NATIONAL SUPPLY CHAIN INTEGRITY MONTH - *CALL TO ACTION*

# BEST PRACTICES

## Obtain Executive Level Commitment for a Supply Chain Risk Management (SCRM) Program

**Build an Integrated Enterprise Team.** A successful SCRM program requires commitment from senior stakeholders from across the enterprise including Security, Information Assurance, Insider Threat, Legal, and Acquisition.

**Communicate across the Organization.** Horizontal and vertical communication is essential to ensure senior stakeholders' investment in the success of a SCRM program. This includes information sharing to inform risk decisions and implement mitigations.

**Establish Training and Awareness Programs.** Organization-wide awareness and training further embeds the SCRM practices with senior stakeholders and empowers employees to manage, mitigate, and respond to supply chain risks.

## Identify Critical Systems, Networks, and Information

**Exercise Asset Management.** Real-time knowledge of the location and operational status of all assets is essential to understanding what systems, networks, and information are critical to the enterprise.

**Prioritize Critical Systems, Networks, and Information.** Identifying critical systems, networks, and information enables stakeholders to prioritize resources for protecting these systems and mitigating supply chain risks.

**Employ Mitigation Tools.** Continuous monitoring of system data and network performance enables rapid implementation of appropriate countermeasures to minimize the impact of an attempted disruption or attack.

## Manage Third Party Risk

**Conduct Due Diligence.** Assess first-tier suppliers regularly to increase visibility into third-party suppliers and service providers. Leverage this data to properly vet vendors who are providing key components to critical systems and networks.

**Incorporate SCRM Requirements into Contracts.** Use SCRM-related security requirements as a primary metric – just like cost, schedule, and performance - for measuring a suppliers' compliance with the contract. These security requirements include personnel security and system and services acquisition, and are fully described in NIST SP 800-161.

**Monitor Compliance.** Monitor suppliers' compliance to SCRM-related security requirements throughout the supply chain lifecycle, even when terminating supplier relationships.