NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Working Group Scope

Purpose

The 2019 ERO Reliability Risk Priorities Report highlighted "Grid Transformation" (Increased Complexity in Protection and Control Systems), "Security Risks" (Physical and Cyber Security Threats), and "Critical Infrastructure Dependencies" (Communications) as three high level risk categories for the ERO Enterprise and electric industry. At the same time, the operational and technological environment of the electrical grid is undergoing rapid transformation. The Security Working Group (SWG) serves the Reliability and Security Technical Committee (RSTC) in providing a formal input process to enhance collaboration between the ERO and industry with an ongoing working group. The SWG also supports industry efforts to mitigate emergent risks by providing technical expertise and feedback to the ERO Enterprise Compliance Assurance group in developing and enhancing security compliance-related products, including guidelines, guidance, best practices and lessons learned.

SWG Objectives/Duties

RSTC oversees the SWG. The SWG will develop a portfolio of technical expertise from industry and other willing participants who will conduct the following activities:

- Develop a process for handling requests from ERO Enterprise compliance assurance staff
- Provide feedback from industry to the ERO Enterprise to improve the Compliance Monitoring and Enforcement Program (CMEP), including a process to deliver that feedback
- Provide guidance to the RSTC on prioritization of compliance assurance products under development
- Provide guidance and feedback for CMEP materials brought before the RSTC for discussion
- Provide timely technical reports to RSTC on CMEP matters related to cyber and physical security
- Attend the RSTC face-to-face meetings to facilitate discussion and allow discourse on CMEP topic areas
- Promote registered entity involvement in the NERC Reliability Standards review and comment process
- Develop materials from organized industry activities (such as tabletop exercises) led by or in collaboration with the SWG
- Review lessons learned published by NERC where the RSTC seeks additional industry feedback to help determine whether additional guidance to industry is necessary
- Coordinate with other industry technical groups
- Collaborate with other NERC stakeholder groups within the RSTC to eliminate potential overlaps, avoid duplicative efforts, and ensure alignment of assignments and responsibilities by coordinating and leveraging expertise across groups to the best extent possible. This includes:

- Coordination with the NERC Security Integration and Technology Enablement Subcommittee (SITES) regarding compliance products being developed and other issues that should inform their discussions about security matters.
- Coordination with other NERC technical groups focused on security and compliance issues to provide useful perspectives on security-related issues that may affect them.

Members, Structure, and Roles and Responsibilities

The SWG will include members with expertise in the following areas:

- Technology design, architecture and engineering in Operational Technology (OT) computing applications, software and hardware platforms, network, carrier and telecom experience at entity data center, OT and industrial control systems (ICS) at transmission and generation control centers, substation and operating station facilities and generation plant and energy centers.
- Design, implementation, and operation of security infrastructure and controls (both physical and cyber) for systems and networks in bulk power system (BPS) control centers, transmission systems, generation facilities, systems critical to BPS restoration, special protection systems, and other systems impacting users, owners, and operators of the BPS
- State-of-the-Art and emerging technologies (e.g., software-as-a-service (SaaS), cloud computing) and how these innovative technologies can be effectively leveraged to improve physical and cyber security, as well as their relationship to compliance with NERC's Reliability Standards.
- Physical and cyber security threat vectors and risks posed by changing technologies for owners, operators, and end-users of the BPS.
- Relevant information security standards and NERC Reliability Standards.
- NERC CMEP and responsible entity compliance programs and processes.
- Various physical and cyber security frameworks, including National Institute of Standards and Technology (NIST), ISO 27001, and others.
- Process development with technical writing and program development.

The SWG will consist of two co-chairs with a two-year term, nominated by the SWG and approved by the RSTC leadership. The co-chairs terms may be extended or be reappointed, as necessary. The SWG sub-team leads may be reappointed, as necessary. NERC staff will be assigned as coordinator (secretary).

Decisions made by the membership will be consensus-based, led by either co-chair. Any minority views will be documented, as necessary. The RSTC will assign a sponsor to advocate on behalf of the SWG and to coordinate with RSTC and its other sub-groups.

Members are those participants who actively participate on SWG initiatives and require "collaborator" access to the SWG extranet site. Observers are those participants who do not need to collaborate on active projects yet desire to remain aware of SWG activities. Members and observers are documented on the mailing lists maintained by NERC.

