | | | | | | | | | | | | |
| 19 | | | | | | | | | | | | | | |
| 20 | | | | | | | | | | | | | | |
| 21 | | | | | | | | | | | | | | |
| 22 | | | | | | | | | | | | | | |
| 23 | | | | | | | | | | | | | | |
| 24 | | | | | | | | | | | | | | |
| 25 | | | | | | | | | | | | | | |
| 26 | | | | | | | | | | | | | | |
| 27 | | | | | | | | | | | | | | |
| 28 | | | | | | | | | | | | | | |
| 29 | | | | | | | | | | | | | | |
| 30 | | | | | | | | | | | | | | |
| 31 | | | | | | | | | | | | | | |
| 32 | | | | | | | | | | | | | | |

[redacted] NOC-2627 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020059 | CIP-002-5.1a | R1. (1.1., 1.2., 1.3.). | High | Lower | July 1, 2016 | July 13, 2018 | Audit | 12/14/2018 | 12/18/2018 |

**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.)**

During a Compliance Audit conducted from [redacted], NPCC determined that [redacted] (the entity) as a [redacted] was in violation of CIP-002-5.1a R1. (1.1., 1.2., 1.3.). [redacted]

This noncompliance started on July 1, 2016 when the entity failed to implement a process to assess applicable assets for BES Cyber Systems. The violation ended on July 13, 2018 when the entity implemented a process to identify its Impact Rating of its Assets.

Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect. In July of 2018, the entity conducted an internal audit and discovered procedures were not updated, but did not see it as a major violation. The entity states it was fully aware the asset was low impact, and that is why they failed to update the documentation.

The root cause of this violation was lack of accountability and management oversight.

**Risk Assessment**

The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify BES Cyber Systems that are applicable to the CIP Standards, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.

The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections.

[redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted]

[redacted]

Additionally, the facility has a 24 hour start-up time and only runs when needed.

No harm is known to have occurred as a result of this noncompliance.

**Mitigation**

To mitigate this violation, the entity:

1) Updated its CIP-002 procedure to Version 5
2) Implemented the entity's updated CIP-002-5.1 procedure. This resulted in an identification of one asset containing low impact BES Cyber Systems.

To prevent recurrence, the entity:

3) Implemented software to create and track tasks. The system will send multiple automatic email reminders to the responsible person until the task is completed. The system will also send escalation emails to overseeing persons if the task has not been completed within a specified amount of time. Tasks will repeat upon closure or with a specified frequency depending on how they are set up.

[redacted] NOC-2627 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020059 | CIP-002-5.1a | R1. (1.1., 1.2., 1.3.). | High | Lower | July 1, 2016 | July 13, 2018 | Audit | 12/14/2018 | 12/18/2018 |

| | |
|---|---|
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.<br><br>Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate based on the underlying conduct, which included the deliberate failure to update its documentation to identify the BES Cyber Systems as required by the Standard. |

[redacted] NOC-2627 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020060 | CIP-002-5.1a | R2. (2.1., 2.2.). | Lower | VSL - Severe | July 1, 2016 | July 13, 2018 | Audit | 12/14/2018 | 12/18/2018 |

**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.)**

During a Compliance Audit conducted from [redacted], NPCC determined stating that [redacted] (the entity) as a [redacted] was in violation of CIP-002-5.1a R2. (2.1., 2.2.). [redacted]

This violation started on July 1, 2016 when the entity failed to review the identifications in requirement R1 and have its CIP Senior Manager or delegate approve the identifications. The violation ended on July 13, 2018 when the entity implemented a process to identify its Impact Rating of its Assets and had its CIP Senior Manager approve the identifications.

Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect. In July of 2018, the entity conducted an internal audit and discovered procedures were not updated, but did not see it as a major violation. The entity states it was fully aware the asset was low, and that is why they failed to update documentation.

The root cause of this violation was lack of accountability and management oversight.

**Risk Assessment**

The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify, review and have its CIP Senior Manager approve BES Cyber Systems that are applicable to the CIP Standards, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.

The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections.

[redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted]

[redacted]

Additionally, the facility has a 24 hour start-up time and only runs when needed.

No harm is known to have occurred as a result of this noncompliance.

**Mitigation**

To mitigate this violation, the entity:

1) Updated its CIP-002 procedure to Version 5
2) Implemented the entity's updated CIP-002-5.1 procedure. This resulted in an identification of one asset containing low impact BES Cyber Systems.

To prevent recurrence, the entity:

3) Implemented software to create and track tasks. The system will send multiple automatic email reminders to the responsible person until the task is completed. The system will also send escalation emails to overseeing persons if the task has not been completed within a specified amount of time. Tasks will repeat upon closure or with a specified frequency depending on how they are set up.

[redacted] NOC-2627 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020060 | CIP-002-5.1a | R2. (2.1., 2.2.). | Lower | VSL - Severe | July 1, 2016 | July 13, 2018 | Audit | 12/14/2018 | 12/18/2018 |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.<br><br>Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate based on the underlying conduct, which included the deliberate failure to have a CIP Senior Manager approve the impact ratings as required by the Standard. | | | | | | | | |

[redacted] NOC-2627 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020061 | CIP-003-6 | R3. | Medium | VSL - Severe | July 1, 2016 | December 1, 2016 | Audit | 12/14/2018 | 12/18/2018 |

| | |
|---|---|
| **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.)** | During a Compliance Audit conducted from [redacted], NPCC determined that [redacted] as a [redacted] was in violation of CIP-003-6 R3. [redacted]<br><br>This violation started on July 1, 2016 when the entity failed to identify a CIP Senior Manager by name. The violation ended on December 1, 2016 when the entity designated a CIP Senior Manager.<br><br>Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect.<br><br>The root cause of this violation was lack of accountability and management oversight. |
| **Risk Assessment** | The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing designate a CIP Senior Manager, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.<br><br>The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections.<br><br>[redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted]<br><br>[redacted]<br><br>Additionally, the facility has a 24 hour start-up time and only runs when needed.<br><br>No harm is known to have occurred as a result of this noncompliance. |
| **Mitigation** | To mitigate this violation, the entity:<br>1) Designated a CIP Senior Manager<br><br>To prevent recurrence, the entity:<br>2) Created automated tasks to maintain documentation for CIP Senior Manager designations. |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC -2627 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020063 | CIP-002-5.1a | R1. (1.1., 1.2., 1.3.). | High | VSL -Lower | July 1, 2016 | July 13, 2018 | Audit | 12/14/2018 | 12/18/2018 |

**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.)**

During a Compliance Audit conducted from [redacted], NPCC determined that [redacted] the entity) as a [redacted] was in violation of CIP-002-5.1a R1. (1.1., 1.2., 1.3.). [redacted]

This noncompliance started on July 1, 2016 when the entity failed to implement a process to assess applicable assets for BES Cyber Systems. The violation ended on July 13, 2018 when the entity implemented a process to identify its Impact Rating of its Assets.

Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect. In July of 2018, the entity conducted an internal audit and discovered procedures were not updated, but did not see it as a major violation. The entity states it was fully aware the asset was low impact, and that is why they failed to update the documentation.

The root cause of this violation was lack of accountability and management oversight.

**Risk Assessment**

The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify BES Cyber Systems that are applicable to the CIP Standards, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.

The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections.

[redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted]

[redacted]

Additionally, the facility has a 24 hour start-up time and only runs when needed.

No harm is known to have occurred as a result of this noncompliance.

**Mitigation**

To mitigate this violation, the entity:

1) Updated its CIP-002 procedure to Version 5
2) Implemented the entity's updated CIP-002-5.1 procedure. This resulted in an identification of one asset containing low impact BES Cyber Systems.

To prevent recurrence, the entity:

3) Implemented software to create and track tasks. The system will send multiple automatic email reminders to the responsible person until the task is completed. The system will also send escalation emails to overseeing persons if the task has not been completed within a specified amount of time. Tasks will repeat upon closure or with a specified frequency depending on how they are set up.

[redacted] NOC -2627 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020063 | CIP-002-5.1a | R1. (1.1., 1.2., 1.3.). | High | VSL -Lower | July 1, 2016 | July 13, 2018 | Audit | 12/14/2018 | 12/18/2018 |
| **Other Factors** | | | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.<br><br>Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate based on the underlying conduct, which included the deliberate failure to update its documentation to identify the BES Cyber Systems as required by the Standard. | | | | | | |

[redacted] NOC -2627 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020064 | CIP-002-5.1a | R2. (2.1., 2.2.). | Lower | VSL - Severe | July 1, 2016 | July 13, 2018 | Audit | 12/14/2018 | 12/18/2018 |

**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.)**

During a Compliance Audit conducted from [redacted], NPCC determined that [redacted] (the entity) as a [redacted], was in violation of CIP-002-5.1a R2. (2.1., 2.2.). [redacted]

This violation started on July 1, 2016 when the entity failed to review the identifications in requirement R1 and have its CIP Senior Manager or delegate approve the identifications. The violation ended on July 13, 2018 when the entity implemented a process to identify its Impact Rating of its Assets and had its CIP Senior Manager approve the identifications.

Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect. In July of 2018, the entity conducted an internal audit and discovered procedures were not updated, but did not see it as a major violation. The entity states it was fully aware the asset was low, and that is why they failed to update documentation.

The root cause of this violation was lack of accountability and management oversight.

**Risk Assessment**

The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify, review and have its CIP Senior Manager approve BES Cyber Systems that are applicable to the CIP Standards, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.

The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections.

[redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted]

[redacted]

Additionally, the facility has a 24 hour start-up time and only runs when needed.

No harm is known to have occurred as a result of this noncompliance.

**Mitigation**

To mitigate this violation, the entity:

1) Updated its CIP-002 procedure to Version 5
2) Implemented the entity's updated CIP-002-5.1 procedure. This resulted in an identification of one asset containing low impact BES Cyber Systems.

To prevent recurrence, the entity:

3) Implemented software to create and track tasks. The system will send multiple automatic email reminders to the responsible person until the task is completed. The system will also send escalation emails to overseeing persons if the task has not been completed within a specified amount of time. Tasks will repeat upon closure or with a specified frequency depending on how they are set up.

[redacted] NOC -2627 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020064 | CIP-002-5.1a | R2. (2.1., 2.2.). | Lower | VSL - Severe | July 1, 2016 | July 13, 2018 | Audit | 12/14/2018 | 12/18/2018 |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.<br><br>Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate based on the underlying conduct, which included the deliberate failure to have a CIP Senior Manager approve the impact ratings as required by the Standard. | | | | | | | | |

[redacted] NOC -2627 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| NPCC2018020062 | CIP-003-6 | R3. | Medium | VSL - Severe | July 1, 2016 | December 1, 2016 | Off-site Audit | 12/14/2018 | 12/18/2018 |

| | |
|---|---|
| **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.)** | During a Compliance Audit conducted from [redacted], NPCC determined that [redacted] (the entity) as a [redacted] it was in violation of CIP-003-6 R3. [redacted]<br><br>This violation started on July 1, 2016 when the entity failed to identify a CIP Senior Manager by name. The violation ended on December 1, 2016 when the entity designated a CIP Senior Manager.<br><br>Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect.<br><br>The root cause of this violation was lack of accountability and management oversight. |
| **Risk Assessment** | The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing designate a CIP Senior Manager, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.<br><br>The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections.<br><br>[redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted]<br><br>[redacted]<br><br>Additionally, the facility has a 24 hour start-up time and only runs when needed.<br><br>No harm is known to have occurred as a result of this noncompliance. |
| **Mitigation** | To mitigate this violation, the entity:<br>1) Designated a CIP Senior Manager<br><br>To prevent recurrence, the entity:<br>2) Created automated tasks to maintain documentation for CIP Senior Manager designations. |
| **Other Factors** | NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017018752 | CIP-007-6 | R5; P5.5 | Medium | Severe | 11/2/2016 (when password length and complexity was not enforced) | 12/14/2016 (when password length and complexity were enforced) | Self-Report | 11/6/2017 | 9/20/2018 |

| | |
|---|---|
| **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 December 5, 2017, the entity submitted a Self-Report stating that, as a as a [redacted] it was in violation with CIP-007-6 R5.<br><br>Specifically, the entity reported that on November 2, 2016, while changing passwords for non-CIP devices, an employee from its [redacted]) team also changed the passwords of two BES Cyber Assets (BCAs) using the same password requirements of the non-CIP devices which was [redacted]. The two BES Cyber Assets (BCAs) were associated with a Medium Impact BES Cyber System (MIBCS) at the primary and backup Control Center. The entity's [redacted] policy clearly documents the password complexity parameter requirements of CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2 for CIP devices. The employee was authorized to change passwords for both CIP and non-CIP devices. The entity discovered this noncompliance on December 9, 2016 during its quarterly access review.<br><br>After reviewing all relevant information, WECC determined the entity failed to implement its documented process for password-only authentication for interactive user access when it did not enforce password parameters for length and complexity, as required by CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2.<br><br>The root cause of the violation was incorrect performance due to lack of process controls around password changes. Specifically, an employee tasked with changing the passwords of non-CIP devices also changed the passwords on two BCAs while performing routine tasks on the non-CIP devices.<br><br>This violation began on November 2, 2016, when password length and complexity was not enforced on two BCAs, and ended on December 14, 2016, when the entity enforced the password length and complexity on the two BCAs, for a total of 43 days of noncompliance. |
| **Risk Assessment** | WECC determined that this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to implement its documented process for password-only authentication for interactive user access when it did not enforce password parameters for length and complexity, as required by CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2.<br><br>The entity implemented good compensating controls. [redacted] No harm is known to have occurred. |
| **Mitigation** | To remediate and mitigate this violation, the entity:<br>a. changed the password length and complexity on the BCAs in scope;<br>b. held a "Fact Finding" meeting with members of the [redacted] team to discuss the CIP asset password policy and employee responsibilities related to the importance of following document processes; and<br>c. reconfigured the BCAs in scope to no longer be CIP assets resulting in the [redacted] team no longer having responsibility for CIP assets. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity has implemented a comprehensive and well organized ICP. Within its ICP is a risk assessment process in which the entity analyzes risk through collaboration between several areas of the company.<br><br>The entity did not receive mitigating credit for self-reporting because the Self-Report was submitted 362 days after the entity discovered the noncompliance. |

| | |
|---|---|
| | WECC considered the entity's CIP-007-6 R5 compliance history in determining the disposition track. WECC considered the entity's CIP-007-6 R5 compliance history to be an aggravating factor in determining the disposition track. |

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2018019340 | CIP-007-6 | R2; P2 | Medium | Severe | 9/7/2017 (when cyber security patches were not tracked) | 2/20/2018 (when the entity tracked, evaluated, and applied applicable software updates) | Self-Certification | 8/14/2018 | 9/24/2018 |

**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 March 1, 2018, the entity submitted a Self-Certification stating that as a [redacted], it was in violation with CIP-007-6 R2.

Specifically, the entity reported that during its Self-Certification review on January 16, 2018, the CIP Lead discovered that commercial software had not been evaluated for security patch applicability that was installed on two Electronic Access Control and Monitoring Systems (EACMS) Cyber Assets associated with a MIBCS at its primary and backup Control Centers. [redacted]. The entity tracked software applicable to its [redacted]" spreadsheet. The [redacted] software had been removed from that list in error. The spreadsheet listed the version of the [redacted] software residing on a single Physical Access Control System (PACS) Cyber Asset as the version in question. The version of [redacted] software residing on the EACMS Cyber Assets was listed on the spreadsheet incorrectly. Earlier in the year, the responsible engineer removed the PACS Cyber Asset from its association to a BES Cyber System. As that was the only Cyber Asset listed on the spreadsheet as containing the [redacted] software, the Cybersecurity Supervisor assumed that all instances of said software had been removed from all MIBCS and associated Cyber Assets. He therefore annotated the entry on the spreadsheet as no longer requiring assessment, when in fact a version of the [redacted] software was still residing on the two EACMS Cyber Assets.

After reviewing all relevant information, WECC determined the entity failed to appropriately implement its patch management process to track, evaluate, and install cyber security patches for applicable Cyber Assets which should include the identification of a source or sources for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists; at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1; and for applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, either apply the patches, create a dated mitigation plan, or revise an existing mitigation plan, as required by CIP-007-6 R2 Parts 2.1, 2.2, and 2.3, respectively.

The root cause of the violation was a less than adequate security patch management tracking process. Specifically, the task of when and how to remove a source from the security patch tracking list was not covered in the documented process.

This violation began on September 7, 2017, when cyber security patches for the two EACMS should have been tracked, and ended on February 20, 2018, when the entity tracked, evaluated, and applied applicable software updates, for a total of 167 days of noncompliance.

**Risk Assessment**

WECC determined that this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to appropriately implement its patch management process to track, evaluate, and install cyber security patches for applicable Cyber Assets which should include the identification of a source or sources for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists; at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1; and for applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, either apply the patches, create a dated mitigation plan, or revise an existing mitigation plan, as required by CIP-007-6 R2 Parts 2.1, 2.2, and 2.3, respectively.

However, the entity implemented good compensating controls. [redacted] No harm is known to have occurred.

**Mitigation**

To remediate and mitigate this violation, the entity:

a. evaluated the commercial software updates released since August 2, 2017;
b. applied applicable security patches to the EACMS Cyber Assets in scope;
c. in conjunction with the commissioning of the new Energy Management System (EMS), update its Security Patch Management Program, to include vendor supported monitored of security patches for the new EMS; and
d. provided training to stakeholders on the updates to the Security Patch Management Program.

