NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Security Metrics Working Group Scope

Statement of Need

The industry relies on physical facilities and cyber systems to be in place and operating as designed in order to support the reliable and resilient operation of the bulk power system (BPS). The industry needs a way to measure and trend the effectiveness of the security controls used to secure these facilities and systems. The Security Metrics Working Group (SMWG) will work closely with the E-ISAC to recommend and develop metrics and periodically review, assess, and report the results. The metrics and other information prepared by the SMWG will help inform industry executives and senior managers and provide answers to questions such as:

- How often do physical and cyber security incidents occur?
- To what extent do these reported incidents cause a loss of customer load?
- What is the extent of security information-sharing across the industry?
- Are cyber security vulnerabilities increasing?

Background

The NERC Planning and Operating Committees have promoted the development of performance metrics for the North American bulk power system through the Performance Analysis Subcommittee. The SMWG will contribute to this work by developing a set of metrics that measures the performance of the security controls that support the reliable and resilient operation of the BPS.

- Definition of security from the perspective of BPS reliability:

  The state of actions taken by entities to detect, prevent, and respond to cyber and physical dangers or threats to the reliability or operability of the BPS.

SMWG Objectives/Duties

Provide an advisory role to NERC and its stakeholders regarding physical and cyber security metrics. Develop cyber and physical security metrics that:

- Align with and support the mission and goals of NERC and the E-ISAC.
- Help BPS operators understand the significance of evolving cyber and physical security risks that could affect the reliable operation of the BPS.
- Provide consistent metrics definitions, data collection, and reporting mechanisms.
- Measure the historic performance of security controls that support the reliable and resilient operation of the BPS.
- Provide leading indicators of incidents or events (e.g., technology, configuration, human factors) that could compromise the effectiveness of the security controls that support the reliable, resilient operation of the BPS.

- Contribute to an overall assessment of BPS reliability consistent with the Adequate Level of Reliability (ALR) framework.

Note: The SMWG will not develop metrics specific to the operational performance of the E-ISAC or individual entities.

Members and Structure

The SMWG will generally follow the organizational structure and voting rights of the Critical Infrastructure Protection Committee (CIPC) with the following addition:

- Non-voting members who are industry subject matter experts, for the work at hand.
- A NERC staff member will be assigned as the non-voting SMWG Coordinator.
- The SMWG chair and vice chair will be appointed by the CIPC EC for one two-year term.

Reporting

The SMWG will work closely with the E-ISAC to define, develop, and review security metrics. The E-ISAC will manage the data collection and quarterly reporting process. The SMWG will administratively report to the CIPC.

SMWG Deliverables and Work Schedule

- Four to six meetings per year. Emphasis will be given to conference calls and web-based meetings.
- To be completed in consultation with EC Sponsor.