NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-008-6 Effectiveness Study Summary

Assessment of Cyber Security Incident Reporting and Response
June 27, 2022

Background

Reliability Standard CIP-008-6 became effective on January 1, 2021, in response to FERC Order No. 848 directing NERC to develop modifications to the Reliability Standards to require reporting of Cyber Security Incidents and attempt(s) to compromise a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS). Consistent with the FERC Order, CIP-008 was modified to address concerns that reporting thresholds may have underestimated the realistic scope of BES cyber-related threats.

Since the effective date of the standard, there has not been a material change in the reported number of Reportable Cyber Security Incidents or Cyber Security Incidents that were determined to be an attempt(s) to compromise an applicable system. Accordingly, in Q3 2021, the ERO Enterprise initiated a study to better understand how registered entities have implemented Reliability Standard CIP-008-6 in response to the modifications. Specifically, the study examined how registered entities are interpreting Reportable Cyber Security Incidents and defining attempt(s) to compromise.

Approach

The ERO Enterprise reviewed previous compliance monitoring engagements to analyze ERO Enterprise CMEP data and issued a questionnaire to approximately 30 registered entities through voluntary mechanisms (e.g., entity engagements, webinars, onsite visits, etc.). The questionnaires focused on four key areas: 1) criteria for reporting and key definitions, 2) organizational internal controls, 3) training and tools, and 4) reporting. In addition, the Regional Entities responded to a set of four questions focused on audit observations and the possible need for a CIP-008-6 Compliance Monitoring and Enforcement Program Practice Guide to provide further guidance regarding compliance-monitoring approaches.

Observations and Recommendations

Based on responses provided, most registered entities have processes and internal controls around the detection, review, coordination, and reporting of cyber security incidents. Also, most entities use advanced detection tools, and the staff is sufficiently trained in incident detection and response. However, the current language of the Reliability Standard permits the use of subjective criteria to define attempt(s) to compromise, and most programs include a provision allowing a level of staff discretion.

ERO Enterprise staff recommend submitting a Standard Authorization Request to address gaps permitting a subjective determination of attempt(s) to compromise. The revised Reliability Standard or definition

should provide a minimum expectation for thresholds to support the definition of attempt(s) to compromise. Thresholds should not be so prescriptive as to require the reporting of every internet-facing firewall port scan, phishing email, or file alerted by endpoint anti-virus scans. Rather, the intent would be to right size the reporting threshold to improve awareness of existing and future cyber security threats and potential vulnerabilities that could compromise a responsible entity's ESP or EACMS.

ERO Enterprise staff will continue to use risk-based compliance monitoring and enforcement with the current Standard, while providing additional industry outreach.