Counterintelligence Webinar Series:

Supply Chain Due Diligence

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

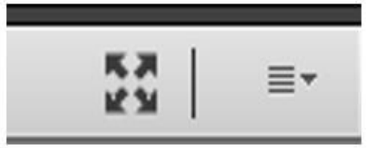
TODAY’S SESSION

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

Enlarge Screen



File Share

Closed Captioning below

Q & A

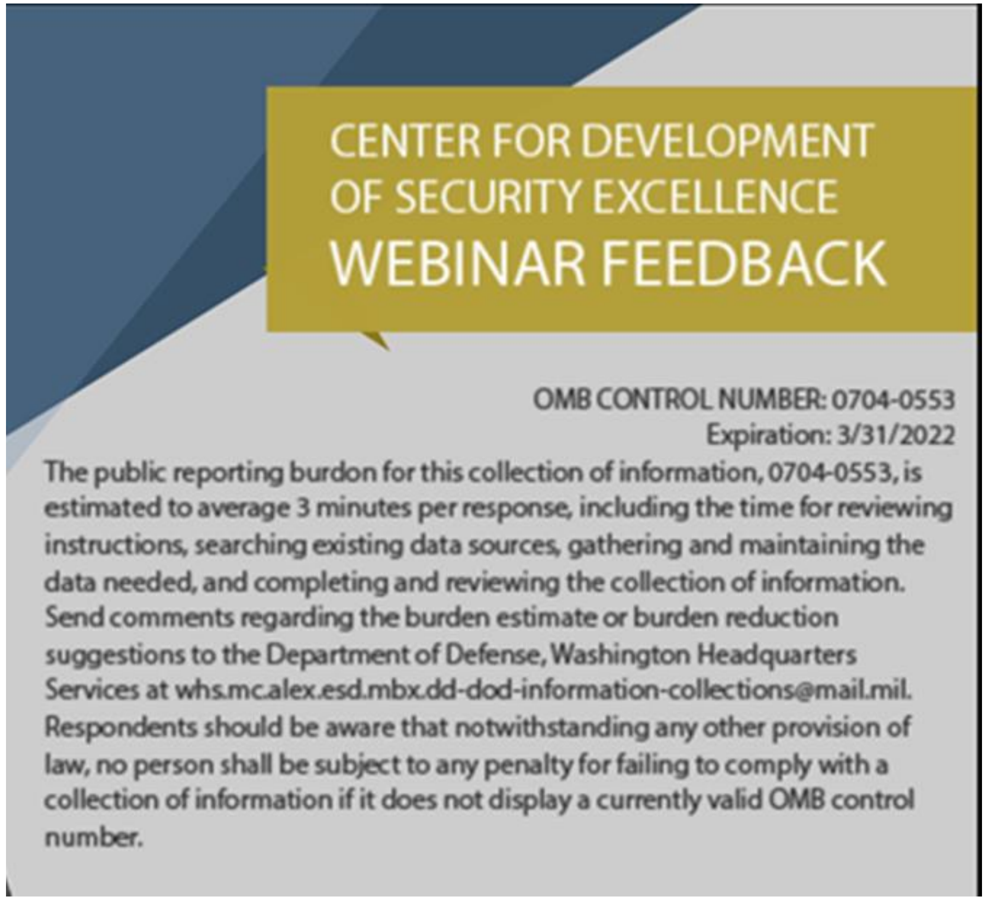
POST EVENT FEEDBACK

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.



CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

WEBINAR FEEDBACK

OMB CONTROL NUMBER: 0704-0553
Expiration: 3/31/2022

The public reporting burdon for this collection of information, 0704-0553, is estimated to average 3 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services at whs.mc.alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

Supply Chain & Cyber Directorate

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

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
NCSC
UNITED STATES OF AMERICA

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.

