Counterintelligence Webinar Series:

Supply Chain: Past, Present, and Future: 2022

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

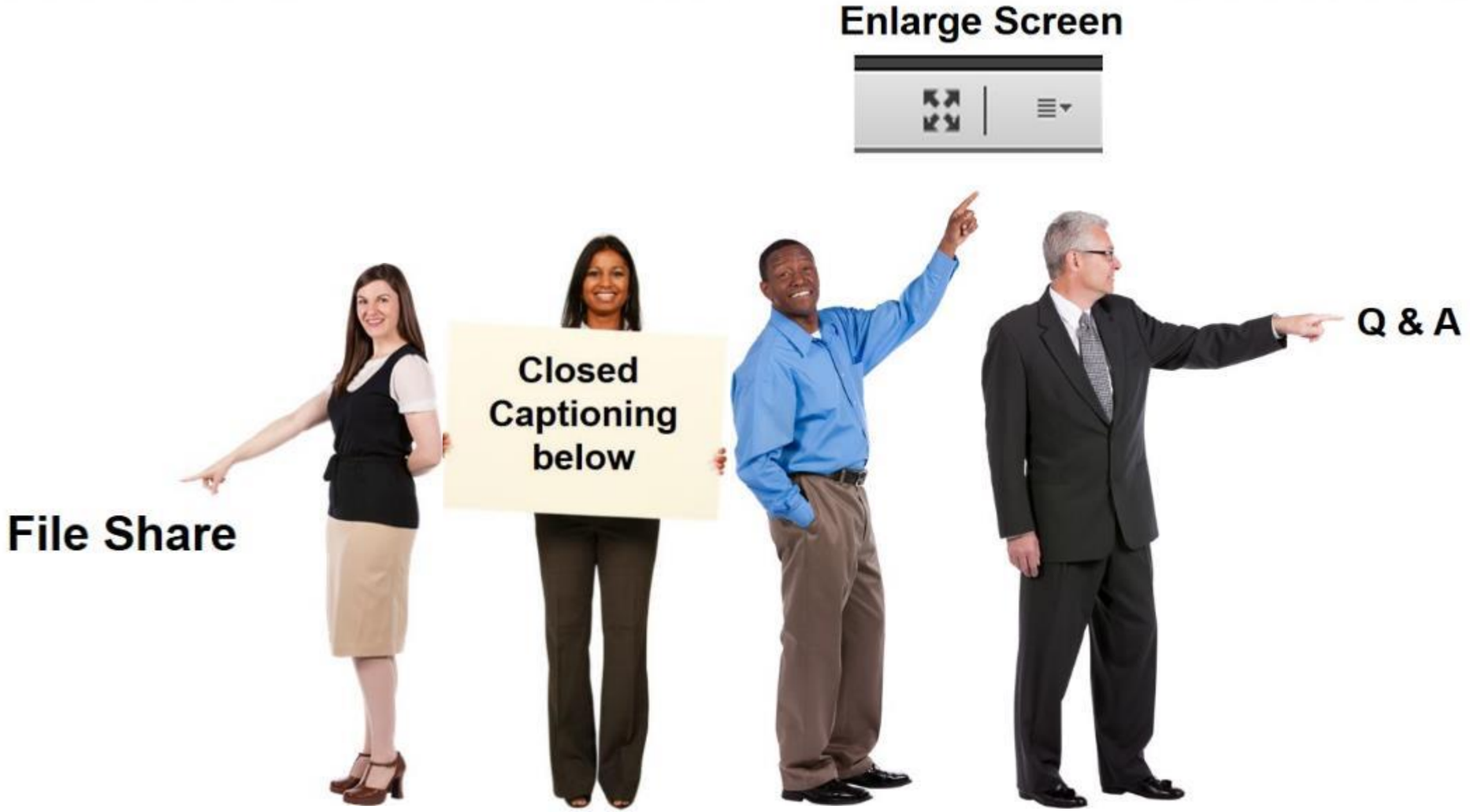
TODAY'S SESSION

Hosts:

- Ed Kobeski, CDSE Counterintelligence (CI)

