ICT SCRM

JOINT INDUSTRY OUTREACH SEMINAR ON STRATEGIC TRADE MANAGEMENT 2021

Dan Dagher
September 28, 2021

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

National Risk Management Center

The National Risk Management Center (NRMC) is a planning, analysis, and collaboration center. CISA coordinates with the critical infrastructure community to identify; analyze; prioritize; and manage risks to National Critical Functions, which are vital to the United States.

MISSION PRIORITIES:

- Analyzes most strategic risks to our Nation's critical infrastructure
- Leads public/private partnership initiatives to manage priority areas of national risk
- Collaborates with the private sector and other stakeholders to better understand future threats.

ICT SCRM Risk Categories

ICT is integral for the daily operations and functionality of U.S. critical infrastructure. Due to the global distribution and interconnected nature of ICT, vulnerabilities to the ICT Supply Chain could have cascading impacts across multiple critical infrastructure sectors.

Risk Categories

Counterfeit Parts

External Attacks on Operations and Capabilities

System Development Life Cycle (SDLC) Processes and Tools

Inherited Risk (Extended Supplier Chain)

Legal Risks

Internal Security Operations and Controls

Economic Risks

External End-to-End Supply Chain Risks (e.g., Natural Disasters, Geo-Political Issues)

Insider Threats

ICT SCRM Resources

Below are a few of the informational products CISA has developed to raise awareness of supply chain vulnerabilities. For a complete list of resources, please visit: www.cisa.gov/supply-chain.

SCRM Essentials
A guide for leaders and staff with actionable steps on how to start implementing organizational SCRM practices to improve their overall security resilience.

Threat Scenarios Report v3
Identifies the processes and criteria for threat-based evaluation of ICT suppliers, products, and services.

Preliminary Considerations of Paths to Enable Improved Multi-Directional Sharing of Supply Chain Risk Information
Offers subject matter expert research on legal and policy considerations for giving liability protection to the federal government and private sector in order to promote information sharing.

Vendor SCRM Template
Provides organizations with a set of questions to help enhance clarity for reporting and vetting processes when purchasing ICT hardware, software, and services.

Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacture Lists
Provides organizations a list of criteria and factors that can be used to inform an organization's decision to build or rely on a qualified list for the acquisition of information and communications technology (ICT) products and services.

Dan Dagher
ICT Supply Chain Risk Management
National Risk Management Center
DHS/CISA

For more information:
cisa.gov/supply-chain

Questions?
ict_scrm_taskforce@hq.dhs.gov