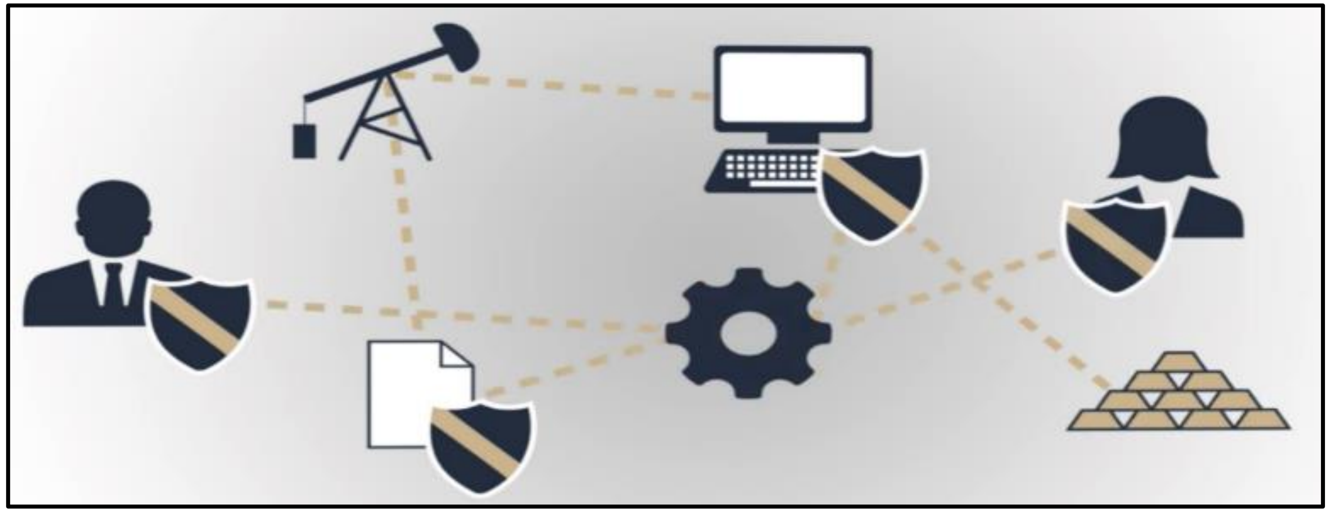
National Counterintelligence Strategy

of the United States of America
2020-2022

Executive Summary

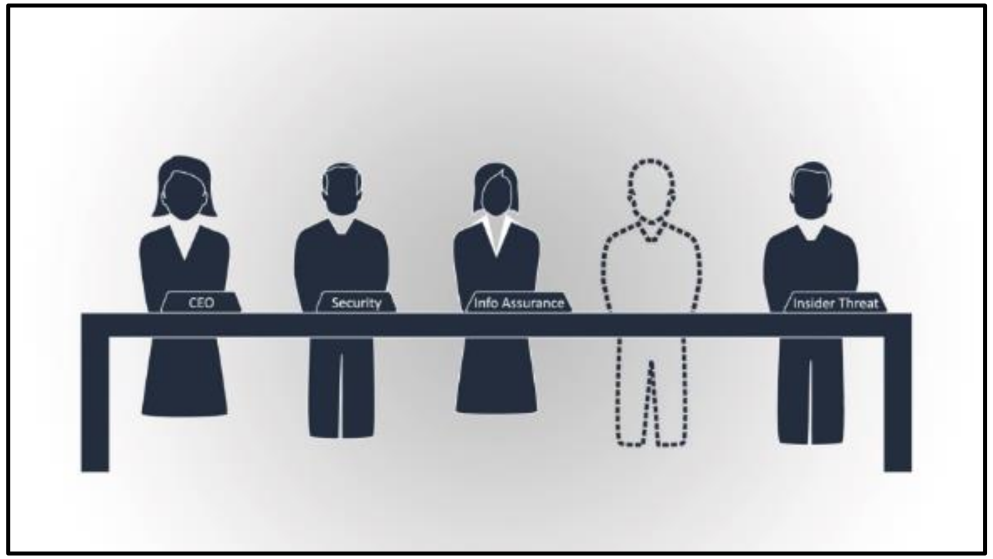
Strategic Objectives

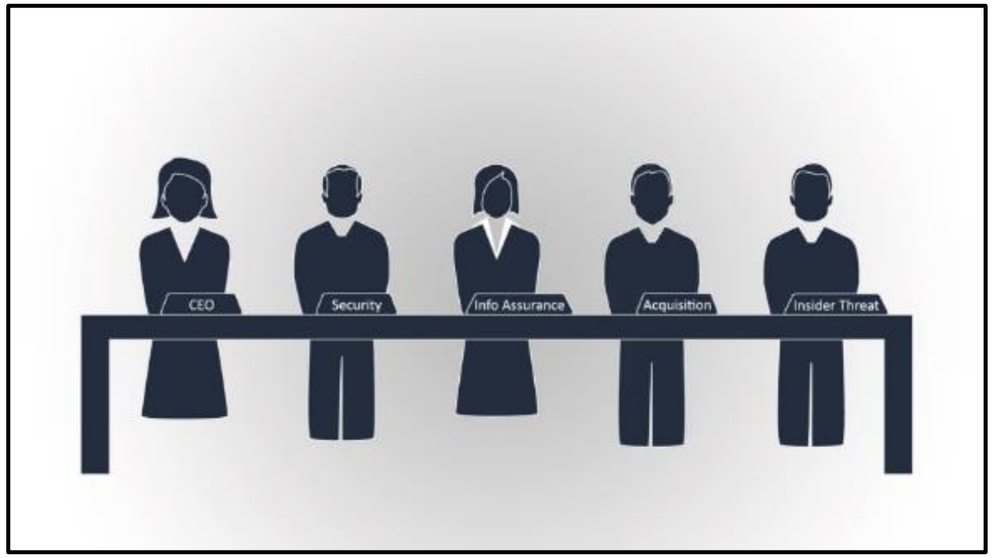
- Protect the Nation’s Critical Infrastructure
- Reduce Threats to Key U.S. Supply Chains
- Counter the Exploitation of the U.S. Economy
- Defend American Democracy against Foreign Influence
- Counter Foreign Intelligence Cyber and Technical Operations



Supply Chain Risk Management (SCRM)

