CDSE Center for Development of Security Excellence

Counterintelligence Webinar Series: Supply Chain Resiliency

LEARN.
PERFORM.
PROTECT.

TODAY'S SESSION

HOST:

Ed Kobeski, CDSE Counterintelligence

GUEST:

SSA Matthew Halvorsen, FBI

Joint Duty Assignment to NCSC

Strategic Program Manager

Supply Chain & Cyber Directorate

Supply Chain Directorate

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

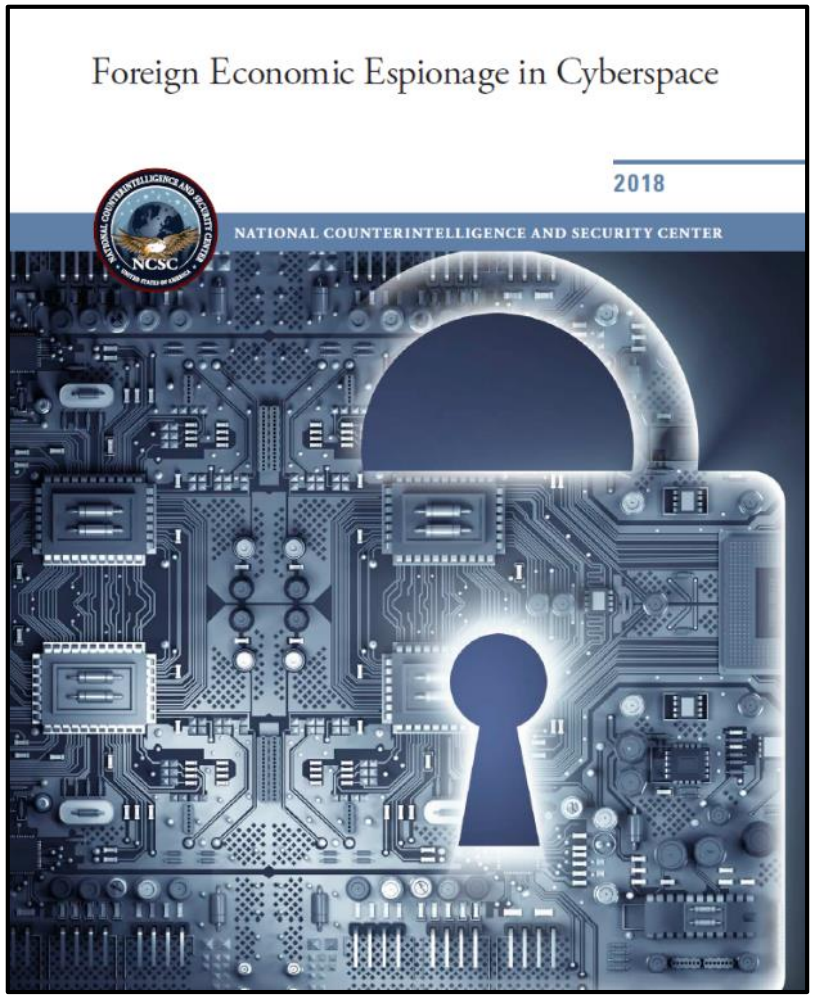
NATIONAL SUPPLY CHAIN INTEGRITY MONTH

Don't be the weakest link

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.

The National Counterintelligence and Security Center (NCSC)



Supply Chain and Cyber Directorate (SCD)

- SCD works with its partners to assess and mitigate the activities of foreign intelligence entities and other adversaries who attempt to compromise the supply chains of our government and industry. These adversaries exploit supply chain vulnerabilities to steal America's intellectual property, corrupt our software, surveil our critical infrastructure, and carry out other malicious activities.

