CDSE Center for Development of Security Excellence

Counterintelligence Webinar Series

Supply Chain Resilience

LEARN.
PERFORM.
PROTECT.

Today's Session:

Host:

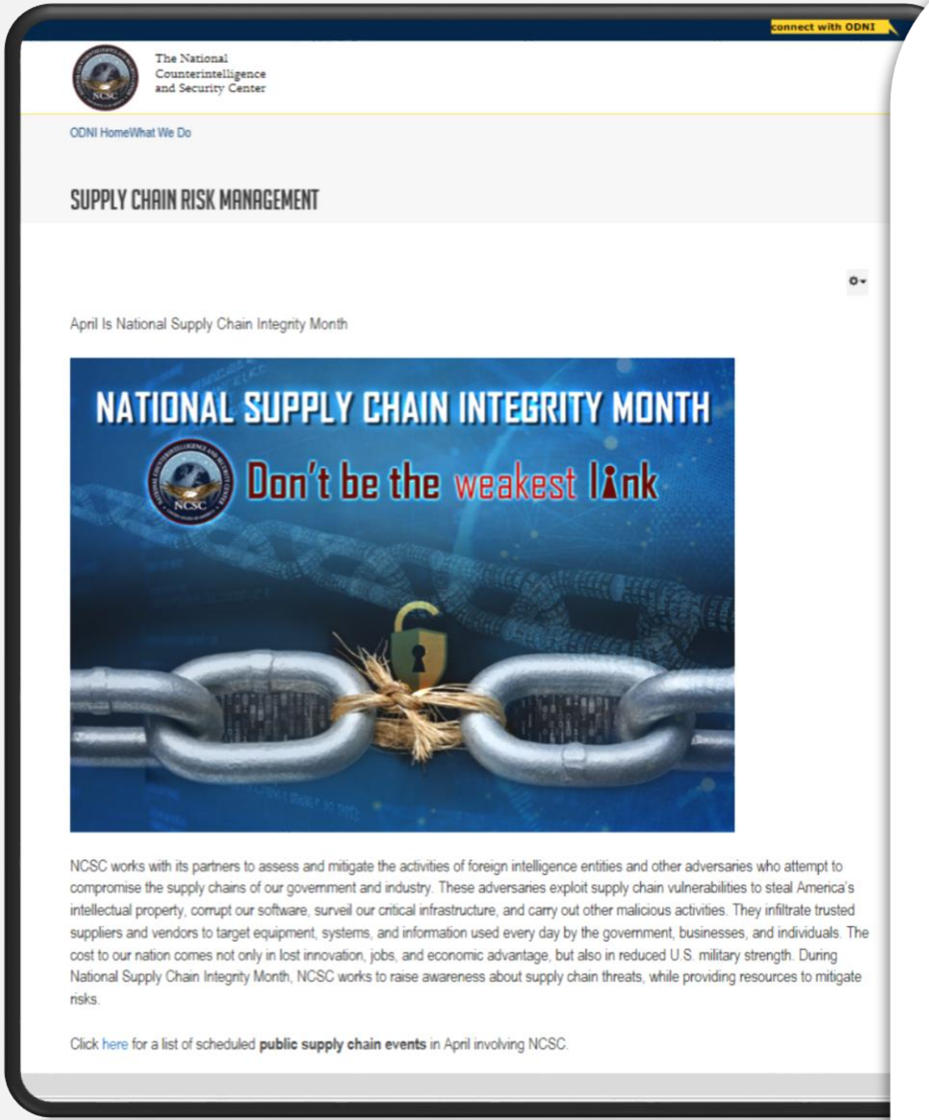
Rebecca Morgan, CDSE Insider Threat

Guest:

- **Ms. Joyce Corell,** ODNI, NCSC, Supply Chain & Cyber Directorate

CDSE Center for Development of Security Excellence

NATIONAL SUPPLY CHAIN INTEGRITY MONTH
NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
NCSC
Don't be the weakest link


connect with ODNI
NATIONAL SUPPLY CHAIN INTEGRITY MONTH
Don't be the weakest link
NCSC