- The management of risk to the integrity, trustworthiness, and authenticity of products and services.
- Addresses foreign intelligence entities (FIE) activities compromising the supply chain, which may include the introduction of counterfeit or malicious.
- Encompasses many disciplines and requires participation from subject matter experts.

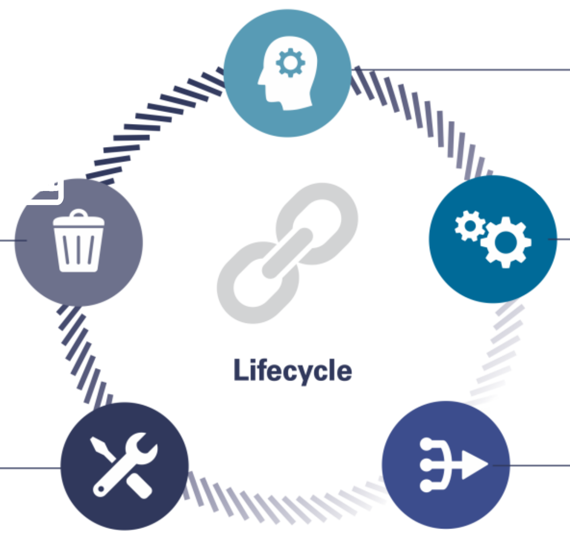




Supply Chain Risk Management (SCRM)

What is a key supply chain?

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



CONTENT & DESIGN

- Data exfiltration
- Intellectual Property (IP) Loss
- Unintentional Design Modifications