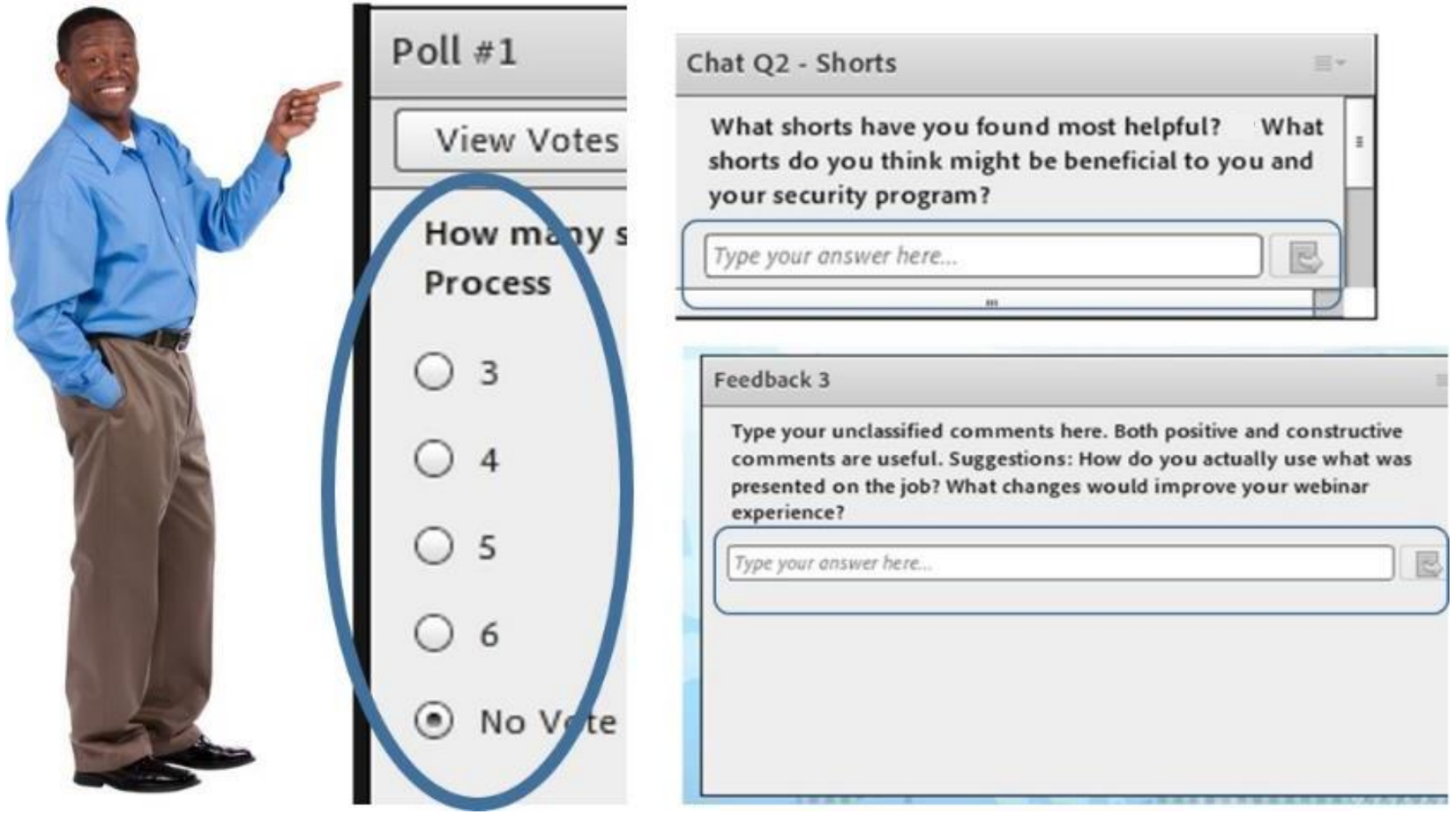
- Supervisory Special Agent (SSA) Matthew Halvorsen, FBI, Joint Duty Assignment to the National Counterintelligence and Security Center (NCSC)

ATTENDEE PARTICIPATION & FEEDBACK



ATTENDEE PARTICIPATION & FEEDBACK

Polls, Chats, and Feedback



POST EVENT FEEDBACK

At the end of our event, please take a few minutes to share your opinions.