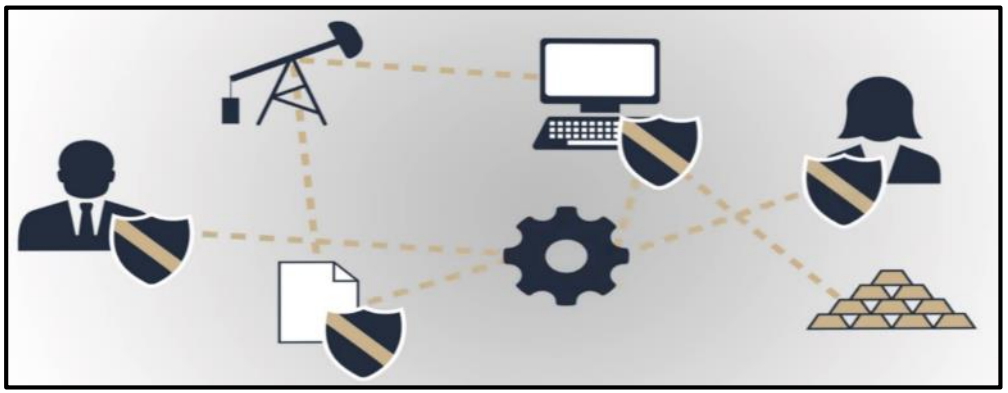
National Counterintelligence Strategy

of the United States of America
2020-2022

Executive Summary

Strategic Objectives, 1 of 2

- Protect the Nation's Critical Infrastructure
  - Protect the nation's civil and commercial, defense mission assurance and continuity of government infrastructure from foreign intelligence entities seeking to exploit or disrupt national critical functions.
- Reduce Threats to Key U.S. Supply Chains
  - Reduce threats to key U.S. supply chains to prevent foreign attempts to compromise the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of the U.S. government, the Defense Industrial Base, and the private sector.

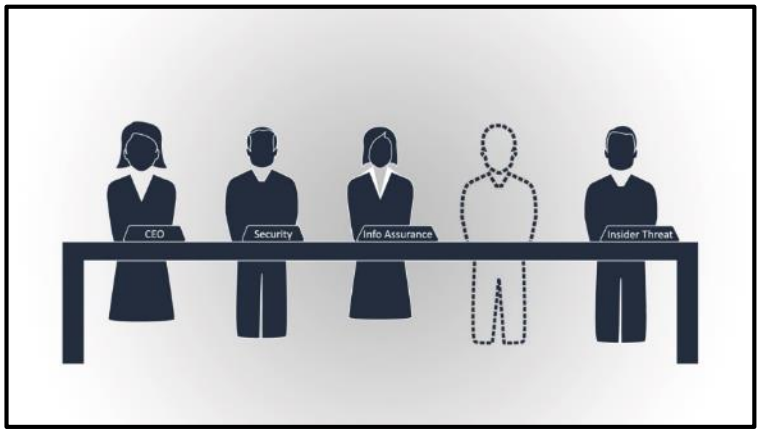


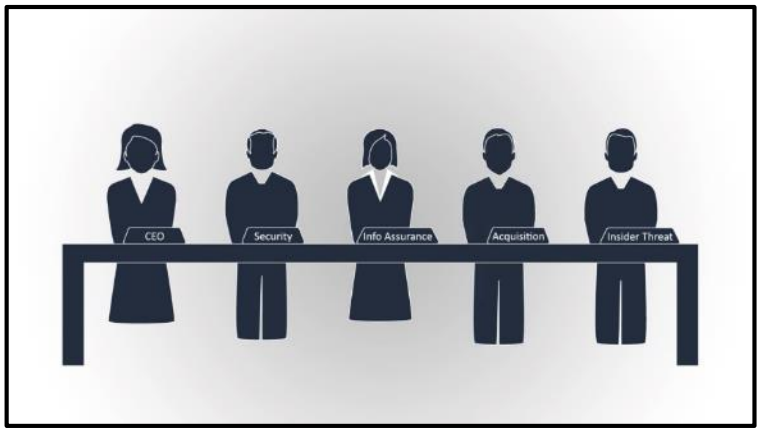
Strategic Objectives, 2 of 2

- Counter the Exploitation of the U.S. Economy
  - Counter the exploitation of the U.S. economy to protect America's competitive advantage in world markets and our technological leadership, and to ensure our economic prosperity and security.
- Defend American Democracy against Foreign Influence
  - Defend the United States against foreign influence to protect America's democratic institutions and processes, and preserve our culture of openness.
- Counter Foreign Intelligence Cyber and Technical Operations
  - Counter foreign intelligence cyber and technical operations that are harmful to U.S. interests.

Supply Chain Risk Management (SCRM)

- Supply Chain Risk Management (SCRM), within the federal government refers to management of risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain.
- It addresses the activities of foreign intelligence entities (FIE) and any other adversarial attempts aimed at compromising the supply chain, which may include the introduction of counterfeit or malicious items into the supply chain.
- Supply chain risk management encompasses many disciplines and requires participation from subject matter experts in acquisition, counterintelligence (CI), information assurance, logistics, program offices, analysis, security, and other relevant functions as necessary.