MANUFACTURE & INTEGRATION

- Malware Insertion
- Intellectual Property Loss
- Counterfeit parts

DEPLOYMENT

- Product Tampering
- Product Theft

MAINTENANCE

- Product Tampering
- Unauthorized access

RETIREMENT

- Counterfeiting
- Intellectual Property Theft

SCRM Highlights

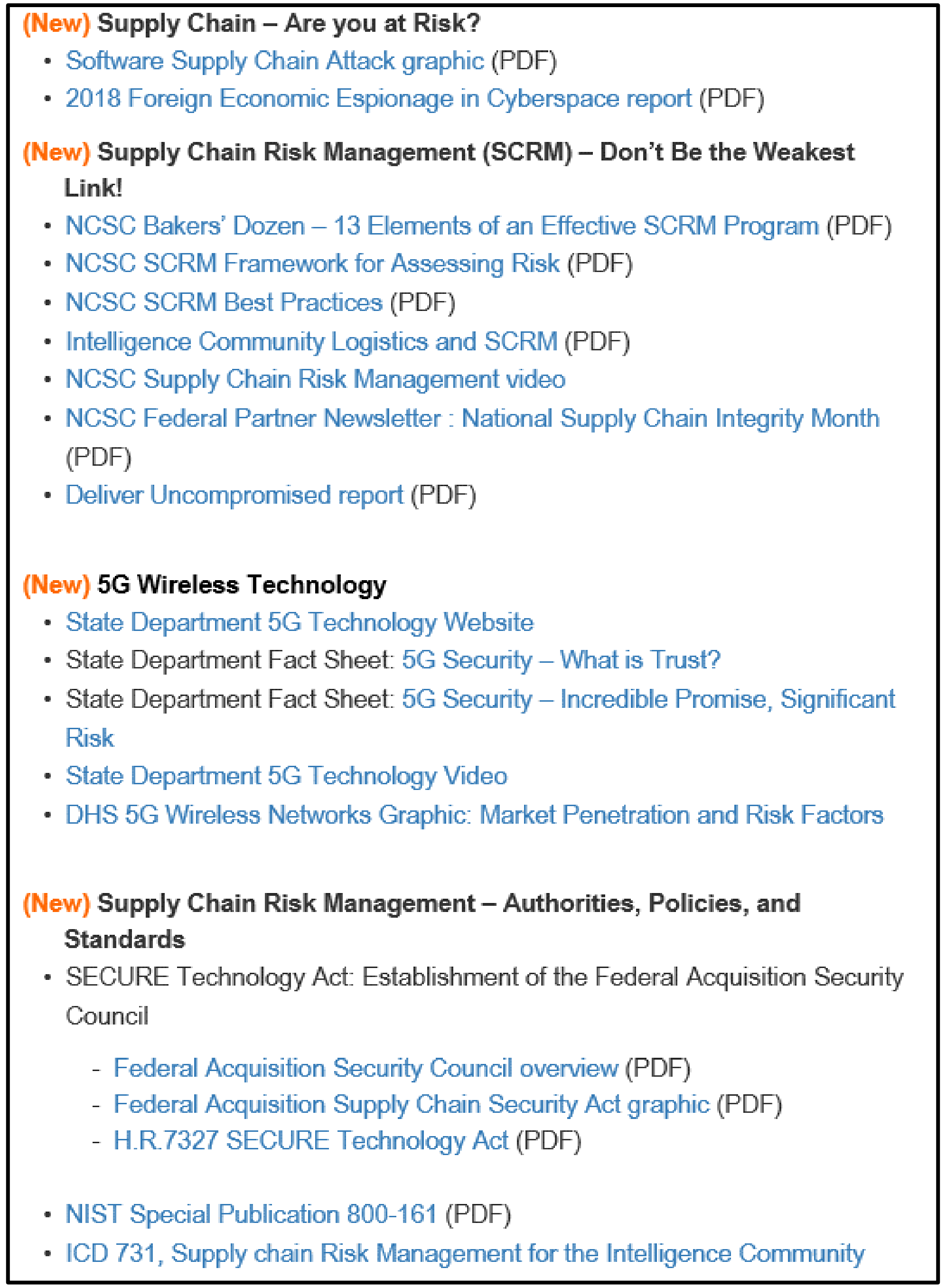
- Executive Level commitment
- Whole team approach
- Information sharing
- Criticality assessment
- Security as a pillar of supply chain
- Black list/white list
- Business due diligence

Business Due Diligence

- What is it?
  - A process involving a detailed inquiry prior to entering into a relationship
- Advantages
  - Informed decision/avoid surprises
  - Highlight future problems
  - Get what you pay for
- Disadvantages
  - Can be lengthy and difficult
  - Seller may be hesitant to share
- How is it conducted
  - Checklist
  - Data set (publicly available v. classified)
  - Tools

Supply Chain Countermeasures

- To reduce threats to key U.S. supply chains, 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.



(New) Supply Chain – Are you at Risk?

- Software Supply Chain Attack graphic (PDF)
- 2018 Foreign Economic Espionage in Cyberspace report (PDF)

(New) Supply Chain Risk Management (SCRM) – Don't Be the Weakest Link!

- NCSC Bakers' Dozen – 13 Elements of an Effective SCRM Program (PDF)
- NCSC SCRM Framework for Assessing Risk (PDF)
- NCSC SCRM Best Practices (PDF)
- Intelligence Community Logistics and SCRM (PDF)
- NCSC Supply Chain Risk Management video
- NCSC Federal Partner Newsletter : National Supply Chain Integrity Month (PDF)
- Deliver Uncompromised report (PDF)