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2018019340 | CIP-007-6 | R2; P2 | Medium | Severe | 9/7/2017 (when cyber security patches were not tracked) | 2/20/2018 (when the entity tracked, evaluated, and applied applicable software updates) | Self-Certification | 8/14/2018 | 9/24/2018 |

| | |
|---|---|
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity has implemented a comprehensive and well organized ICP. Within its ICP is a risk assessment process in which the entity analyzes risk through collaboration between several areas of the company.<br><br>The entity did not receive mitigating credit for self-reporting because the Self-Report was submitted 362 days after the entity discovered the noncompliance.<br><br>WECC considered the entity's CIP-007-6 R2 compliance history in determining the disposition track. WECC considered the entity's CIP-007-6 R2 compliance history to be an aggravating factor in determining the disposition track. |

[redacted] $87,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017018489 | CIP-003-2 | R4 | Medium | Severe | 9/22/2010 | 7/12/2017 | Self-Report | 11/8/2017 | 7/13/2018 |

| | |
|---|---|
| **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 October 18, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-003-2 R4. Specifically, the entity reported that on September 22, 2010, an employee from the [redacted] group had inadvertently uploaded Critical Cyber Asset (CCA) information to the [redacted] file share. On July 11, 2017 the [redacted] group discovered the CCA information and notified the [redacted] group. [redacted] examined the information that was stored on the [redacted] file share and found that it was CCA Information as defined by the entity's [redacted] Program and should have been protected according to the program. With further examination of the security permissions associated with the [redacted] file share, the [redacted] group noted 14 unauthorized individuals with access to the CCA information. The CCA information on the [redacted] file share included all [redacted] On July 12, 2017, the [redacted] group removed the CCA information from the [redacted] file share.<br><br>After reviewing all relevant information, WECC determined the entity failed to implement its program to identify, classify, and protect information associated with CCAs, as required by CIP-003-2 R4.<br><br>The root cause of the violation was an individual who did not follow the procedures the entity had in place. Specifically, the individual who placed the CCA information on the [redacted] file share did not follow the expectations outlined in the entity's Information Protection Program. |
| **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. In this instance, the entity failed to implement its program to identify, classify, and protect information associated with CCAs, as required by CIP-003-2 R4.<br><br>The entity had implemented weak controls to prevent and/or detect the noncompliance. However, the entity had compensating controls in place that lessened the risk. Access to the CCA information by someone with malicious intent would not have provided any direct physical or electronic access to the High Impact BES Cyber Systems (HIBCS) or Medium Impact BES Cyber Systems (MIBCS); the access simply provided information that might be used to exploit a vulnerability in the entity's defenses if a malicious actor was able to penetrate the perimeter defenses. The entity had also implemented a defense-in-depth approach to cyber security. [redacted] No harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the entity:<br><br>1) removed the CCA information from the [redacted] file share;<br>2) created a secure [redacted] file share that is designated as a BES Cyber System Information (BCSI) repository with all the appropriate controls; and<br>3) conducted BCSI Protection Program training with appropriate individuals. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. However, it is worth noting that the violation duration for CIP-003-2 R4 is significant and should have been found much sooner, had the entity had better internal controls in place; especially considering the implementation of later versions of the Standard and Requirement.<br><br>WECC considered the entity's CIP-003 R4 compliance history in determining the penalty. WECC considered the entity's CIP-003 R4 compliance history to be an aggravating factor in the penalty determination. |

[redacted] $87,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017018732 | CIP-007-6 | R5 | Medium | Severe | 7/1/2016 | 2/13/2018 | Self-Report | 8/15/2018 | TBD |

| | |
|---|---|
| **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 December 4, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-007-6 R5. Specifically, the entity reported that on July 17, 2017, it discovered multiple devices that did not have methods to enforce authentication of interactive user access. Upon further review conducted on July 26, 2017, the entity verified that three [redacted] Cyber Assets, categorized as Protected Cyber Assets (PCAs) associated with the Medium Impact BES Cyber Systems (MIBCS) without External Routable Connectivity (ERC) at three separate substations did not have passwords. The PCAs contained software and applications written in-house by the entity and an administrator account where the password functionality had not been enabled. The PCAs had been designated to monitor and control the health of three [redacted] at two of the substations, and to monitor and control a [redacted] and [redacted] at a third substation. When CIP-007 Version 5 went into effect, these Cyber Assets were not updated to enforce authentication of interactive user access because of potential operational and safety impacts, as well as a lack of clarity over the interpretation of the Requirement. If the PCA lost communication to the [redacted], designated as BES Cyber Assets (BCAs), for any reason, [redacted] This delay would have caused [redacted] into the [redacted] which the entity believes would have introduced risk to the reliability of the BES.<br><br>After reviewing all relevant information, WECC determined the entity failed to have a method(s) to enforce authentication of interactive user access, where technically feasible; change known default passwords, per Cyber Asset capability; and for password-only authentication for interactive user access, either technically or procedurally enforce password parameters, as required by CIP-007-6 R5 Parts 5.1, 5.4, and 5.5 Sub-Parts 5.5.1 and 5.5.2, respectively for three PCAs.<br><br>The root cause of the violation was an insufficient number of trained or experienced employees assigned to a task. Specifically, in its transition to CIP Version 5, the entity did not ensure that the persons responsible for identifying and implementing security controls for PCAs had adequate training and/or experience to appropriately protect them. |
| **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. In this instance, the entity failed to have a method(s) to enforce authentication of interactive user access, where technically feasible; change known default passwords, per Cyber Asset capability; and for password only authentication for interactive user access, either technically or procedurally enforce password parameters, as required by CIP-007-6 R5 Parts 5.1, 5.4, and 5.5 Sub-Parts 5.5.1 and 5.5.2, respectively.<br><br>The entity had implemented weak controls to prevent and/or detect this noncompliance. However, the entity had compensating controls in place that lessened the risk. [redacted] No harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the entity:<br><br>1) adjusted the operability of the applications on the PCAs to allow for password functionality. This step will take programmatic and/or configuration changes to ensure that the devices and associated applications operate as expected with the enablement of the password functionality. These changes will need to be tested and implemented and are complicated by the fact that the devices are located [redacted];<br>2) enabled the password functionality on the three PCAs to implement authentication of user access;<br>3) changed the default password on the three PCAs; and<br>4) had [redacted] meet with the group responsible for the PCAs to review and discuss the [redacted] procedures. This discussion included specific training related to actions required for default and generic account passwords. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.<br><br>WECC considered the entity's CIP-007 R5 compliance history in determining the penalty. WECC considered the entity's CIP-007 R5 compliance history to be an aggravating factor in the penalty determination. |

[redacted] $87,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017229 | CIP-011-2 | R1 | Medium | Severe | 8/12/2016 | 8/31/2016 | Self-Report | 3/1/2017 | 1/31/2018 |

| | |
|---|---|
| **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 30, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-011-2 R1. Specifically, the entity's [redacted] group utilized the [redacted] application as a patching tool for the Microsoft devices in its High Impact BES Cyber Systems (HIBCS) and associated Electronic Access Control and Monitoring System devices (EACMS) within the [redacted]. To ensure the protection of the HIBCS and [redacted] and associated critical devices in the secure environment, the [redacted] group had utilized a [redacted] approach. The first server resided [redacted] and contained all the pertinent information about Microsoft devices that required patches and updates, which included the [redacted] of the applicable BCAs and PCAs within the HIBCS ESP. The second server resided [redacted] This [redacted] was fully controlled by [redacted] personnel and also contained pertinent information about Microsoft devices that required patches and updates, which included [redacted] of the applicable EACMS within the [redacted]. In accordance with the entity's [redacted] Program, the entity had identified and classified the information on the first and second server as BCSI. The third server resided [redacted], on the entity's [redacted] and [redacted] for the applicable BCAs, PCAs, and EACMS. This server did not contain any IP addresses or host names that would be considered BCSI, but rather the server [redacted]. The [redacted] setup was utilized to ensure that the HIBCS and EACMS were isolated from direct internet connectivity. [redacted] In the spring of 2016, the entity's [redacted] group began experiencing technical issues with the [redacted] application at which time they reinstalled the [redacted] application and reconfigured all [redacted]. The reconfiguration was completed on August 12, 2016. However, on August 26, 2016, the entity's [redacted] group notified the [redacted] department that the [redacted] application setup process inadvertently [redacted] of all its Windows-based HIBCS BCAs and associated Windows-based PCAs, as well as all the EACMS devices, onto a server in its [redacted]. Once the issue was discovered, the entity's [redacted] group took immediate steps to correct the issue: 1) they deleted the [redacted] server's [redacted] database that contained all the [redacted]; 2) on August 31, 2016, they deleted all of the backups of the [redacted] server's [redacted] database that had been created since the reinstall from August 12, 2016 to August 26, 2016.<br><br>After reviewing all relevant information, WECC determined the entity failed to protect and securely handle its BCSI while in storage as required by CIP-011-2 R1 Part 1.2.<br><br>The root cause of the violation was a less than adequate review of work. Specifically, due to a configuration error in the [redacted] application, BCSI was replicated outside the secured CIP environment, and the entity had no peer review process in place to ensure the application was setup correctly. |
| **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. In this instance, the entity failed to protect and securely handle its BCSI while in storage as required by CIP-011-2 R1 Part 1.2.<br><br>The entity had implemented weak controls to prevent this noncompliance. However, the entity had compensating controls in place that lessened the risk. The limited exposure of the BCSI to internal employees was restricted to those who have elevated privileges within the entity's environment and all have a valid business need for access to the [redacted] server. The BSCI that was exposed did not contain usernames or passwords. Without this information, it would be difficult for a person with malicious intent to access any of the devices within the HIBCS or [redacted] Lastly, the entity has a [redacted]. No harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the entity:<br><br>1) deleted its [redacted] server database files and associated backups;<br>2) implemented an automated system in order to avoid manual configuration errors and the need for manual reviews of work; and<br>3) implemented a third-party patching solution that prevents BSCI from being replicated outside of the ESP or [redacted] to avoid future issues with manual patching. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.<br><br>WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] $87,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2018020044 | CIP-011-2 | R1 | Medium | Severe | 7/1/2016 | 1/25/2017 | Self-Report | 12/19/2017 | 1/31/2018 |