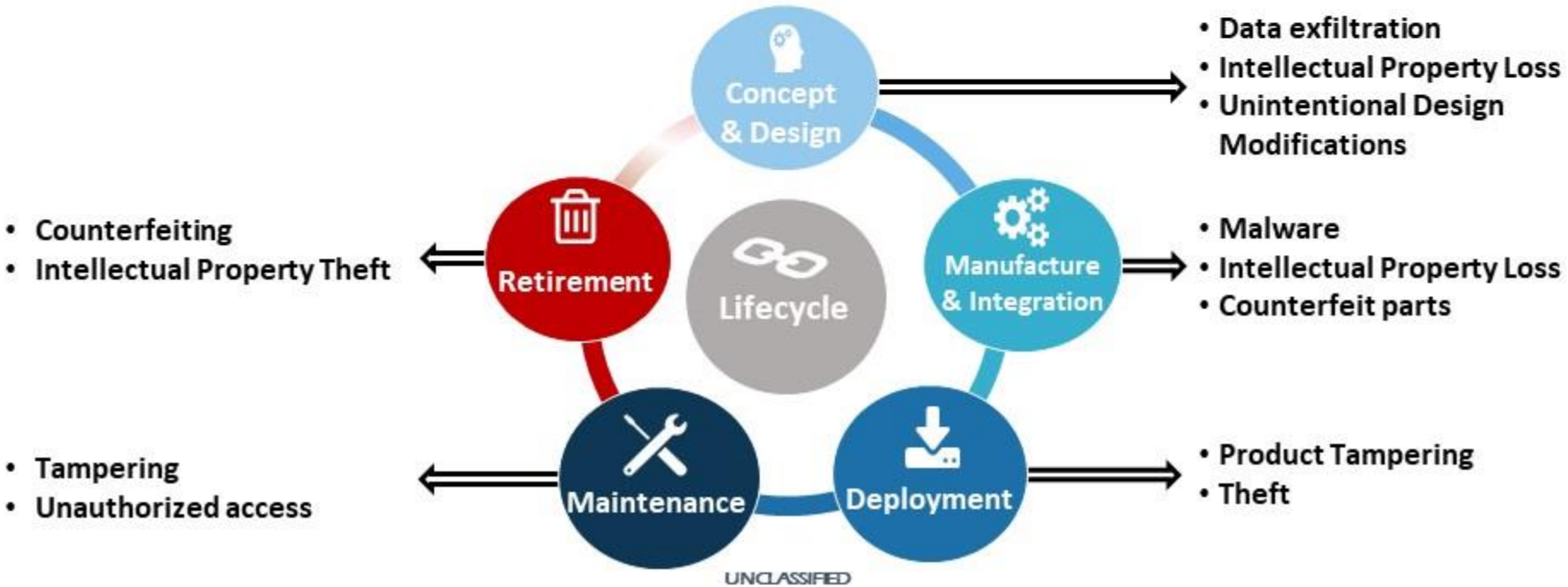




Supply Chain Risk Management (SCRM)

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 chain 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.



Two Supply Chain Statutes

- SECURE Technology Act – December 2018

T. 5178 PUBLIC LAW 115–390—DEC. 21, 2018

TITLE II—FEDERAL ACQUISITION SUPPLY CHAIN SECURITY

n

note. **SEC. 201. SHORT TITLE.**

This title may be cited as the "Federal Acquisition Supply Chain Security Act of 2018".

SEC. 202. FEDERAL ACQUISITION SUPPLY CHAIN SECURITY.

(a) IN GENERAL.—Chapter 13 of title 41, United States Code, 1 is amended by adding at the end the following new subchapter:

"SUBCHAPTER III—FEDERAL ACQUISITION SUPPLY CHAIN SECURITY

1. **"§ 1321. Definitions**

"In this subchapter:

"(1) APPROPRIATE CONGRESSIONAL COMMITTEES AND LEADERSHIP.—The term 'appropriate congressional committees and leadership' means—

Federal Acquisition Security Council – Overview

Federal Acquisition Supply Chain Security Act

Federal Acquisition Security Council

Provide Acquisition Security and SCRM Strategy and Guidance

- Recommend development of NIST standards for covered articles
- Conduct SCRM assessments
- Develop criteria to share information pertaining to SCRM with other federal and non federal entities
- Recommend exclusion of source of a covered article
- Engage private sector entities to improve information sharing
- Establish criteria/procedures and issue recommendations to exclude/remove covered articles