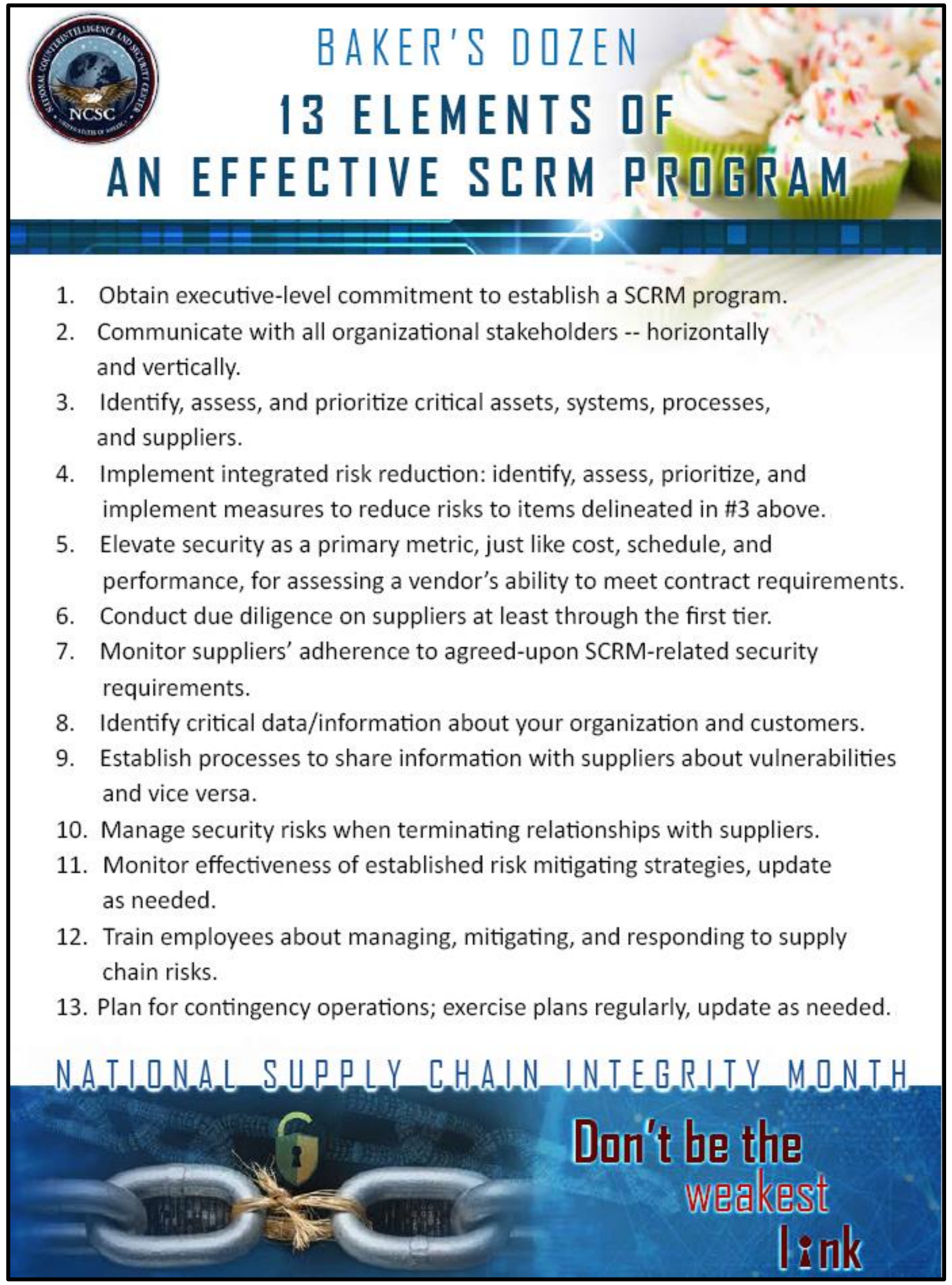
(New) 5G Wireless Technology

- State Department 5G Technology Website
- State Department Fact Sheet: 5G Security – What is Trust?
- State Department Fact Sheet: 5G Security – Incredible Promise, Significant Risk
- State Department 5G Technology Video
- DHS 5G Wireless Networks Graphic: Market Penetration and Risk Factors

(New) Supply Chain Risk Management – Authorities, Policies, and Standards

- 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)
- NIST Special Publication 800-161 (PDF)
- ICD 731, Supply chain Risk Management for the Intelligence Community