| | |
|---|---|
| **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 30, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-011-2 R1. Specifically, the entity reported that it utilized a baselining tool to scan devices within its Physical Access Control System (PACS) environment to gather information related to baseline configurations, device ports, services, accounts, and other information used to meet CIP compliance. The scan engine, which was part of the baselining tool, was located on [redacted] and was used to run scans against PACS assets [redacted]. The scan engine reports the results back to the baselining tool management console where they were kept [redacted]. The baselining tool management console controls the scan engine, telling it where to scan, when to scan, what to scan for, etc. The baselining tool database resides [redacted] On September 28, 2016, during a review of its systems, the entity discovered that both the baselining tool database and management console were not designated as BSCI repositories; therefore, they did not have the protective CIP controls that would normally be applied to BCSI. The missing controls included [redacted] as required by CIP-004-6 R4 Part 4.1.3, and [redacted]<br><br>After reviewing all relevant information, WECC determined the entity failed to appropriately identify BCSI associated with its PACS, as required by CIP-011-2 R1 Part 1.1. Failing to identify the PACS data in the baselining tool as BCSI resulted in it not being identified as a BCSI repository, which in turn caused the entity to not provide the appropriate authorized electronic and physical access controls as required by CIP-004-6 R4 Part 4.1.3.<br><br>The root cause of the violation was the entity's oversight of a critical device which led to the misidentification of the information contained within the device that should have been classified as restricted and therefore protected as BCSI. |
| **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. In this instance, the entity failed to appropriately identify BCSI associated with its PACS, as required by CIP-011-2 R1 Part 1.1. Failing to identify the PACS data in the baselining tool as BCSI resulted in it not being identified as a BCSI repository, which in turn caused the entity to not provide the appropriate authorized electronic and physical access controls as required by CIP-004-6 R4 Part 4.1.3.<br><br>The entity had implemented weak controls to prevent and/or detect this noncompliance. However, the entity had compensating controls in place that lessened the risk. The limited exposure of the BCSI to internal employees was restricted to those who had elevated privileges within the entity's environment and all had a valid business need for access. In addition, all [redacted] was logged and, as needed, [redacted]. Lastly, the entity's [redacted] No harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the entity:<br><br>1) identified the PACS data as BCSI;<br>2) added the baselining tool database and management console servers to a [redacted] and designated them as BCSI repositories;<br>3) deleted all baselining tool backups in the [redacted] and rescheduled future backups to the [redacted];<br>4) updated its process to include accurate information and expectations regarding this Standard and Requirement;<br>5) updated its procedure to include a specific email to be utilized for PACS-related questions; and<br>6) added access controls:<br>i) authorization process to access [redacted]; and<br>ii) established shared account password management;<br>a) all account passwords were reset with system-generated strong passwords;<br>b) account passwords [redacted]; and<br>c) account passwords [redacted]. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.<br><br>WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] $87,000

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2018020045 | CIP-011-2 | R1 | Medium | Severe | 1/12/2017 | 1/12/2017 | Self-Report | 12/19/2017 | 1/31/2018 |

| | |
|---|---|
| **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 May 1, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-011-2 R1. Specifically, the entity reported that on January 12, 2017, its [redacted] group was notified of an event related to an employee potentially sending [redacted] BCSI to an external company earlier that day. The employee stated that errors began occurring with a [redacted] server and since an [redacted] "go live" was a few days away, the employee contacted the [redacted] Customer Support group for resolution. [redacted] provided the software that integrates the [redacted] to the [redacted]. The [redacted] Customer Support requested the employee send the entity's [redacted] configuration database to them so that they could troubleshoot the issues. The employee did not think there was an issue with sending the entity's [redacted] configuration database to [redacted] Customer Support group because: (1) the entity had a signed Mutual Nondisclosure & Confidentiality Agreement (MNDA) with [redacted]; (2) the information [redacted] was requesting was typical configuration database information for a vendor to have; and (3) the employee believed that the configuration database file would not be human readable. The employee was aware of the entity's [redacted] Program requirement to encrypt BCSI sent externally but at the time she did not know the information within the configuration database file was BCSI. Therefore, the employee sent the [redacted] configuration database file, [redacted] by email. After sending the email, the employee opened the configuration database file and realized it included [redacted] The [redacted] servers were MIBCS BCAs and resided in an [redacted], between the HIBCS [redacted] and the MIBCS [redacted]. The purpose of the [redacted] servers was to send and receive [redacted] data for use in the entity's HIBCS.<br><br>After reviewing all relevant information, WECC determined the entity failed to securely handle its BCSI during transit, as required by CIP-011-2 R1 Part 1.2.<br><br>The root cause of the violation was an omission of steps based on assumption. Specifically, the employee that sent the data to an external vendor assumed that it was not BCSI and did not confirm those assumptions prior to sending BCSI [redacted] by email. |
| **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. In this instance, the entity failed to securely handle its BCSI during transit, as required by CIP-011-2 R1 Part 1.2.<br><br>The entity had implemented weak controls to prevent this noncompliance. However, the entity had compensating controls in place that lessoned the risk. The limited exposure of the BCSI to an external source was restricted to a vendor where an NDA already existed and was in effect. The BSCI that was exposed did not contain usernames or passwords. Without this information, it would be difficult for a person with malicious intent to access any of the devices within the HIBCS or MIBCS. No harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the entity:<br><br>1) requested and confirmed [redacted] destroyed all copies of the BCSI that was emailed; and<br>2) provided additional CIP Access Training, which included training on its [redacted] Program, to the employee who sent the [redacted] email. |
| **Other Factors** | WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.<br><br>WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance. |

**COVER PAGE**

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notice of Penalty in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

| Count | Violation ID | Category 1 | Category 2 | Category 3 | Category 4 | Category 5 | Category 6 | Category 7 | Category 8 | Category 9 | Category 10 | Category 11 | Category 12 | CEII PROTECTION (YEARS) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | WECC2016016686 | Yes | | Yes | Yes | | | | | Yes | | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 2 | WECC2017017207 | Yes | Yes | Yes | Yes | | | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 3 | WECC2017016991 | | | Yes | Yes | | | | | | | Yes | | Category 2 – 12: 2 years |
| 4 | WECC2017017204 | | | Yes | Yes | | | | | | Yes | | | Category 2 – 12: 2 years |
| 5 | WECC2017017208 | Yes | Yes | Yes | Yes | | | | | Yes | Yes | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 6 | WECC2017017206 | | | Yes | Yes | | | | | | Yes | | | Category 2 – 12: 2 years |
| 7 | | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | | |
| 11 | | | | | | | | | | | | | | |
| 12 | | | | | | | | | | | | | | |
| 13 | | | | | | | | | | | | | | |
| 14 | | | | | | | | | | | | | | |
| 15 | | | | | | | | | | | | | | |
| 16 | | | | | | | | | | | | | | |
| 17 | | | | | | | | | | | | | | |
| 18 | | | | | | | | | | | | | | |
| 19 | | | | | | | | | | | | | | |
| 20 | | | | | | | | | | | | | | |
| 21 | | | | | | | | | | | | | | |
| 22 | | | | | | | | | | | | | | |
| 23 | | | | | | | | | | | | | | |
| 24 | | | | | | | | | | | | | | |
| 25 | | | | | | | | | | | | | | |
| 26 | | | | | | | | | | | | | | |
| 27 | | | | | | | | | | | | | | |
| 28 | | | | | | | | | | | | | | |
| 29 | | | | | | | | | | | | | | |
| 30 | | | | | | | | | | | | | | |
| 31 | | | | | | | | | | | | | | |
| 32 | | | | | | | | | | | | | | |
| 33 | | | | | | | | | | | | | | |
| 34 | | | | | | | | | | | | | | |
| 35 | | | | | | | | | | | | | | |
| 36 | | | | | | | | | | | | | | |