FASC Committee Members

FASC Chair

Exclusions/ Removal

Industry

Can Establish

- Program Office
- Committee
- Working Groups
- Other Bodies

Will Establish

- Information Sharing EA
- Shared Service EA
- Common Contract Solution EA

FASC – Information Sharing Requirements

Objective

- Meet SECURE Technology Act supply chain information sharing requirements
- Departments and Agencies Sharing with the 1) FASC and 2) with each other
- FASC sharing with 1) Executive Agencies, 2) other Federal entities, and 3) Non-Federal entities (Congress, Allied Partners, and Private Industry)

MUST

- Identify the content to be shared
- Determine circumstances for mandatory sharing and voluntary sharing
- Determine circumstances where shared information may be relied upon for mitigation, including removal or exclusion

MUST NOT

- Conflict with existing data protections for information being shared including :
  - National Security Classification
  - Personally Identifiable Information (PII)
  - Procurement-Sensitive
  - Proprietary

NDAA FY 20 – Supply Chain Information Sharing Task Force

IAA Sec. 6306

- DNI shall establish task force for sharing supply chain IC information with the federal acquisition community.

Statutory TF Members (*Member of FASC as well)

- DHS*
- GSA*
- OMB-OFPP*
- FBI*
- DOD-DCSA
- The Director of NCSC* – Serves as Taskforce Chairperson
- Any other members DNI appoints

Alignment with FASC efforts:

- Centralizes IC supply chain information sharing with federal acquisition community
- Reinforces ICD 731 standards for protecting supply chain information while sharing responsibly
- Supports the FASC information sharing needs
- Unified voice on threats to the supply chain

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 Counterintelligence and Security Center
Supply Chain Directorate

Supply Chain Risk Management
Best Practices

Introduction: The U.S. is under systematic assault by Foreign Intelligence Entities[1] (FIEs) who have augmented traditional intelligence operations with nontraditional methods, including economic espionage, supply chain exploitation, and the use of students, scientists, and corporate employees, to collect both classified and unclassified information. The scale of this effort has put entire industries at risk.

Specifically, the globalization of supply chains presents a major attack vector, characterized by a complex web of contracts and subcontracts for component parts, services, and manufacturing. FIEs use this complexity to obfuscate efforts to penetrate sensitive research and development programs, steal vast amounts of personally identifiable information (PII) and intellectual property (IP), and insert malware into critical components. Supply chain exploitation, especially when executed in concert with cyber intrusions, malicious insiders, and economic espionage, threatens the integrity of key U.S. economic, critical infrastructure, and research/development sectors. The following "best practices" provide options to address this threat.

Governance and Administrative Actions

Establish Internal Policies and Processes

- Develop internal company policies and processes that implement Supply Chain Risk Management (SCRM).
- Identify and document roles and responsibilities across the enterprise.
- Create a Capability Maturity Model (CMM) for the SCRM program.
- Delineate decision making authority and escalation process.
- Ensure that SCRM is part of the organization's annual enterprise risk assessment process.

Questions and Concerns

Questions?

For more information on NCSC and Supply Chain, visit:

https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

NEXT WEEK!!

INSIDER THREAT WEBINAR SERIES: Insider Threat and Equal Employment Opportunity (EEO)

LEARN.
PERFORM.
PROTECT.