NCSC Products



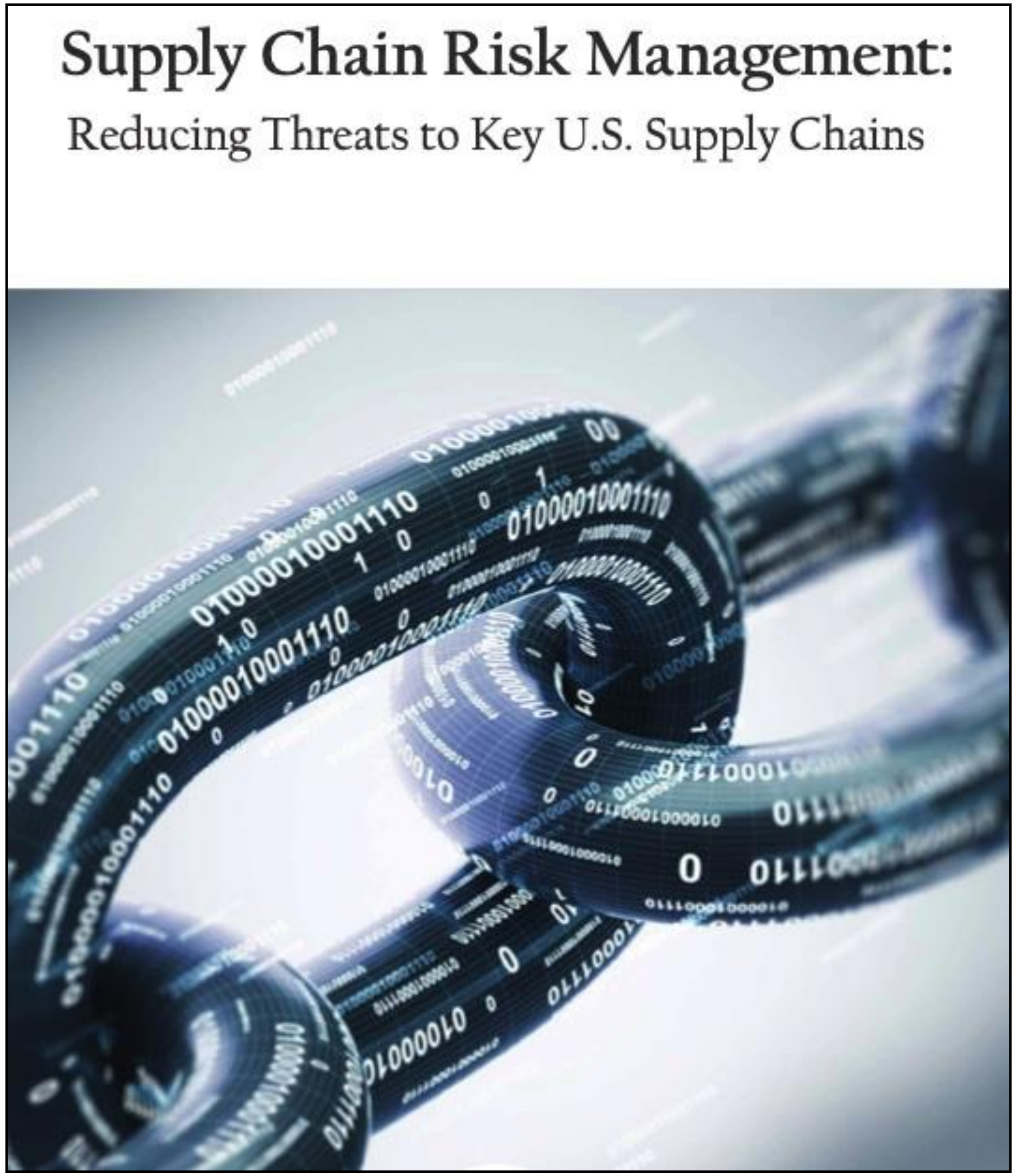
BAKER'S DOZEN

13 ELEMENTS OF AN EFFECTIVE SCRM PROGRAM

1. Obtain executive-level commitment to establish a SCRM program.
2. Communicate with all organizational stakeholders -- horizontally and vertically.
3. Identify, assess, and prioritize critical assets, systems, processes, and suppliers.
4. Implement integrated risk reduction: identify, assess, prioritize, and implement measures to reduce risks to items delineated in #3 above.
5. Elevate security as a primary metric, just like cost, schedule, and performance, for assessing a vendor's ability to meet contract requirements.
6. Conduct due diligence on suppliers at least through the first tier.
7. Monitor suppliers' adherence to agreed-upon SCRM-related security requirements.
8. Identify critical data/information about your organization and customers.
9. Establish processes to share information with suppliers about vulnerabilities and vice versa.
10. Manage security risks when terminating relationships with suppliers.
11. Monitor effectiveness of established risk mitigating strategies, update as needed.
12. Train employees about managing, mitigating, and responding to supply chain risks.
13. Plan for contingency operations; exercise plans regularly, update as needed.

