COVER PAGE

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

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

Filing Date: October 31, 2019

[redacted] $84,000

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
NPCC2018019849	CIP-005-5	R1.	Medium	VSL - Severe	7/1/2016	6/6/2018	On-site Audit	9/6/2018	7/31/2019

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

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
NPCC2018019848	CIP-005-5	R2.	Medium	VSL - Moderate	11/18/2016	6/7/2018	On-site Audit	12/10/2018	7/31/2019

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

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
NPCC2018019847	CIP-007-6	R2.	Medium	VSL - Severe	7/1/2016	7/19/2018	On-site Audit	11/28/2018	7/31/2019

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

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
NPCC2018019846	CIP-007-6	R5.	Medium	VSL - Severe	7/1/2016	9/28/2018	On-site Audit	10/17/2018	7/31/2019

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

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
NPCC2018019845	CIP-010-2	R3.	Medium	VSL - Severe	7/1/2016	6/6/2018	On-site Audit	9/6/2018	7/31/2019

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