Filing Date: March 28, 2019

[redacted] – [redacted] NOC-2612 No 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 |
|---|---|---|---|---|---|---|---|---|---|
| WECC2016016686 | CIP-002-5.1 | R1; P1.2 | High | Lower | 7/1/2016 (when the Standard became mandatory and enforceable) | 5/11/2017 (Mitigation Plan completion) | Self-Report | 5/11/2017 | 6/1/2017 |

| | |
|---|---|
| **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 December 16, 2016, the entity submitted a Self-Report stating that, [redacted], it was in noncompliance with CIP-002-5.1 R1.<br><br>Specifically, the entity reported it started its BES Asset analysis utilizing CIP Version 5 criteria in November 2014. The most comprehensive data sources for the entity's asset characteristics were identified and used to categorize the BES Assets. The first entity-approved CIP-002-5.1 BES Cyber System list was published May 12, 2015 to align with the entity's CIP Version 5 transition project. During the entity's November 2016 CIP-002-5.1 BES Cyber System review, a new preferential data source was identified and used to re-categorize the Low Impact Bulk Electric System (BES) Cyber Systems (LIBCS) at a substation to Medium Impact BES Cyber Systems (MIBCS). Upon evaluation of the change, it was determined that the BES Asset information used to initially categorize the LIBCS was unclear and incomplete which resulted in the incorrect impact rating for the BES Cyber Systems at that substation. The entity had categorized the BES Cyber System at the substation as LIBCS because the initial CIP-002-5.1 analysis determined there were only [redacted] lines, with connections to two other substations (weighted value of [redacted]) at the substation, when actually the substation had [redacted] lines, with connections to four other transmission assets (weighted value of [redacted]). Additionally, the substation had [redacted] ties to two different entities. Therefore, BES Cyber Systems should have been identified as MIBCS. The data for all other previously identified BES Cyber Systems was then compared and found to be consistent and did not yield any additional change to impact ratings. The newly categorized MIBCS did not have External Routable Connectivity (ERC).<br><br>After reviewing all relevant information, WECC determined that the entity failed to correctly identify each of its MIBCS as defined by CIP-002-5.1 R1 sub-part 1.2. Consequently, the entity did not apply the applicable CIP requirements to the MIBCS without ERC which it was required to have in place to comply with several other CIP Standards and Requirements.<br><br>The root causes of the violation were less than adequate procedures, documents, and records to ensure proper evaluation of BES Assets. Specifically, the entity utilized an evaluation process that relied on outdated information and a manual review, which resulted in the entity overlooking critical information needed for identifying and categorizing the impact rating of a BES Cyber System.<br><br>WECC determined that this issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable, and ended on May 11, 2017, when the entity completed its Mitigation Plan. |
| **Risk Assessment** | This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to correctly identify each of its MIBCS as defined by CIP-002-5.1 R1 sub-part 1.2.<br><br>The MIBCS in scope had no ERC. The number of CIP requirements applicable to MIBCS without ERC is limited. However, [redacted] had no additional controls to detect or prevent this violation from occurring or compensate for the potential harm. Nevertheless, no harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the entity:<br><br>1) updated its CIP-002 BES Cyber System list to include the reclassification of the BES Cyber System in scope, and obtained CIP senior management signature;<br>2) updated its BES Cyber Systems Identification process to incorporate the accurate data source for CIP-002 identification;<br>3) confirmed compliance or identified deficiencies with other applicable CIP Standards that require mitigation; and<br>4) mitigated all CIP compliance deficiencies resulting from the identification of the MIBCS without ERC, which included patch management, baseline configuration, and cyber vulnerability assessments. |
| **Other Factors** | WECC reviewed [redacted] internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>[redacted]<br><br>[redacted] |

| | | | |
|---|---|---|---|
| [redacted] | | NOC-2612 | No Penalty |
| | WECC considered [redacted] CIP-002-5.1 R1 compliance history in determining the disposition track. WECC considered [redacted] CIP-002-5.1 R1 compliance history to be an aggravating factor in the disposition determination. | | |

[redacted] NOC-2593 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017207 | CIP-007-6 | R1; P1.1 | Medium | High | 7/1/2016 (when the Standard became mandatory and enforceable on [redacted]) | 2/28/2017 (when [redacted] disabled the ports that were not needed) | Compliance Audit | 1/8/2018 | 1/29/2018 |

| | |
|---|---|
| **Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)** | During a Compliance Audit [redacted], WECC determined that [redacted] was in violation of CIP-007-6 R1 Part 1.1<br><br>Specifically, when [redacted] was preparing its baseline on a workstation classified as a BES Cyber Asset (BCA) associated with its Medium Impact BES Cyber System (MIBCS), it evaluated all ports, and those that were considered unneeded were slated for removal. During the audit, [redacted] provided the audit team a [redacted] that [redacted] on the BCA not reflected in the devices' baseline. Upon further review, [redacted] determined that the baseline was correct and that the unnecessary ports had been overlooked during the removal process. The BCA in scope is an engineering workstation in the primary Control Center's separate but associated data center, and is not actively used by [redacted] to monitor or control the supervisory control and data acquisition (SCADA) network.<br><br>WECC concluded that [redacted] failed to ensure that only those logical network accessible ports that were determined to be needed on a BCA within the MIBCS were enabled.<br><br>The root cause of the violation was due to an oversight by the employee responsible for disabling the ports who did not follow [redacted]'s documented procedure for disabling unneeded ports that were not part of the baseline configuration and the lack of an internal control to ensure employees followed the procedure.<br><br>The violation duration was 242 days. [redacted] did not have detective controls in place that could have helped identify the issues sooner and to lessen the violation duration. WECC believes had it not been for [redacted]'s Compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC applied an aggravating factor and escalated the disposition treatment to an expedited settlement. |
| **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. In this instance, [redacted] failed to enable only logical network accessible ports that were determined to be needed. Such failure could result in a malicious actor gaining access to the BCA to cause harm to [redacted]'s SCADA system, which could affect [redacted]'s [redacted] and its [redacted].<br><br>However, [redacted] implemented access control at the Electronic Security Perimeter (ESP) to only allow approved traffic into the protected network. [redacted] also implemented [redacted] inside the ESP. Based on the controls in place, WECC determined the likelihood of the potential harm occurring was low. |
| **Mitigation** | To mitigate this violation, [redacted]:<br><br>1) disabled logical network ports determined to be unneeded on the BES Cyber Asset in scope;<br>2) updated documentation to require a [redacted] be performed each time a change is made to a baseline configuration and validate it against the baseline;<br>3) documented a process to periodically review baseline configurations against a report of open ports to ensure only necessary logical ports are open and that the baselines are accurate;<br>4) trained personnel on the updated documentation and processes; and<br>5) added CIP-007 as a regular agenda item for the monthly CIP Compliance meetings. |
| **Other Factors** | WECC reviewed [redacted]'s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although [redacted] has a documented ICP, WECC determined that [redacted] did not implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner.<br><br>WECC considered [redacted]'s compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2593 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017016991 | CIP-007-6 | R2; P2.1, 2.2, 2.3 | Medium | High | 7/1/2016 (when the Standard became mandatory and enforceable on [redacted]) | 2/23/2017 (for Part 2.1 when [redacted] included patching sources in its patch management process)<br><br>9/21/2017 (for Parts 2.2 and 2.3 when [redacted] evaluated security patches and updated its mitigation plan) | Self-Report | 8/2/2017 | 12/22/2017 |

**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 [redacted] submitted a Self-Report, stating that, [redacted] it was in violation of CIP-007-6 R2 Part 2.2.

Specifically, [redacted] reported that, for three Cyber Assets classified as Bulk Electric System Cyber Assets (BCAs) it did not assess security patches after the initial review of security patches on July 1, 2016 was conducted, pursuant to CIP-007-6 R2 Part 2.2. The devices and software in scope support the primary and backup Control Centers containing a Medium Impact Bulk Electric System Cyber System (MIBCS).

After reviewing all relevant information, WECC determined a scope increase from the original Self-Report. WECC identified three additional devices classified as Protected Cyber Assets (PCA), where [redacted] failed to maintain documentation that it had performed a patch evaluation at least once every 35 days, as required by Part 2.2. Additionally, [redacted] did not document a patch source as required by Part 2.1. for one Electronic Access or Monitoring System (EACMS) and seven Physical Access Control Systems (PACS). Lastly, WECC determined that [redacted] created a mitigation plan for security patches assessed and not applied; however, did not include specific implementation timeframes, as required by Part 2.3.