Your feedback helps us improve the quality of our offerings.

Responding will only take a few minutes.

Responding is optional.

AUDIENCE POLL QUESTION #1

What is Supply Chain?

A. Product Inventory Counts

B. A connected system moving products and services closer to the end user

C. An over-used excuse for shortages at the grocery store

D. A Fleetwood Mac song?

AUDIENCE POLL QUESTION #2

What is the theme for this year's National Counterintelligence and Security Center (NCSC) Supply Chain Integrity Month?

A. A Call To Action!

B. Stop Stranding Boats in Critical Waterways

C. Fortify the Chain

D. Supply Chain II: Electric Boogaloo

FORTIFY THE CHAIN

Supply Chain & Cyber Directorate

SSA Matthew Halvorsen, FBI
Joint Duty Assignment to NCSC
Strategic Program Manager
Supply Chain & Cyber Directorate

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER (NCSC)

- **NCSC Mission:** Lead and support the U.S. Government's counterintelligence (CI) and security activities critical to protecting our Nation; provide CI outreach to U.S. private sector entities at risk of foreign intelligence penetration; and issue public warnings regarding intelligence threats to the U.S.
- Foreign intelligence entities, which may include foreign governments, corporations, and their proxies, are actively targeting information, assets, and technologies that are vital to both U.S. national security and our global competitiveness.
- Increasingly, U.S. companies are in the cross-hairs of these foreign intelligence entities, which are breaching private computer networks, pilfering American business secrets and innovation, and carrying out other illicit activities.

NATIONAL COUNTERINTELLIGENCE STRATEGY

National Counterintelligence
Strategy
of the United States of America
2020-2022

Executive Summary

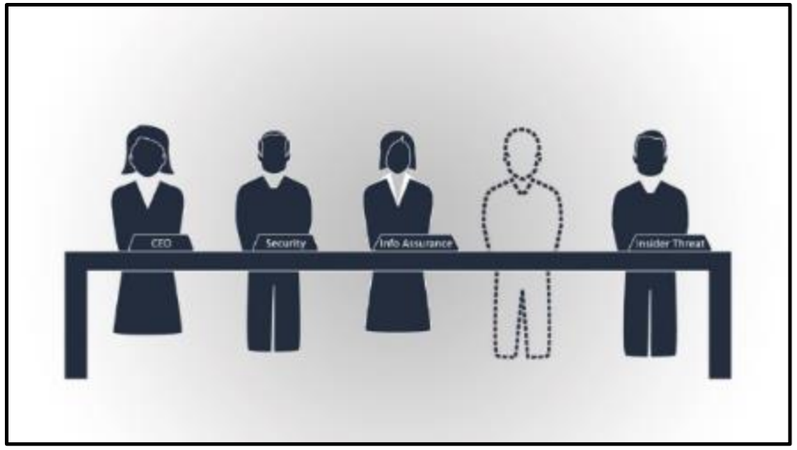
NATIONAL COUNTERINTELLIGENCE STRATEGY

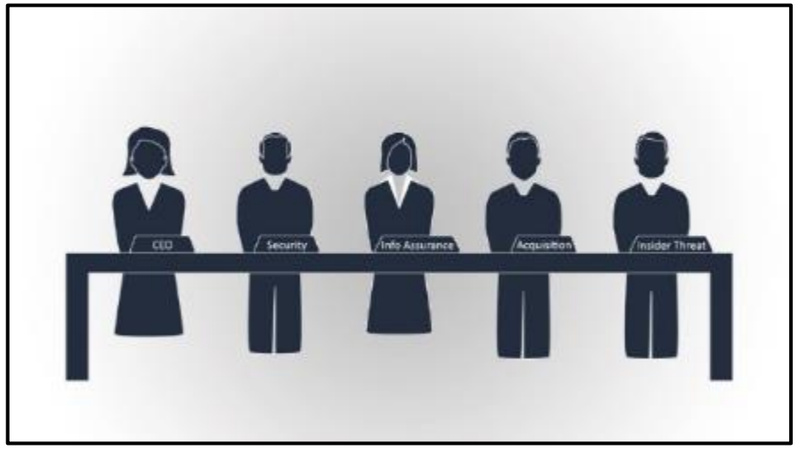
To meet the Strategic Supply Chain Objective, the U.S. Government will:

- Enhance capabilities to detect and respond to supply chain threats.
- Advance supply chain integrity and security across the Federal Government.
- Expand outreach on supply chain threats, risk management, and best practices.

