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.

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

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]. To mitigate this violation, the entity: 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; 2) held internal meetings with Subject Matter Experts to determine approaches for preventing a future reoccurrence of this issue; 3) reviewed [redacted], tested as needed, and remediated where necessary; 4) deployed [redacted] as noted in the root-cause explanation; 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 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. 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. 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.

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].

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.

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.

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:

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;
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;
3) integrated the evidence requirements into the entity's ports and services policies and procedures;
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
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.

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.

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. 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.					

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.

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.

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;

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;
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;
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];
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
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.

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. 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.

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. 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. 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: 1) verified the security controls of the baseline configuration change and documented the verification; 2) updated its baseline configuration for a change that deviated from an existing baseline configuration; 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 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. 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. 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.

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. 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. 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, WECC2017614526 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. 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]
Mitigation	To mitigate this violation, the entity has: 1) placed the BCA inside the ESP; and 2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices.
Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017614526, 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. WECC 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
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.

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.

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, WECC2017614526 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.

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) documented all enabled logical network accessible ports; and
2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices.

Other Factors

These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017614526, 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.

WECC 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
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. 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. 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, WECC2017614526 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. 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) added the BCA to the patch source tracking spreadsheet; 2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices; and 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.

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, WECC2017614526 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.

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.

Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017614526, 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. 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.

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, WECC2017614526 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;

	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 4) updated the change management software to require: a. a documented baseline configuration be completed as part of the commissioning process before deploying into an ESP; and 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, WECC2017614526, 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. WECC 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
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. 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. 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: 1) activated alarms for existing forced entry and door held open alarms during business hours; 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 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, WECC2017614526, 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. WECC 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
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] 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. 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. 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: 1) evaluated security patches released since the previous evaluation; 2) installed the applicable security patch. 3) provided additional training to technical staff on security patching activities; 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; 5) updated its patch management program to clearly define the process for creating a mitigation plan when a security patch cannot be installed; 6) trained technicians on the new process; 7) created an annual task to review the patch management program with technicians to reinforce the entire patch management program; 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; 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 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.

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]

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.

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.

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:

1) evaluated security patches released since the previous evaluation;
2) installed the applicable security patch.
3) provided additional training to technical staff on security patching activities;
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;
5) updated its patch management program to clearly define the process for creating a mitigation plan when a security patch cannot be installed;
6) trained technicians on the new process;
7) created an annual task to review the patch management program with technicians to reinforce the entire patch management program;
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;
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
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, WECC2017614526, 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.

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.

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]

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.

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.

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:

1) evaluated security patches released since the previous evaluation;
2) installed the applicable security patch.
3) provided additional training to technical staff on security patching activities;
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;
5) updated its patch management program to clearly define the process for creating a mitigation plan when a security patch cannot be installed;
6) trained technicians on the new process;
7) created an annual task to review the patch management program with technicians to reinforce the entire patch management program;
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;
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
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, WECC2017614526, 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.

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.

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]

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.

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:

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;
2) updated its technician procedure to include more detail on configuring the Windows auditing section; and
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, WECC2017614526, 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.

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.

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;

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; 6) communicated changes to its Change Advisory Board; and 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. WECC considered the entity's CIP-002-5.1 R1 compliance history to be an aggravating factor in the penalty determination.						