NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Internal Controls Related to Identifying, Mitigating, and Preventing Recurrence of Noncompliance

Ed Kichline, Senior Counsel and Director of Enforcement Oversight
Leigh Faugust, CCEP, Enforcement Counsel
February 6, 2018

CIP-007-6 R1

Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)

Hypothetical 1

The Regional Entity (RE) discovered the violation during a Compliance Audit. It determined the registered entity failed to establish and document a process to ensure that logical network accessible ports that have been determined to be needed are enabled. The entity also: a) enabled one or more ports or services not required for normal and emergency operations on its Bulk Electric System (BES) Cyber; b) did not disable one or more other ports or services, including those used for testing purposes, prior to production use for BES Cyber Assets; and c) for cases where unused ports and services could not be disabled due to technical limitations, did not document compensating measure(s) applied to mitigate risk.

This failure increased the likelihood of infiltration of unauthorized network traffic through ports and services that are not necessary for normal or emergency operations, but nevertheless remain enabled. This type of infiltration could cause significant harm to the entity's BES Cyber Assets.

Hypothetical 2

The RE discovered the violation during a Compliance Audit. It determined the entity did not disable any unnecessary ports and services on BES Cyber Assets, relying instead on its firewalls to deny ingress. This type of blocking ports and services did not take into account several malicious attack vectors, such as internal disgruntled workers or false origination data. Additionally, since the firewall rules allowed any traffic to leave the ESP to any destination, those rules did not protect the entity from “man-in-the-middle” attacks. The risk to the entity is that failing to disable unnecessary ports and services on Cyber Assets could lead to operational failure of its Energy Management System. Systems with access into the ESP and which have a lower level of protection than BES Cyber Assets could be compromised through lateral movement in the corporate network and could potentially compromise those assets.

The entity's documentation indicated a proper approach to addressing the requirements of CIP-007-3a R2 for the firewall only and did not address what was behind the firewall (things in the ESP). The entity did provide evidence that it used application white-listing to mitigate the damage of malware. Nevertheless, as the entity uses its firewalls to control BES Cyber Asset ports and services, the impact of the firewall rules is critical. In this case,

there is a specific firewall rule that allows all outbound traffic to communicate from the ESP to other, less secure networks. No actual harm is known to have occurred.

Hypothetical 3

The entity submitted a Self-Report stating it failed to provide proper justification for four services enabled on a network switch device.

The entity had preventive controls in place to prevent the unauthorized access to devices. The entity knew the switch was being used and had user accounts that were specifically configured to connect to that device and its services. The entity's user accounts had strong, complex passwords and the entity monitored the network switch device and its services, even though it was not listed in their baseline. Additionally, the entity had strong compensating controls in place if the affected open ports and services were compromised. For example, it implemented a defense-in-depth architecture of physical and logical Cyber Security controls, including physical security mechanisms, special locks, closed circuit television (CCTV), and logical perimeter and internal cyber security controls. The internal cyber security controls included firewalls, vulnerability scanning tools, and a Security Events Management System (SEM logging). The entity also uses a managed security services provider to monitor the services and provide alerts of signature-based intrusion events and potential anomalous traffic crossing into and out of the established ESP using the security defense appliances and a log collection infrastructure. This monitoring and alerting is provided 24 hours a day, seven days a week. Key trained and experienced personnel are notified via pager, email, and/or telephone of any alerts, as warranted by the severity level assigned to the alert.

PRC-005 R2

Purpose: To document and implement programs for the maintenance of all Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying affecting the reliability of the Bulk Electric System (BES) so that they are kept in working order.

Hypothetical 1

The RE determined during a Compliance Audit that the entity failed to demonstrate that it followed its Protection System maintenance and testing program for the facilities reviewed during the Compliance Audit. In some cases, the RE could not verify that all of the steps listed in the entity’s maintenance and testing program were being completed. In other cases, the entity had no records showing that a number of Protection System devices had ever been maintained and tested. The RE determined the violation was attributable to historical weaknesses in certain key management practices and internal controls related to protection system maintenance and testing.

The RE requested additional information on the entity's protection system management program. The PRC-005 manager initially refused to provide further information on its performance of maintenance, stating that he had already performed an extent of condition review and was willing to attest to its completion and lack of findings. RE enforcement staff escalated the request after not receiving the information, and its chief executive officer called the chief operating officer of the entity. During this conversation, it became apparent that executive leadership at the entity was completely unaware of the follow-up requests. The entity conducted an internal investigation and discovered that its PRC-005 manager had failed to complete maintenance and testing for nearly all of its Protection System communication devices, batteries, and relays since June 18, 2007, and instead had

fabricated review and maintenance documents to cover the failure. The entity had one prior violation of PRC-005 R2.

Hypothetical 2

The entity submitted a Self-Certification stating that it was in violation of PRC-005-1.1b R2. Over the course of a year, the entity performed an extensive review of its PRC program and the PRC instances to identify patterns so that it could implement holistic improvements to prevent recurrence. Through this review, the entity identified multiple instances of noncompliance with PRC-005 R2.

Despite the multiple violations, the PRC instances are not indicative of a systemic issue with the entity's testing and maintenance program. Rather, the PRC instances involved less than one half of one percent (only 0.19 percent) of the entity's total batteries, chargers, and relays in the Regions' footprints and stem from a variety of causes. After its review, the entity attributed the PRC Instances to inadequate configuration management processes. New equipment was not appropriately tracked in the entity's asset management database during the commissioning process, which resulted in testing and maintenance outside of the defined interval.

The entity voluntarily provided the RE with an abundance of information regarding the violation in a manner that was detailed, thorough, and timely, and was open with the RE regarding its violations, processes, systems, and organization. This insight has allowed the RE to better analyze the violation.

Hypothetical 3

The entity submitted a Self-Report stating that it had an issue of PRC-005-1.1b R2. The entity identified several PRC-005 violations related to missed component test intervals at its facilities. Those violations were self-reported to its RE in 2015, and a mitigation plan was later submitted and completed.

Following completion of the 2015 PRC-005 mitigation plan, the entity discovered that it did not clearly document PRC-005 compliance testing of the various devices related to a facility's electrical interconnection. This ambiguity existed for a number of reasons, including: (1) legacy interconnection maintenance practices; (2) lack of clarity and specificity in information related to PRC-005 devices; and (3) personnel turnover. Upon discovery, the entity performed a rigorous review of its entire PRC-005 program with a verification of each applicable component.

The entity personnel did not confirm and document that testing was completed for all applicable relays and the associated communications channel. The entity personnel did not implement a testing schedule upon receiving the proper notification and did not understand which personnel were responsible for completing the testing. The entity discovered the deficiency during an internal review of its relay inventory list and corrected the issue promptly. No harm is known to have occurred.

Although the current noncompliance involves conduct that is similar to previous noncompliance, the current noncompliance involves high-frequency conduct, testing Protection System components, for which the entity has demonstrated an ability to identify, assess, and correct noncompliances. The entity self-identified and reported the issue because of the effective execution of its compliance program and the installation of internal controls that yielded identification of the issues. The entity was proactive in working with the RE once it identified the issue and kept the RE informed as it was conducting its extensive review of its PRC program and the PRC instances to identify patterns in contributing causes. The entity also worked closely with its RE when developing its mitigation strategy.