SUPPLY CHAIN RISK MANAGEMENT (SCRM)

- The management of risk to the integrity, trustworthiness, and authenticity of products and services.
- Addresses foreign intelligence entity (FIE) activity compromising the supply chain, including the introduction of counterfeit parts or malicious code.
- Encompasses many disciplines and requires participation from subject matter experts.
- Type of supply chain attack





SUPPLY CHAIN RISK MANAGEMENT (SCRM)

- A supply chain is an interconnected web of people, processes, technology, information, and resources that delivers a product or service.
- One key supply chain is the information and communications technology (ICT) supply chain; it supplies the hardware, software, firmware, networks, systems, and services that underpin the U.S. Government and the private industry.

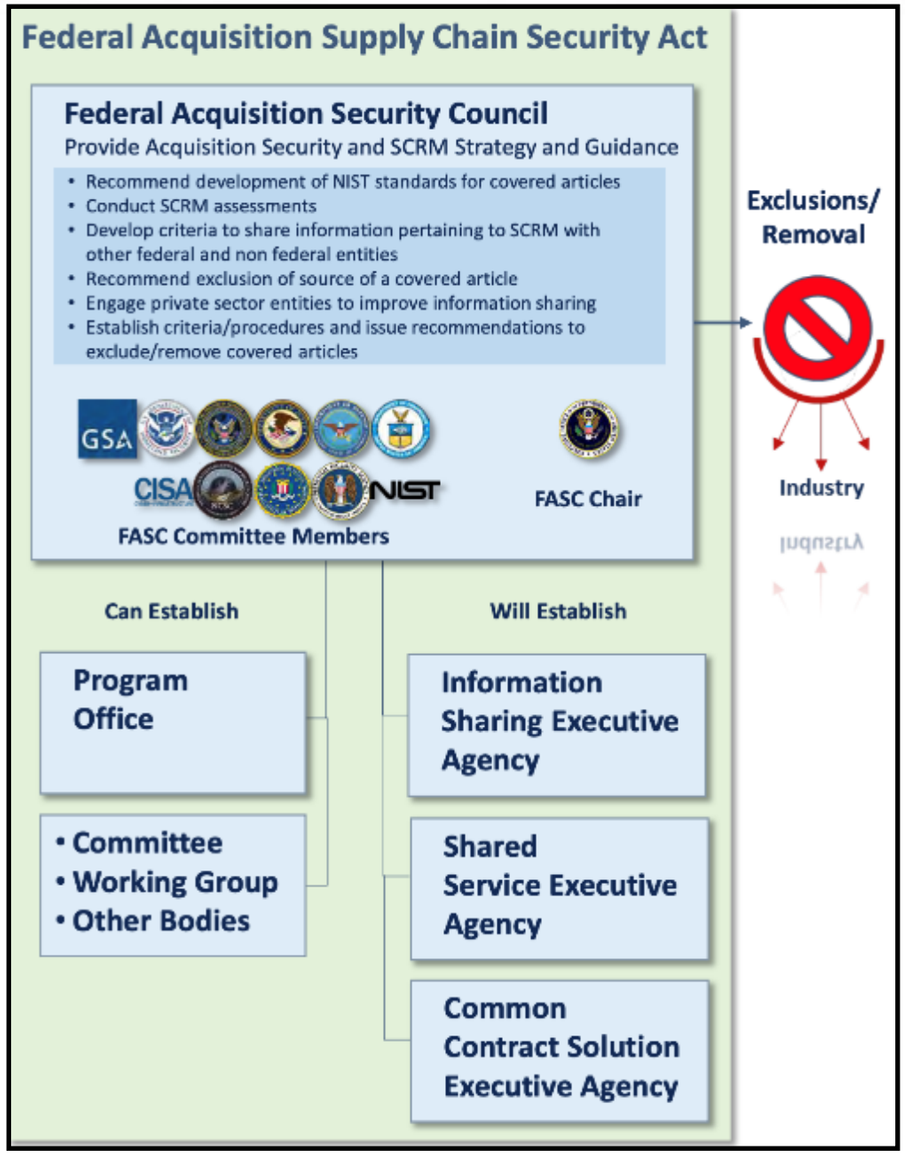
E.O. 14107- AMERICA'S SUPPLY CHAINS

- The goal of EO 14017 was to determine supply chain risks to six critical US industrial sectors. Each one year report identified threats, vulnerabilities, and consequences to the:
  - DOD Industrial Base (DOD)
  - Energy Industrial Base (DOE)
  - Transportation Industrial Base (DOT)
  - Agricultural Food Supply Chain (Dept. of Agriculture)
  - Public Health Industrial Base (HHS)