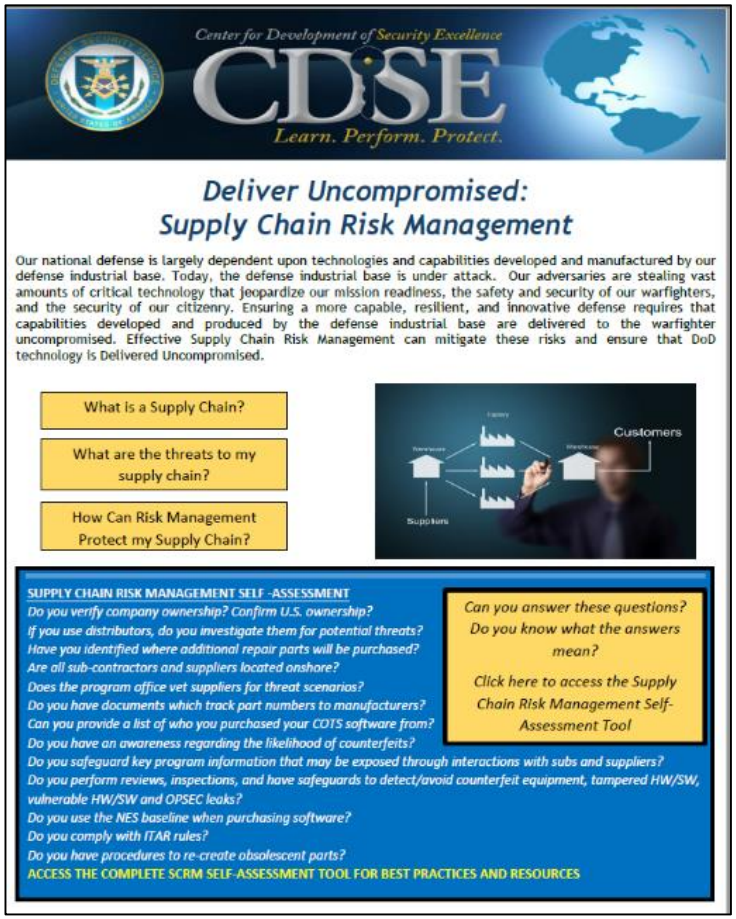
TIME: 30 April, 1200-1300 EST

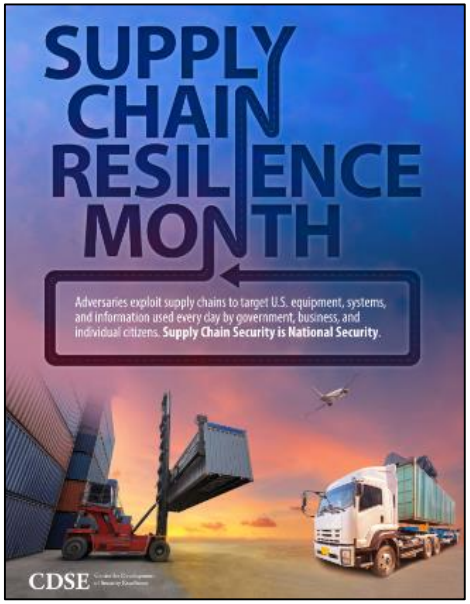
HOST: Mr. Steve Resel
CDSE Insider Threat

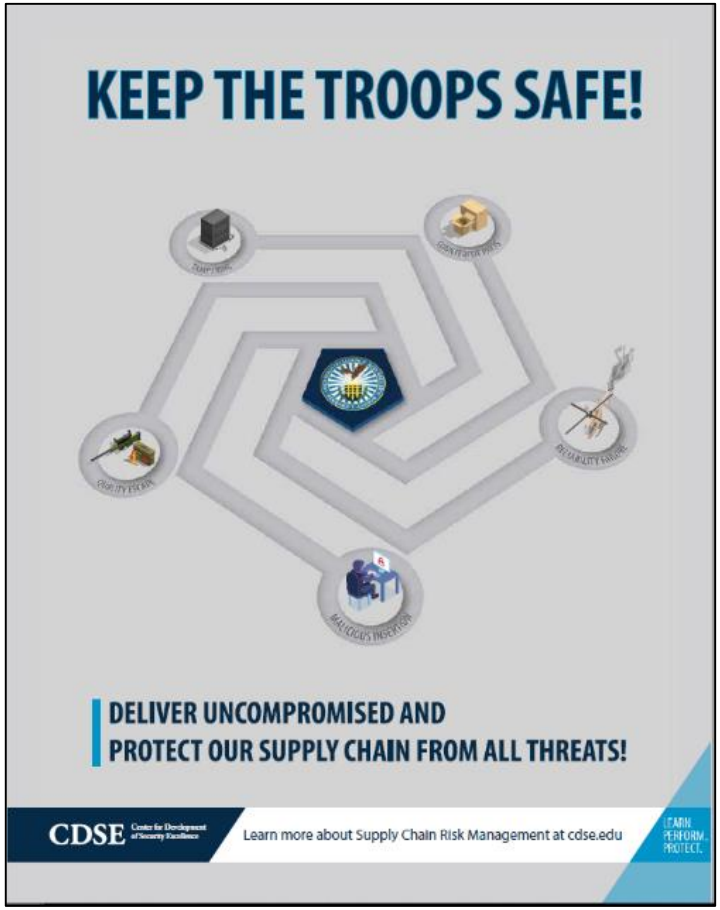
GUEST: Ms. Edie Brumskill
EEO Program Manager,
Capital Metro Area
Office of Diversity & Equal Opportunity