The root cause of the violation was a less than adequate security patch management program for CIP compliance. Specifically, [redacted]'s lack of knowledge and understanding of CIP Standards resulted in the implementation of a less than adequate security patch management program.

The violation duration was 237 days for Part 2.1 and 447 days for Parts 2.2 and 2.3. [redacted] did not have detective controls in place that could have helped identify the issues sooner and to lessen the violation duration. WECC believes had it not been for [redacted]'s Compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC applied an aggravating factor and escalated the disposition treatment to an expedited settlement.

**Risk Assessment**

This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, [redacted] failed to evaluate security patches within 35 calendar days of the last evaluation; to document a patch source for applicable assets; to maintain documentation that it had performed patch evaluations once every 35 calendar days for its MIBCS and associated PCAs, EACMS and PACs, pursuant to CIP-007-5 R2 Parts 2.1, 2.2 and 2.3. Such failure could potentially result in a malicious actor using known attack methods to gain control of a BES Cyber System. If control was established, the malicious actor could cause reboots, freezes, or install malware in the systems. An attack on the devices in scope could cause disruption, restriction of visibility, or affect the operating capabilities of [redacted]'s systems which could lead to unintended consequences that could affect the BES.

However, the likelihood of the risk occurring was significantly reduced by the preventative controls [redacted] had implemented. Specifically, [redacted] implemented protections at each Electronic Security Perimeter (ESP) to permit only allowed traffic into and out of the ESP as well as implementing Intrusion Detection System devices to each network to detect malicious code. Three of the devices in question were not connected to the public internet; had no browser access or email, and were protected by CIP controls in CIP-004, CIP-005, CIP-006 and CIP-007. Infractions related to the remaining eleven devices constituted documentation failures for the Standard, however the evaluations were being conducted. In addition, [redacted] is a very small municipal power company that employs few staff and has an extremely low turnover. Based on this, WECC determined that the likelihood of the potential harm occurring was low.

**Mitigation**

To mitigate this violation, [redacted]:

1) updated the patch tracking workbook to include and maintain a list of all applicable devices and software;
2) installed applicable patches where appropriate or mitigation plans with required implementation timeframes were developed and approved by the CIP senior manager;
3) reviewed other supporting documents to determine if additional updates were needed;
4) now maintains a list for all applicable devices under the purview of the system support group (i.e. EACMS, PACS, and BCA switches); and
5) added patch tracking to its bi-monthly CIP Compliance Meeting agenda. Regular discussions with an appropriate level of view will ensure maintenance and consistency across SCADA Support and Systems Support to continue to meet expectations over time.

| [redacted] | NOC-2593 | $0 |
|---|---|---|

| | |
|---|---|
| **Other Factors** | WECC reviewed [redacted]'s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although [redacted] has a documented ICP, WECC determined that [redacted] did not implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner.<br><br>WECC considered [redacted]'s compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2593 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017204 | CIP-004-6 | R4; P4.1, 4.2 | Medium | Moderate | 7/1/2016 (for Part 4.1 when the Standard became mandatory and enforceable on [redacted])<br><br>10/1/2016 (for Part 4.2 when the Standard became mandatory and enforceable on [redacted]) | 12/8/2017 (when [redacted] updated documented authorization records for access granted, and verified CIP access against authorization records) | Compliance Audit | 12/13/2017 | 1/29/2018 |

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

During a Compliance Audit [redacted] WECC determined that [redacted] was in violation of CIP-004-6 R4 Part 4.1 and Part 4.2.

Specifically, for CIP-004-6 R4 Part 4.1, WECC determined that [redacted] was not able to demonstrate that it implemented its access management program per its documented processes. [redacted] documented that it utilized an Access Request Form and a CIP-004 Access Management Program spreadsheet when authorizing electronic or unescorted physical access to its Medium Impact Bulk Electric System Cyber System (MIBCS) and their associated Cyber Assets or when authorizing access to designated storage locations. From July 1, 2016 through November 21, 2016, [redacted] granted electronic and/or unescorted physical access to its MIBCS and associated Cyber Assets to five employees without having completed [redacted]'s Access Request Form per [redacted]'s Access Management and Revocation Program and Procedure. Relating to CIP-004-6 R4 Part 4.2, [redacted] states in its Access Management and Revocation Program and Procedure that quarterly reviews are conducted by comparing Access Request Forms to its CIP Unescorted Physical Security Perimeter and Electronic Security Perimeter list. However, [redacted] did not utilize the Access Request Forms; therefore, [redacted] did not have dated documentation of the verification between the list of employees who have been authorized for access and the list of personnel who have access, at least one each calendar quarter.

WECC concluded that [redacted] used a process other than that which was documented and failed to update its documented process to authorize electronic access, unescorted physical access, and/or access to designated storage locations.

The root cause of the violation was management policy guidance or expectations were not well-defined, understood, or enforced. Specifically, [redacted] was new to CIP Standards and Requirements and its subject matter experts and compliance staff lacked understanding of required evidence and retention periods.

The violation duration was 525 days for Part 4.1 and 433 days for Part 4.2. [redacted] did not have detective controls in place that could have helped identify the issues sooner and to lessen the violation duration. WECC believes had it not been for [redacted]'s Compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC applied an aggravating factor and escalated the disposition treatment to an expedited settlement.

**Risk Assessment**

This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, [redacted] failed to document dated authorization records and include a business need for access granting pursuant to CIP-004-6 R4 Part 4.1, and failed to verify once each calendar quarter that employees with CIP access had authorization records pursuant to CIP-004-6 R4 Part 4.2. Such failure could result in unauthorized employees having electronic access, unescorted physical access and/or access to designated storage locations containing BES Cyber System information. This access could intentionally or unintentionally lead to misuse of information or devices that support [redacted]'s compliance obligations; thereby potentially affecting the reliability of the BPS.

[redacted] is a very small municipal power company that employs few staff and has an extremely low turnover. Based on this, WECC determined that the potential likelihood of the harm occurring was low.

**Mitigation**

To mitigate this violation, [redacted]:

1) updated its Access Management and Revocation Program and Procedure to reflect current practices;
2) holds monthly meetings to discuss CIP compliance;
3) updated its spreadsheet to document employees that have access and to document the performance of quarterly reviews, annual reviews, and revocations; and
4) provided training on the new Access Management and Revocation Program and Procedures.

**Other Factors**

WECC reviewed [redacted]'s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although [redacted] has a documented ICP, WECC determined that [redacted] did not implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner.

WECC considered [redacted]'s compliance history and determined there were no relevant instances of noncompliance.

[redacted] NOC-2593 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017208 | CIP-010-2 | R1; P1.1, 1.2, 1.3, and 1.4 | Medium | High | 7/1/2016 (when the Standard became mandatory and enforceable on [redacted]) | 5/31/2017 (when baseline configurations were updated) | Compliance Audit | 1/22/2018 | 2/26/2018 |

| | |
|---|---|
| **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.)** | During a Compliance Audit [redacted], WECC determined that [redacted] was in violation of CIP-010-2 R1 Parts 1.1.4, 1.1.5, 1.2, 1.3 and 1.4.<br><br>Specifically, [redacted] failed to include [redacted] in its baseline configuration for [redacted] classified as Protected Cyber Assets; one Physical Access Control Systems (PACS) server; one supervisory control and data acquisition (SCADA) [redacted] classified as a Bulk Electric System (BES) Cyber Asset, one [redacted] and three [redacted] classified as Electronic Access Control or Monitoring Systems (EACMS), all associated with its Medium Impact Bulk Electric System (BES) Cyber System (MIBCS) pursuant to CIP-010-2 R1 Part 1.1.4.<br><br>WECC auditors also identified a PACS server that had a security patch update installed after the mandatory and enforceable date of July 1, 2016, that was not included on the device's baseline configuration pursuant to CIP-010-2 R1 Part 1.1.5. Lastly, for the PACS [redacted], [redacted] was not able to provide evidence that any of the required change management activities per CIP-010-2 R1 Parts 1.2, 1.3 and 1.4 had been performed when it installed [redacted] on the PACS [redacted] on January 30, 2017. The installation of this software would have caused a deviation from the device's baseline configuration.<br><br>WECC concluded that [redacted] failed to: 1) include logical network accessible ports in its baseline configuration for 10 devices; 2) include an installed security patch in the baseline configuration for one PACS [redacted]; and 3) provide evidence that it performed CIP-010-2 R1 Parts 1.1, 1.2, 1.3, and 1.4 for the installed security patch on the PACS [redacted].<br><br>The root cause of the violation was [redacted] not following its documented process. Specifically, [redacted] developed adequate documented processes to ensure compliance with CIP-010-2 R1; however, [redacted] did not have adequate internal controls to ensure those processes were followed.<br><br>The violation duration was 334 days. [redacted] did not have detective controls in place that could have helped identify the issues sooner and to lessen the violation duration. WECC believes had it not been for [redacted]'s Compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC applied an aggravating factor and escalated the disposition treatment to an expedited settlement. |
| **Risk Assessment** | This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, [redacted] failed to maintain baseline configurations to include logical network accessible ports and security patches applied to assets, and failed to perform required change management activities for BES Cyber Assets, EACMS, and PACS pursuant to CIP-010-2 R1 Parts 1.1, 1.2, 1.3, and 1.4. Such failure could result in a lack of protective measures for those ports due to not knowing which ports were accessible, which could lead to cyber security vulnerabilities in those network devices, thereby potentially affecting [redacted]'s [redacted] and its [redacted].<br><br>[redacted] did not implement adequate internal controls to ensure its documented processes for CIP-010-2 R1 were followed; to ensure potential incidents caused by poorly executed baseline configurations and change management processes would be minimized; and to detect baseline configuration errors and change management process exclusions. [redacted] is a small municipal power company. Based on this, WECC determined that the likelihood of the potential harm occurring was low. |
| **Mitigation** | To mitigate this violation, [redacted]:<br><br>1) updated the baseline configurations for the devices in scope;<br>2) updated its Change Control and Configuration Management Procedure to include the required use of a CIP-010 Change Request form for the documentation of all changes, including the verification that all CIP-005, CIP-007, and CIP-010 security controls are met and a step to update baseline configuration changes as required by CIP-010-2 R1 Part 1.3;<br>3) held a meeting to discuss the changes to the procedure and offer guidance to ensure the baselines are consistent, accurate, and updated quickly after a well-managed change to the CIP-010 R1 part 1.1 baseline component;<br>4) included baseline changes as a standing item for discussion and reinforcement at monthly CIP compliance meetings; and<br>5) will review all baselines, on an annual basis at the minimum, to ensure they are accurate and up-to-date. |