  - Information Communications Technology Industrial Base (DHS and Commerce)

E.O. 14107- CI & SECURITY RISKS FOR EACH SECTOR

Fortifying SCRM Programs will *Reduce Risks to and Build Resilience in these Critical Sectors.*

SCRM PROGRAMS



Supply Chain Risk Management – Authorities, Policies, and Standards

- Executive Order 13806 report (PDF)
- Executive Order 14017 – America's Supply Chains (PDF)
- SECURE Technology Act: Establishment of the Federal Acquisition Security Council
  - Federal Acquisition Security Council overview (PDF)
  - Federal Acquisition Supply Chain Security Act graphic (PDF)
  - H.R.7327 SECURE Technology Act (PDF)
  - (New) FASC Final Rule (PDF)
- NIST Special Publication 800-161 (PDF)
- ICD 731, Supply chain Risk Management for the Intelligence Community (PDF)

Tools

- User Manual: The Outsourcing Network Services Assessment Tool (ONSAT) (PDF)
- (New) ONSAT Tool

National Supply Chain Integrity Month – A Call to Action

- Press Release: National Supply Chain Integrity Month – A Call to Action
- Software Supply Chain Attacks – 2021
- Supply Chain Risk Management: Best Practices in One Page – 2021
- Framework for Assessing Risks - 2021

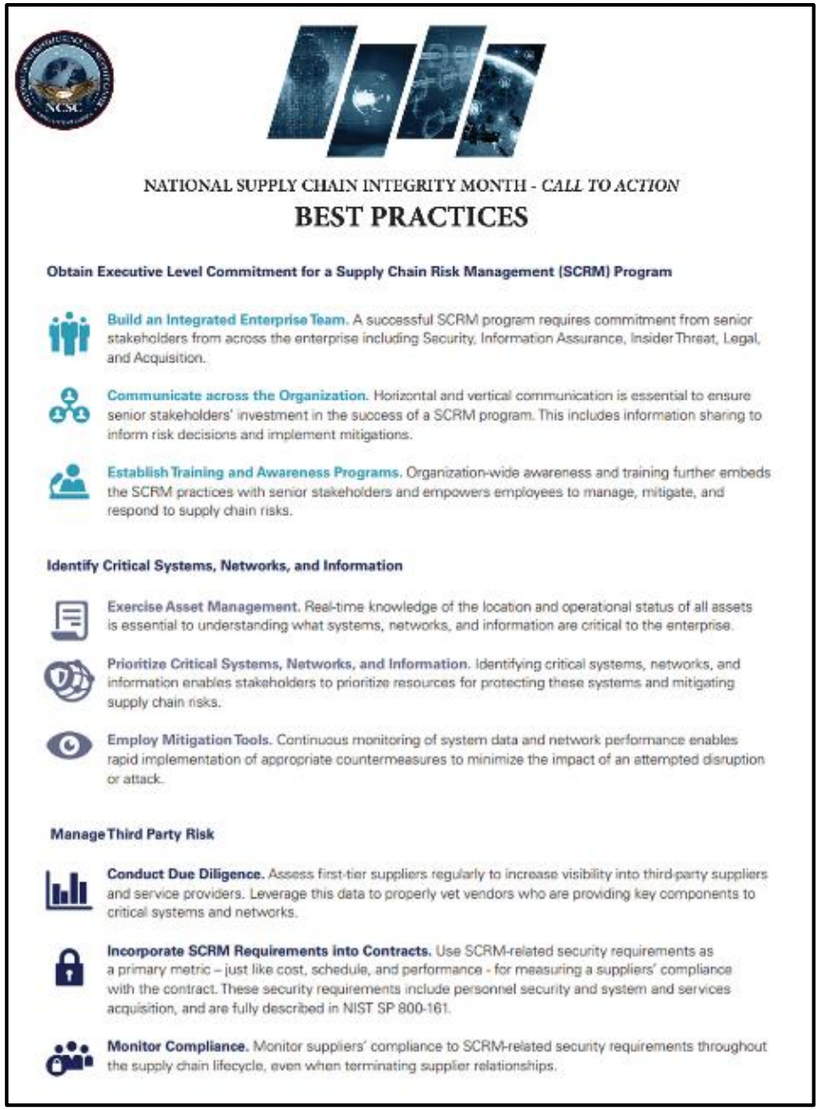
Supply Chain Risk Management: Reducing Threats to Key U.S. Supply Chains

