COVER PAGE

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

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	FRCC2018019002			Yes	Yes								Yes	Category 2 – 12: 2 years
2	FRCC2018019016	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
3	SPP2017018137			Yes	Yes				Yes	Yes	Yes		Yes	Category 2 – 12: 2 year
4														
5														
6														
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														
25														
26														
27														
28														
29														
30														
31														
32														
33														
34														
35														
36														
37														

Filing Date: February 28, 2019

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

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

	assessment of [redacted] appeared to be complete, however the mitigation only addressed Vendor #1. Subsequent issues were discovered with Vendors #2 and #3 that were not addressed by the previous mitigation plan. The current instance was discovered as part of a follow up Spot Check of [redacted]. FRCC resolved this noncompliance in an SNOP as aggravation for the previous 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
FRCC2018019016	CIP-007-6	R5: P5.6; 5.7	Medium	Severe	7/1/2016 (when the Entity failed to enforce password changes and limit unsuccessful authentication attempts or generate alerts)	1/24/2018 (when the Entity corrected the patching issues, updated the procedures to prevent reoccurrence, and trained appropriate personnel)	Spot Check	6/1/2018	8/10/2018

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

Other Factors	FRCC determined the Entity's internal compliance program (ICP) and positive cooperation as mitigating factors when determining the penalty. FRCC reviewed 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
SPP2017018137	CIP-008-3	R1	Lower	High	3/17/2016 (fifteen months [redacted] had transitioned to CIP Version 5] after successful completion of the last test)	9/26/2017 (test was successfully completed)	Self-Report	8/22/2018	1/11/2019

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