[redacted] NOC-2593 $0

| | |
|---|---|
| **Other Factors** | WECC reviewed [redacted]'s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although [redacted] has a documented ICP, WECC determined that [redacted] did not implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner.<br><br>WECC considered [redacted]'s compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2593 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| WECC2017017206 | CIP-004-6 | R5; P5.1 | Medium | Moderate | 8/24/2016 (when documented process were not followed) | 12/8/2017 Mitigation Plan completion | Compliance Audit | 12/8/2017 | 2/8/2018 |

| | |
|---|---|
| **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.)** | During a Compliance Audit [redacted] WECC determined that [redacted] it was in violation of CIP-004-6 R5 Part 5.1.<br><br>Specifically, [redacted] was unable to demonstrate that it implemented its access management program per its documented processes. [redacted] documented that it utilized an Access Request Form and a CIP-004 Access Management Program spreadsheet when revoking electronic or unescorted physical access to its Medium Impact Bulk Electric System Cyber System (MIBCS) and their associated Cyber Assets. However, [redacted] was not able to provide evidence on the spreadsheet of one employee's unescorted physical access being revoked, nor did [redacted] provide any completed Access Request Forms as stated in its process document.<br><br>Additionally, [redacted] was unable to provide evidence demonstrating that the process to remove one retiring employee's unescorted physical access was initiated upon a termination action and the removals completed within 24 hours of the termination action. WECC reviewed an email dated August 23, 2016, which [redacted] submitted as evidence demonstrating the removal of an employee's ability for unescorted physical access upon a termination action. The email stated that an employee no longer worked for the City and should no longer have access to the primary and backup Control Centers; however, the email contained no confirmation that the employee's unescorted physical access had been removed within 24 hours of the termination action, nor was [redacted] able to provide system logs to confirm access revocation had occurred within 24 hours of the termination action.<br><br>After reviewing all relevant information, WECC determined a decrease in scope from the original audit finding. Subsequent to the audit, [redacted] was able to provide WECC evidence that demonstrated compliance of revocation of unescorted physical access for the one employee in scope. However, WECC determined that [redacted] did fail to follow its documented processes for initiating removal of an employee's ability for CIP access upon a termination action.<br><br>The root cause of the violation was management policy guidance or expectations were not well defined, understood, or enforced. Specifically, [redacted] staff lacked the understanding of required evidence to demonstrate compliance and the retention periods for said evidence.<br><br>The violation duration was 471 days. [redacted] did not have detective controls in place that could have helped identify the issues sooner and to lessen the violation duration. WECC believes had it not been for [redacted]'s Compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC applied an aggravating factor and escalated the disposition treatment to an expedited settlement. |
| **Risk Assessment** | This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, [redacted] failed to provide evidence to demonstrate the removal of the ability for access or the actual unescorted physical access within 24 hours after a termination action. Such failure could result in unauthorized physical access to BES Cyber Systems with the intent to cause damage or outages; thereby potentially affecting the reliability of the BPS.<br><br>[redacted] is a very small municipal power company that employs few staff and has an extremely low turnover. Based on this, WECC determined that likelihood of the potential harm occurring was low. |
| **Mitigation** | To mitigate this violation, [redacted]:<br><br>1) updated its Access Management and Revocation Program and Procedure to reflect current practices and detailed tracking of CIP access management;<br>2) holds monthly meetings to discuss CIP compliance;<br>3) updated its spreadsheet to document employees that have access and to document the performance of quarterly reviews, annual reviews, and revocations; and<br>4) provided training on the new Access Management and Revocation Program and Procedures. |
| **Other Factors** | WECC reviewed [redacted]'s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although [redacted] has a documented ICP, WECC determined that [redacted] did not implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner.<br><br>WECC considered [redacted]'s compliance history and determined there were no relevant instances of noncompliance. |

**COVER PAGE**

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notice 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 | FRCC2018019002 | | | Yes | Yes | | | | | | | | Yes | Category 2 – 12: 2 years |
| 2 | FRCC2018019016 | Yes | | Yes | Yes | | | | | | | | | Category 1: 3 years; Category 2 – 12: 2 years |
| 3 | SPP2017018137 | | | Yes | Yes | | | | Yes | Yes | Yes | | Yes | Category 2 – 12: 2 year |
| 4 | | | | | | | | | | | | | | |
| 5 | | | | | | | | | | | | | | |
| 6 | | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | | |
| 11 | | | | | | | | | | | | | | |
| 12 | | | | | | | | | | | | | | |
| 13 | | | | | | | | | | | | | | |
| 14 | | | | | | | | | | | | | | |
| 15 | | | | | | | | | | | | | | |
| 16 | | | | | | | | | | | | | | |
| 17 | | | | | | | | | | | | | | |
| 18 | | | | | | | | | | | | | | |
| 19 | | | | | | | | | | | | | | |
| 20 | | | | | | | | | | | | | | |
| 21 | | | | | | | | | | | | | | |
| 22 | | | | | | | | | | | | | | |
| 23 | | | | | | | | | | | | | | |
| 24 | | | | | | | | | | | | | | |
| 25 | | | | | | | | | | | | | | |
| 26 | | | | | | | | | | | | | | |
| 27 | | | | | | | | | | | | | | |
| 28 | | | | | | | | | | | | | | |
| 29 | | | | | | | | | | | | | | |
| 30 | | | | | | | | | | | | | | |
| 31 | | | | | | | | | | | | | | |
| 32 | | | | | | | | | | | | | | |
| 33 | | | | | | | | | | | | | | |
| 34 | | | | | | | | | | | | | | |
| 35 | | | | | | | | | | | | | | |
| 36 | | | | | | | | | | | | | | |
| 37 | | | | | | | | | | | | | | |

Filing Date: February 28, 2019

[redacted] – [redacted] NOC-2607 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| FRCC2018019002 | CIP-007-6 | R2; P2.2 | Medium | Severe | 3/23/2017 (the day after the previous mitigation plan was completed) | 3/5/2018 (when patches were evaluated and completed) | Spot Check | 3/31/2018 | 8/10/2018 |