- NTIA Releases Minimum Elements for a Software Bill of Materials
- NCSC Supply Chain Risk Management Tri-Fold: Reducing Threats to Key U.S. Supply Chains (PDF)

Sector-Specific Supply Chain Best Practices

- Information and Communications Technology Sector
- Manufacturing and Production Sector
- Health Care Sector
- Energy Sector
- Ongoing Cyber Threats to U.S. Water and Wastewater Systems Joint Cybersecurity Advisory (PDF)

NCSC SCRM GUIDANCE PRODUCTS



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.

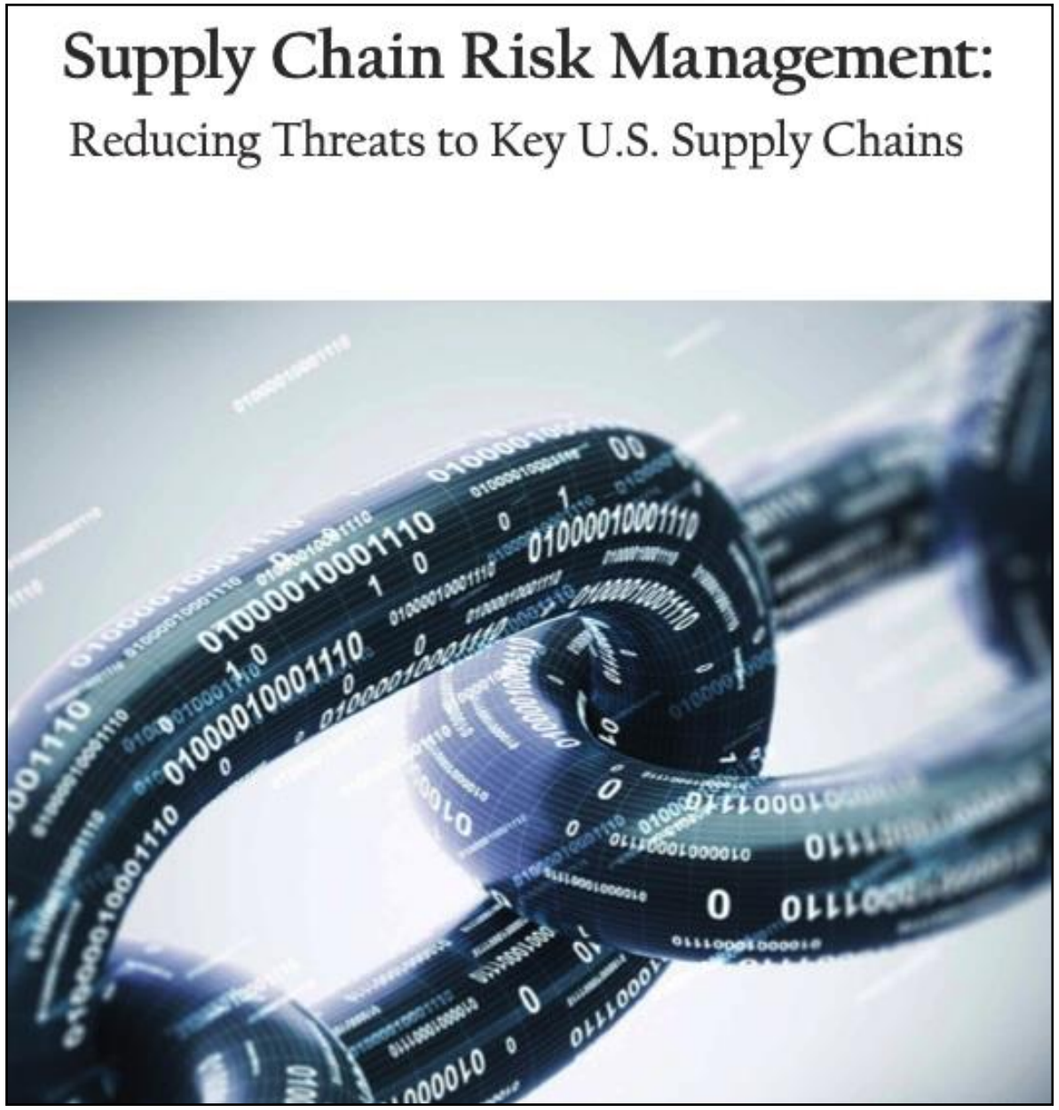
Employ Mitigation Tools. Continuous monitoring of system data and network performance enables rapid implementation of appropriate countermeasures to minimize the impact of an attempted disruption or attack.