The RACI (Responsible, Accountable, Consulted, and Informed)[1] chart in **Appendix A: Roles and Responsibilities** shows the main roles and responsibilities for the SWG.

Reporting and Duration

The SWG will report to the NERC RSTC. The duration of the SWG is expected to be indefinite so long as the group is deemed beneficial by the RSTC and effectively accomplishing its purpose.

SWG Deliverables and Work Plan

The SWG will develop a work plan that will be submitted to the RSTC. Work products that support industry efforts relating to leveraging emerging technologies and security enhancements into conventional planning, operations, and design practices will address one or more of the following areas:

- Technical reference documents, technical reports, white papers, best practices, and tools
- Reliability guidelines and security guidelines as assigned by the RSTC or through periodic review
- Compliance implementation guidance
- Lessons Learned
- Standard Authorization Requests (SAR)
- Supporting materials and expertise to other NERC working groups / subcommittees

The SWG work plan will be maintained throughout the group's existence and will be documented in the RSTC Strategic Plan and updated as needed by the RSTC.

Meetings

The SWG conducts a minimum of four meetings per year and strives to conduct monthly meetings. Emphasis will be given to conference calls and web-based meetings prior to the RSTC quarterly meetings. If face-to-face meetings are required, every effort will be made to meet at the same location as the RSTC quarterly meeting.

The SWG co-chairs or their designee provides a report at each RSTC quarterly meeting as needed. The SWG has a process for handling RSTC requests in consultation with the RSTC sponsor and NERC staff coordinator. Sub-team meetings are conducted by the sub-team leads on a frequency determined by the sub-teams that are appropriate to the project and workload. Sub-team updates are given at the periodic SWG meetings.

[1] https://www.softwareadvice.com/resources/what-is-a-raci-chart/

Appendix A: Roles and Responsibilities

Table A.1: SWG RACI (Responsible, Accountable, Consulted, Informed)								
Description	**RSTC Sponsor**	**SWG Co-Chairs**	**Sub-Team Lead**	**Sub-Team Member**	**NERC Staff (Secretary / Coordinator)**	**NERC Staff (Support)**	**SWG Member**	**SWG Observer**
Organize monthly/quarterly SWG Meetings	I	R, A	I	I	C	I	C	I
Organize Sub-team meetings	I	A	R, A	C	C	I	I	I
Coordinate Sub-team activities, ensure completion of Sub-team tasks	I	I	A	R	I	I	I	I
Administrative review of products completed	C	A	R	C	C	I	I	I
Drive RSTC review/acceptance process	C	R, A	C	C	C	I	I	I
Perform sub-team tasks	N/A	I	A	R	I	I	I	I
Coordinate with other working groups	I	R, A	C	C	I	I	I	I
Meet with SWG chair/co-chair for status, problem-solving	C	C	R, A	C	I	I	N/A	N/A
POC for SWG for industry groups	C	R, A	C	I	I	I	I	I
Problem-solve for delivery dates	I	C	R, A	R	C	I	I	I
Maintain extranet site	I	R, A	R, A	R	I	I	I	I
Send out and collect calls for volunteers	I	R, A	C	C	C	C	I	I
Drive continuous improvement for SWG processes	C	R, A	R	C	C	C	C	I
Endorse SWG products	C	R, A	C	I	C	I	I	I
Provide SWG Scope Guidance	A	R	C	C	I	I	I	I
Provide daily guidance to sub-teams	N/A	A	R	C	I	I	I	I
Extranet design changes, tools	I	R, A	C	C	I	I	I	I
Manage project input process	C	R, A	C	C	I	I	I	I
Maintain and monitor work processes	I	A	R	C	C	I	I	I
Approve SWG Work Plan	C	A	R	C	C	I	I	I
Manage mailing lists and overall SharePoint environment (extranet)	N/A	A	C	C	C	R	I	I

Appendix B: Version History

Table B.1: SWG Scope Version History			
Date	**Page**	**Description**	**Version**
2/3/2021	All	Draft SWG Scope Approved by the Security Working Group	0.1
3/2/2021	All	SWG Scope approved by the Reliability and Security Technical Committee	1.0
1/31/2024	All	Reviewed by SWG leadership; co-chair changes from vice chair verbiage; RACI review.	1.1
3/15/2024	All	Revisions approved by the Reliability and Security Technical Committee	2.0