COVER PAGE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Other Factors

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

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

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

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

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