| | |
|---|---|
| **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.)** | During a Spot Check conducted from January 15, 2018 through January 19, 2018, FRCC determined that the Entity, [redacted], was in noncompliance with CIP-007-6 R2 (Part 2.2).<br><br>This noncompliance started on March 23, 2017, when the Entity failed to evaluate its security patches for applicability at least once every 35 calendar days on 12 out of 29 (41.4%) Cyber Assets (CA). The noncompliance ended March 5, 2018 when patches were evaluated and completed.<br><br>The missed patches were for four (4) Energy Management System (EMS) servers, five (5) operator workstations within the EMS network, one (1) PACS server, and two (2) Programmable Local Access Control Panels. Although every patch was not critical, there were critical patches that missed the 35-day installation window. These missed patches could have prolonged the presence of software vulnerabilities, which, if exploited, could grant access to unauthorized personnel or misuse of Cyber Assets.<br><br>Although the patches in question did not meet the 35-day requirement, they were being installed on a quarterly basis. The entity did perform a vulnerability review and determined that during the time when the available security patches were not evaluated and applied as required, there were no known instances of unauthorized access or breaches to the entity's BES Cyber Systems and their associated EACMS, PACS, and PCAs.<br><br>Specifically, the Entity CAs were being monitored by three external vendors. For all nine (9) of the CAs managed by External Vendor #2 and three (3) out of five (5) CAs managed by External Vendor #3, the Entity failed to at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1 as required by CIP-007-6 (R2.2).<br><br>The root cause was multiple vendors responsible for patching on different segments (Supervisory Control and Data Acquisition (SCADA), non-SCADA) of the Entity CAs and a lack of the Entity oversight. |
| **Risk Assessment** | This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).<br><br>Specifically, the Entity's failure to execute their patch management process could have prolonged the presence of software vulnerabilities, which if exploited, could grant access to unauthorized personnel or misuse of Cyber Assets impacting the reliability of the BPS.<br><br>The risk was reduced because all the devices were protected by a Physical Security Perimeter and all the Cyber Assets were within the Electronic Security Perimeter. In addition, Vendor #3 was completing the assessments quarterly instead of every 35 days.<br><br>No harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the Entity:<br>1) evaluated and applied all security patches;<br>2) designated a single vendor (Vendor #1) to monitor for all newly released security patches<br>3) verified with Vendor #2 their responsibility to apply security patches on monthly basis;<br>4) developed internal control to ensure evaluation and application of Vendor #2 security patches;<br>5) developed situational awareness internal control to ensure SME applies security patches, including:<br>- set-up an email from HelpDesk to Vendor #1 SME as a reminder to coordinate patching that needs to be completed for all vendors<br>- set-up an email from HelpDesk informing the Entity SME that patching due date is approaching; and<br>6) trained all applicable personnel on new processes and/or procedures. |
| **Other Factors** | FRCC determined the Entity's internal compliance program (ICP) and positive cooperation as mitigating factors when determining the penalty.<br><br>FRCC reviewed the Entity's compliance history and determined there was a relevant instance of noncompliance, which is considered to be aggravating. The previous extent of condition and gap |

[redacted] – [redacted] NOC-2607 $0

| | |
|---|---|
| | assessment of [redacted] appeared to be complete, however the mitigation only addressed Vendor #1. Subsequent issues were discovered with Vendors #2 and #3 that were not addressed by the previous mitigation plan. The current instance was discovered as part of a follow up Spot Check of [redacted].<br><br>FRCC resolved this noncompliance in an SNOP as aggravation for the previous noncompliance. |

[redacted] – [redacted] NOC-2607 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| FRCC2018019016 | CIP-007-6 | R5: P5.6; 5.7 | Medium | Severe | 7/1/2016 (when the Entity failed to enforce password changes and limit unsuccessful authentication attempts or generate alerts) | 1/24/2018 (when the Entity corrected the patching issues, updated the procedures to prevent reoccurrence, and trained appropriate personnel) | Spot Check | 6/1/2018 | 8/10/2018 |

| | |
|---|---|
| **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.)** | During a Spot Check conducted from January 15, 2018 through January 19, 2018, FRCC determined that the Entity, [redacted], was in noncompliance with CIP-007-6 R5 (Parts 5.6 & 5.7).<br><br>This noncompliance started when the Standard became mandatory and enforceable on July 1, 2016, when the Entity failed to enforce password changes, and limit unsuccessful authentication attempts or generate alerts, and ended on January 24, 2018 when the Entity updated their processes to require the changing of passwords and limited unsuccessful authentication attempts as well as established required alerting.<br><br>Specifically, for Part 5.6, the Entity failed to enforce password changes or an obligation to change the password at least once every 15 calendar months for all eight (8) shared accounts as required by CIP-007-6 R5, Part 5.6.<br><br>For Part 5.7, the Entity failed to implement controls to limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts on the three (3) firewalls and four (4) switches as required by CIP-007-6 R5, Part 5.7.<br><br>The root cause was an absence of internal controls related to password changes on shared accounts. |
| **Risk Assessment** | This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system.<br><br>Specifically, the Entity's failure to change the passwords by the required timeframe could expose the passwords to malicious individuals allowing unauthorized access to Cyber Assets.<br><br>This risk was increased because some of the Cyber Assets at issue were designed to provide perimeter protection to other BES Cyber Assets. Additionally, the Entity's failure to configure an account lockout policy or alerting after a certain number of failed authentication attempts, which serves to prevent unauthorized access through an online guessing or brute force attack, could have caused reliability concerns for the Entity.<br><br>From July 1, 2016 to June 1, 2018 there was no known unauthorized access or breaches to any of the Entity's Cyber Assets.<br><br>No harm is known to have occurred. |
| **Mitigation** | To mitigate this violation, the Entity:<br>P5.6:<br>1) scheduled the process of changing the passwords for shared accounts to take place each year during the first quarter to ensure they are changed within the required timeframe;<br>2) set up Help Desk ticketing system that will issue auto-generated tickets the first month of each year with the list of shared accounts in the body of the ticket that need to have their passwords changed;<br>3) reviewed all shared accounts to ensure that all accounts are justified and still needed;<br>4) changed all shared account passwords;<br>5) configured [redacted] to monitor all shared accounts and track when passwords have been changed; and<br>6) generated an annual report that identifies shared accounts where the passwords have not been changed in the last 365 days.<br><br>P5.7:<br>1) updated SIEM to analyze the logs from the firewalls and switches;<br>2) tested and verified logs for all applicable Cyber Assets in SIEM;<br>3) created rules and reporting in SIEM to produce alerts based on the threshold of 5 unsuccessful attempts occurring; and<br>4) trained Entity personnel on newly instituted internal controls for the requirement. |

[redacted] – [redacted] NOC-2607 $0

| | |
|---|---|
| **Other Factors** | FRCC determined the Entity's internal compliance program (ICP) and positive cooperation as mitigating factors when determining the penalty.<br><br>FRCC reviewed the Entity's compliance history and determined there were no relevant instances of noncompliance. |

[redacted] NOC-2614 $0

| NERC Violation ID | Reliability Standard | Req. | Violation Risk Factor | Violation Severity Level | Violation Start Date | Violation End Date | Method of Discovery | Mitigation Completion Date | Date Regional Entity Verified Completion of Mitigation |
|---|---|---|---|---|---|---|---|---|---|
| SPP2017018137 | CIP-008-3 | R1 | Lower | High | 3/17/2016 (fifteen months [redacted] had transitioned to CIP Version 5] after successful completion of the last test) | 9/26/2017 (test was successfully completed) | Self-Report | 8/22/2018 | 1/11/2019 |

| | |
|---|---|
| **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 August 10, 2017, [redacted] submitted a Self-Report, stating that, as a [redacted], it was in noncompliance with CIP-008-3 R1. [redacted] stated that it failed to perform an adequate test of its Cyber Security Incident response plan between December 17, 2014 and September 26, 2017. [redacted] reports that it did perform a test on March 28, 2017, but that test did not meet [redacted] standards; specifically the test was more general than [redacted] expected and did not include specific steps for implementing a response to a Cyber Security Incident to the degree that [redacted] expected. [redacted] states that it detected this noncompliance after a new CIP Senior Manager was designated and the CIP Senior Manager conducted a full review of [redacted] compliance activities.<br><br>The noncompliance was caused by inadequate internal controls to provide oversight regarding the completion of this task. |
| **Risk Assessment** | The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the bulk power system. [redacted] conducted a test that did not meet all the requirements of its program (albeit 11 days late), thus the risk of the noncompliance was reduced because the noncompliance was essentially for conducting an incomplete test, as opposed to not conducting any type of testing. Additionally, the subsequent testing of the Cyber Security Incident plan was successful. Finally, employees are trained under CIP-004-6 R2, which includes response and recovery to Cyber Security Incidents. No harm is known to have occurred. |
| **Mitigation** | To mitigate this noncompliance, [redacted]<br><br>1) performed the required test;<br>2) reviewed and revised the Cyber Security Incident response plan to better align with its standards for level of detail; and<br>3) scheduled the next required execution of the Cyber Security Incident response plan to occur within 11 months of the last test. |
| **Other Factors** | MRO reviewed [redacted] internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.<br><br>MRO considered [redacted] compliance history in determining the disposition track. [redacted] relevant prior noncompliance with CIP-008-3 R1 includes a prior moderate risk violation of CIP-008-3 R1 ([redacted] that was mitigated on [redacted]. [redacted]. In the prior violation, [redacted] conducted tests in 2012 and 2013 that were incomplete under its procedure. [redacted]. MRO considered [redacted] CIP-008-3 R1 compliance history to be an aggravating factor in the disposition track.<br><br>In determining the penalty, MRO considered the investments that [redacted] has made in its compliance program since the [redacted]. At the time of the [redacted], [redacted] Finally, the noncompliance was detected after [redacted] named a new CIP Senior Manager, who undertook a review of [redacted] CIP program that included two internal audits conducted by third-party compliance companies. |