NATIONAL SUPPLY CHAIN INTEGRITY MONTH

Don't be the weakest link



Supply Chain Risk Management:

Reducing Threats to Key U.S. Supply Chains

Questions and Concerns

Questions?

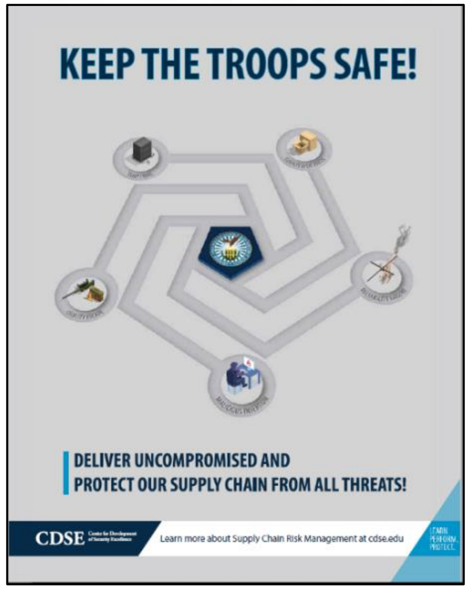
For more information on NCSC and Supply Chain, visit:

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



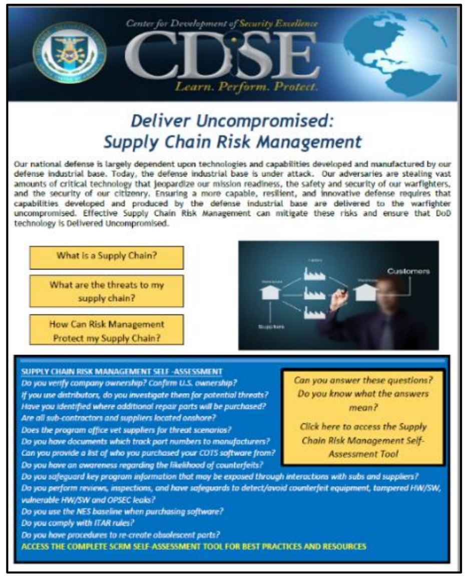
KEEP THE TROOPS SAFE!

DELIVER UNCOMPROMISED AND
PROTECT OUR SUPPLY CHAIN FROM ALL THREATS!

CDSE Center for Development of Security Excellence

Learn more about Supply Chain Risk Management at cdse.edu

LEARN. PERFORM. PROTECT.



Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

Deliver Uncompromised:
Supply Chain Risk Management

Our national defense is largely dependent upon technologies and capabilities developed and manufactured by our defense industrial base. Today, the defense industrial base is under attack. Our adversaries are stealing vast amounts of critical technology that jeopardize our mission readiness, the safety and security of our warfighters, and the security of our citizenry. Ensuring a more capable, resilient, and innovative defense requires that capabilities developed and produced by the defense industrial base are delivered to the warfighter uncompromised. Effective Supply Chain Risk Management can mitigate these risks and ensure that DoD technology is Delivered Uncompromised.

What is a Supply Chain?

What are the threats to my supply chain?

How Can Risk Management Protect my Supply Chain?

SUPPLY CHAIN RISK MANAGEMENT SELF -ASSESSMENT

Do you verify company ownership? Confirm U.S. ownership?
If you use distributors, do you investigate them for potential threats?
Have you identified where additional repair parts will be purchased?
Are all sub-contractors and suppliers located onshore?
Does the program office vet suppliers for threat scenarios?
Do you have documents which track part numbers to manufacturers?
Can you provide a list of who you purchased your COTS software from?
Do you have an awareness regarding the likelihood of counterfeits?
Do you safeguard key program information that may be exposed through interactions with subs and suppliers?
Do you perform reviews, inspections, and have safeguards to detect/avoid counterfeit equipment, tampered HW/SW, vulnerable HW/SW and OPSEC leaks?
Do you use the NES baseline when purchasing software?
Do you comply with ITAR rules?
Do you have procedures to re-create obsolescent parts?
ACCESS THE COMPLETE SCRM SELF-ASSESSMENT TOOL FOR BEST PRACTICES AND RESOURCES

Can you answer these questions? Do you know what the answers mean?

