NEW YORK STATE RELIABILITY COUNCIL
MEETING 212: December 2, 2016
Report for Agenda Item 8.1: Michael Forte
NPCC Board of Directors Report

The upcoming NPCC Board of Directors (BOD) meeting will be held on December 7th. In lieu of a BOD report, the following is a summary of a recent NERC cyber security (CIP) compliance violation which resulted in a penalty of $1,125,000.

NERC CIP Compliance Violation

NERC filed a Notice of Penalty regarding noncompliance by an Unidentified Registered Entity (URE) in the WECC Region. The URE had a total of 19 NERC CIP compliance violations. All of the violations were self-reported by URE.

The root cause of the violations was URE's failure to have a comprehensive change management, configuration, and communication process during the testing and installation phases of new substations. URE failed to verify that NERC CIP Standards had been implemented. Specifically, URE did not perform the steps necessary to ensure that new Critical Assets (the substations) be afforded all the security controls necessitated by NERC CIP Standards.

URE connected substations to the Bulk Electric System (BES) without ensuring those substations were afforded adequate CIP protections prior to being energized. Specifically, URE failed to protect the substations with firewalls, as well as failed to complete its physical access control system configurations. Numerous consequences could follow the failure to ensure CIP protections prior to energizing the substations. For example, there was an increased risk that a malicious individual would enter the substation without authorization and take any number of negative actions. The malicious individual could have modified relay settings to prevent relays from opening upon a detected fault in the line, allowing the fault to continue and potentially damage neighboring substations.

The following are some of the NERC CIP violations:

- URE failed to utilize its process of change control and configuration management for Critical Cyber Assets (CCAs);
- URE did not implement organizational processes for control of electronic access at all Electronic Access Points to the Electronic Security Perimeter (ESP);
- URE failed to perform annual Cyber Vulnerability Assessment (CVA) of the Electronic Access Points to the ESPs;
- URE failed to ensure that Cyber Assets used in the access control and/or monitoring of the ESP resided within an identified Physical Security Perimeter (PSP);
- URE did not implement controls for monitoring physical access at all access points to all PSPs and failed to immediately review unauthorized access attempts; and
- URE did not implement a process to ensure that only those ports and services required for normal and emergency operations were enabled.

WECC determined that these violations collectively posed a serious and substantial risk to the reliability of the BPS.