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.



QUESTIONS AND CONCERNS

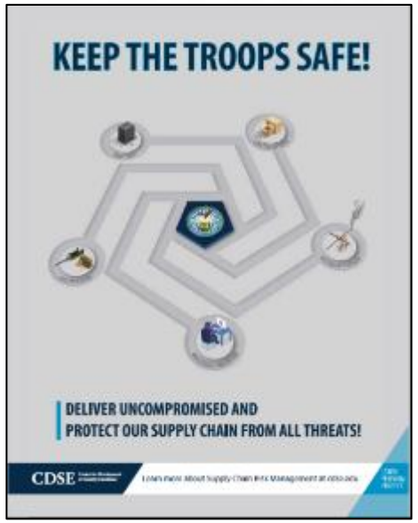
For more information on NCSC and Supply Chain, visit:

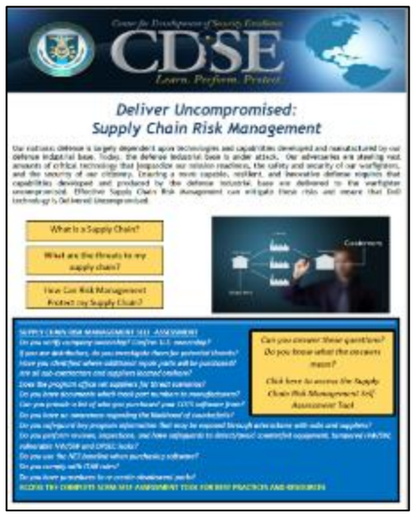
www.ncsc.gov

ncsc-supplychain@dni.gov

SSA Matthew Halvorsen, FBI
NCSC/SCD
301.243.0123 (o)
202.439.6351 (m)
Mjhalvorsen@fbi.gov

RESOURCES





[eLearn: DOD Supply Chain Fundamentals]

[eLearn: Contracting for the Rest of Us]

[eLearn: Thwarting the Enemy: Providing Counterintelligence & Threat Awareness to the Defense Industrial Base]

[eLearn: Supply Chain Risk Management for Information and Communications Technology]

[eLearn: Introduction to Risk Management]

[Job Aid: Supply Chain Risk Management]

[Job Aid: Software Supply Chain Attacks]