Click here to access the Supply Chain Risk Management Self-Assessment Tool

eLearn: DOD Supply Chain Fundamentals

eLearn: Life Cycle Logistics for the Rest of Us

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

Counterintelligence Toolkit: Supply Chain Risk Management

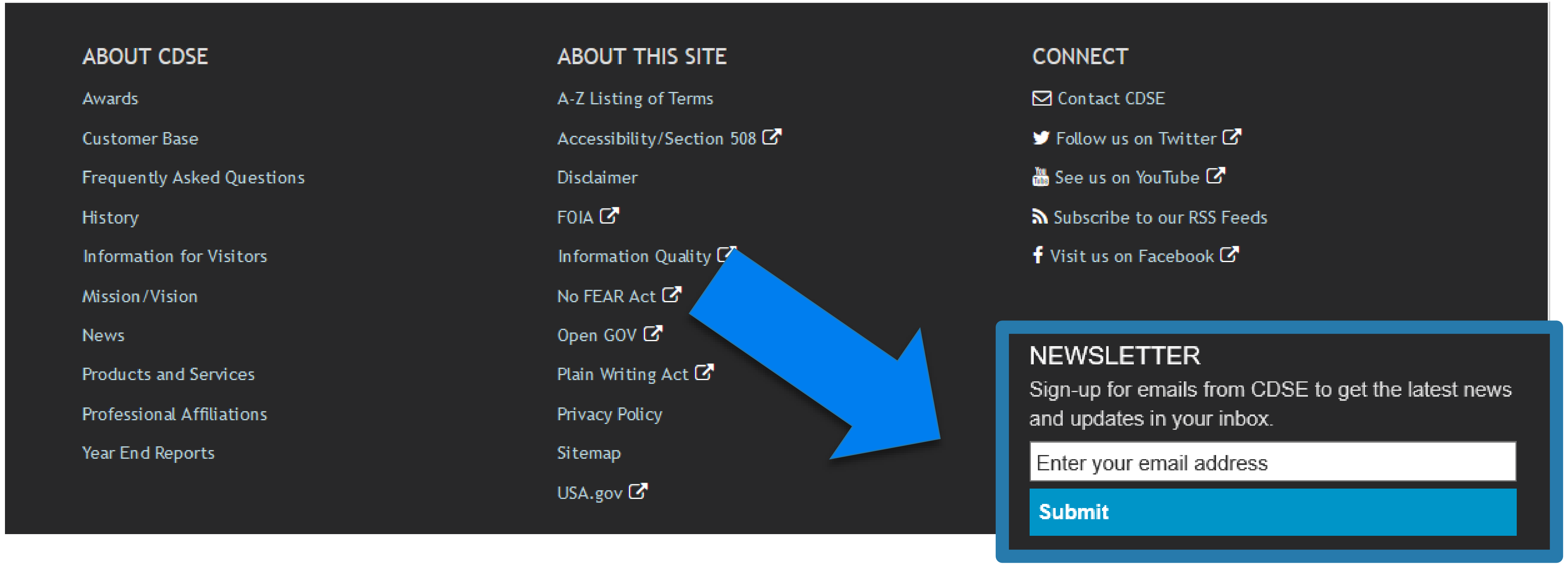
Cybersecurity Supply Chain Toolkit

Director of National Intelligence Supply Chain Toolkit

VIEW MORE MATERIALS HERE:
https://www.cdse.edu/toolkits/ci/supply.html

SUBSCRIPTION SERVICE

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



ABOUT CDSE

- Awards
- Customer Base
- Frequently Asked Questions
- History
- Information for Visitors
- Mission/Vision
- News
- Products and Services
- Professional Affiliations
- Year End Reports

ABOUT THIS SITE

- A-Z Listing of Terms
- Accessibility/Section 508
- Disclaimer
- FOIA
- Information Quality
- No FEAR Act
- Open GOV
- Plain Writing Act
- Privacy Policy
- Sitemap
- USA.gov

CONNECT

- Contact CDSE
- Follow us on Twitter
- See us on YouTube
- Subscribe to our RSS Feeds
- Visit us on Facebook

NEWSLETTER

Sign-up for emails from CDSE to get the latest news and updates in your inbox.

Enter your email address

Submit

sign up for
the latest updates

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
June 16	Overview of Continuous Vetting (CV) Methodology
July 29	Organizational Culture and Countering Insider Threats: Best Practice Examples from the United States Marine Corps

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