COVER PAGE

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

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

Filing Date: August 29, 2019

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

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

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

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