Register Now: https://www.cdse.edu/catalog/webinars/index.html

National Supply Chain Integrity Month



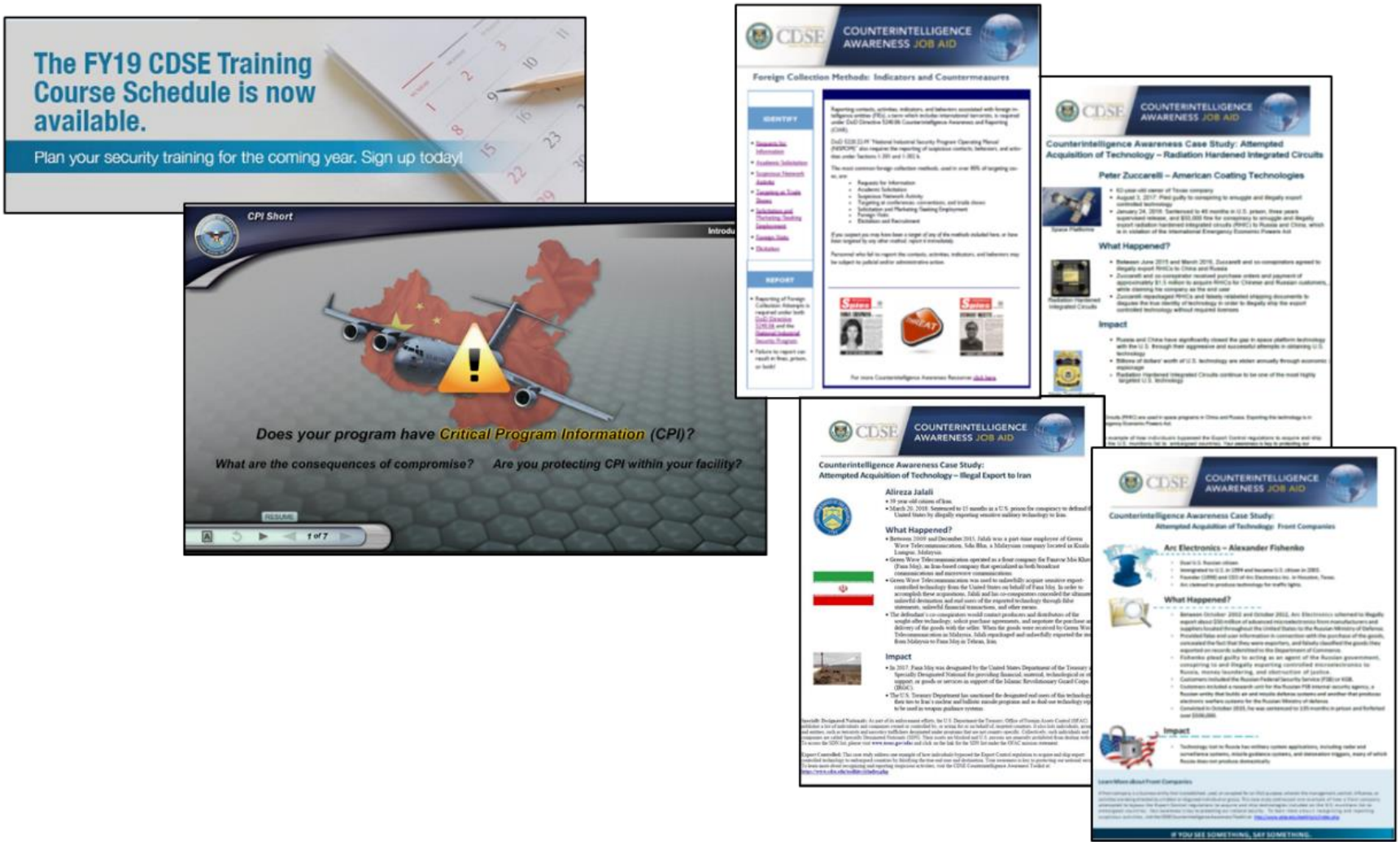




VIEW MORE MATERIAL HERE:

https://www.ncsc.gov

CDSE CI Training and Job Aids



CDSE WANTS TO HEAR FROM YOU!

CDSE Counterintelligence POC:

Ed Kobeski

410-689-7842

EMAIL: Edwin.f.Kobeski.civ@mail.mil