Cyber Supply Chain Risk Management: Program Briefing

National Risk Management Center
Cybersecurity and Infrastructure Security Agency

SSCA 2018 Winter Forum
December 19, 2018

Emile Monette
Emile.Monette@hq.dhs.gov

Mission and Scope

Mission

Facilitate national efforts to address risks to the global information and communications technology supply chain

1. Secure the supply chain for the Department's ICT enterprise
2. Assist all Federal D/As, SLTT, and critical infrastructure with securing supply chains for their ICT enterprises

The C-SCRM Program is CISA's cyber supply chain activity:

- Develops and deploys supply chain risk management capabilities
- Coordinates and participates in stakeholder efforts to prioritize, develop, and implement programs and projects to address risks in the global information and communications technology (ICT) supply chain.

Scope

Comprehensive approach to identification, assessment, mitigation, and management of risks to ICT supply chains

- All-hazards
  - Cyber and traditional supply chain security
  - People, processes, and technology
  - Natural and man-made
  - Intentional and unintentional
- Increase transparency and accountability
  - Use of standards and best practices
  - Changes to acquisition strategy and practice
  - Coordinate and share intra- and inter-government actions and knowledge

Context

Background

The Cybersecurity and Infrastructure Security Agency (CISA) Cyber Supply Chain Risk Management (C-SCRM) Program was conceived as part of CISA's implementation of government-wide information security policies and practices and coordination of the overall Federal effort to enhance the security and resilience of our Nation's Critical Infrastructure.

The C-SCRM Program is a functional component of the National Risk Management Center (NRMC), and the NRMC established the C-SCRM Program Management Office (PMO) to serve as the lead organization and central coordination point for all CISA supply chain risk management activities.

Definition

C-SCRM is: *The process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of ICT (including IoT) products and service supply chains.*

- C-SCRM covers the entire lifecycle of ICT (including design, development, distribution, deployment, acquisition, sustainment, and destruction)
- Encompasses hardware, software, and information assurance, along with traditional supply chain management and supply chain security practices.

Lines of Effort (planned)

Supply Chain Fusion Center

Supply Chain Assessment Service

- Address multiple tiers of a supply chain (manufacturer, sub-contractor, sub-sub-contractor, etc.)
- Assess threats using open source information infused with intelligence
- Recommend mitigations based on threats identified

Supply Chain Threat and Mitigation Information Sharing

- Centralized information repository
- Enables re-use of information and strategic analysis of supply chain threats

Qualified Bidder and Manufacturer Lists

- Establishing and managing approved product and service provider lists, tailored for specific use cases

Public-Private Partnership

ICT SCRM Task Force

- Platform for strategic relationship management with private sector
- Primary forum for DHS and private sector to engage on ICT supply chain risk
    - Information Sharing between government and private sector
    - Provide consistent method for supply chain threat assessment
    - Develop criteria for first Approved Products List
    - Inventory SCRM initiatives and identify gaps
    - OEM and Authorized Reseller Purchasing

Software and Supply Chain Assurance Forum

- Co-sponsor with DoD, GSA, NIST

Capacity Building

Organizational Capability Assessment

- Assisting stakeholders with strategic and operational assessment and planning of C-SCRM capabilities
    - Facilitated process bridges the traditional silos of Logistics, Operations, Cybersecurity, and Acquisition
    - Assesses and documents current capability
    - Provides guidance on steps to improve

Training, Education, and Guidance

- Provide buyers guides, training courses, and implementation tools to assist with improving supply chain risk management capabilities
    - Cybersecurity in Acquisition course
    - Supply Chain Risk Management Awareness course
    - IoT Procurement Guide