[Job Aid: Baker's Dozen: 13 Elements of an Effective SCRM Program]

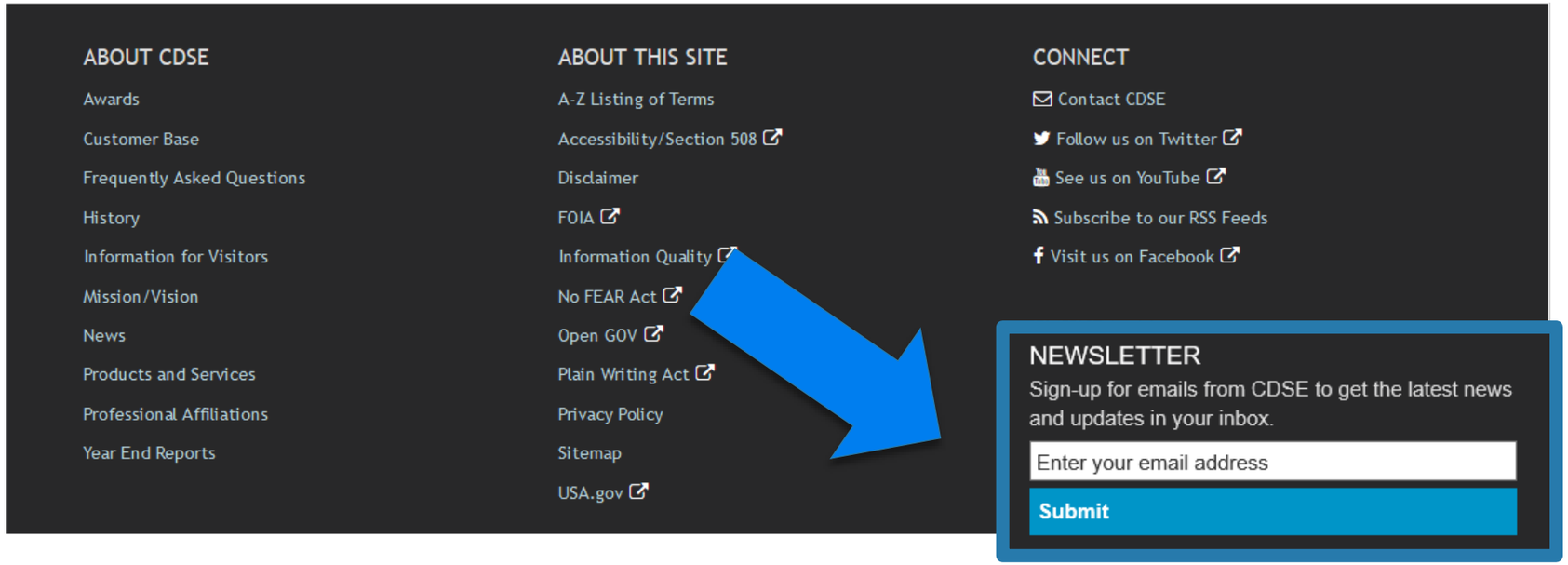
[Job Aid: Framework for Assessing Risks]

[Director of National Intelligence Supply Chain Toolkit]

VIEW MORE MATERIALS HERE:
https://www.cdse.edu/Training/Toolkits/Counterintelligence-Awareness-Toolkit/

SUBSCRIPTION SERVICE

Sign up to get the latest CDSE news and updates delivered straight to your inbox!



https://www.cdse.edu/news/index.html

SOCIAL MEDIA

Make sure to check out our social media accounts!

CDSE – Center for Development of Security Excellence

Like our page on Facebook!

@TheCDSE

Follow us on Twitter!

Center for Development of Security Excellence

Subscribe to our channel on YouTube!

UPCOMING CDSE WEBINARS

Date	Title
April 28	Microelectronics and Supply Chain 2022

For more information and to register for these webinars, visit https://www.cdse.edu/catalog/webinars/index.html

CDSE WANTS TO HEAR FROM YOU!

CDSE Counterintelligence Awareness
Ed Kobeski
edwin.f.kobeski.civ@mail.mil