The National Counterintelligence and Security Center

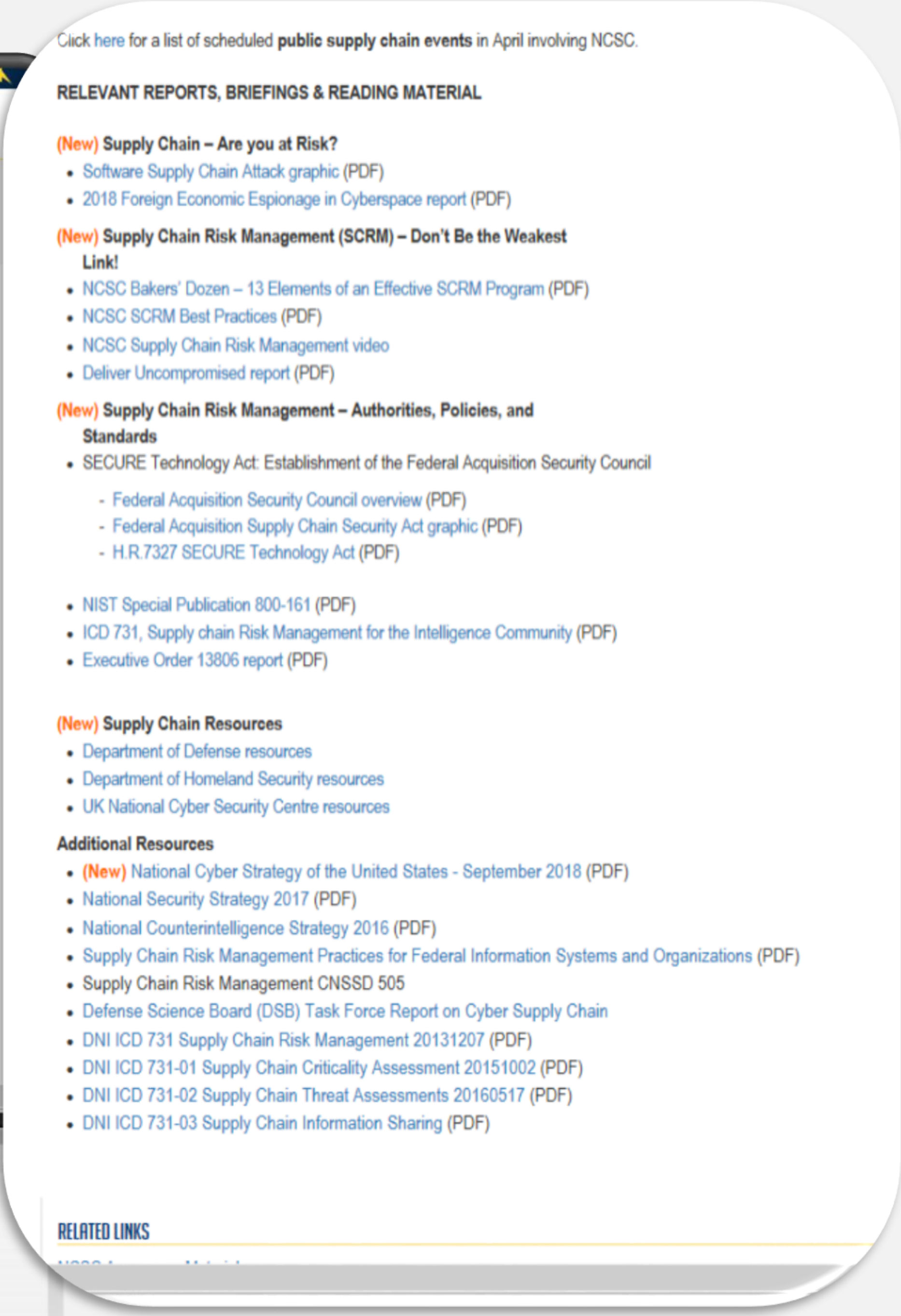
ODNI HomeWhat We Do

SUPPLY CHAIN RISK MANAGEMENT

April Is National Supply Chain Integrity Month

NCSC 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. They infiltrate trusted suppliers and vendors to target equipment, systems, and information used every day by the government, businesses, and individuals. The cost to our nation comes not only in lost innovation, jobs, and economic advantage, but also in reduced U.S. military strength. During National Supply Chain Integrity Month, NCSC works to raise awareness about supply chain threats, while providing resources to mitigate risks.

Click here for a list of scheduled **public supply chain events** in April involving NCSC.



Click here for a list of scheduled **public supply chain events** in April involving NCSC.

RELEVANT REPORTS, BRIEFINGS & READING MATERIAL

(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 Best Practices (PDF)
- NCSC Supply Chain Risk Management video
- Deliver Uncompromised report (PDF)

(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 (PDF)
- Executive Order 13806 report (PDF)

(New) **Supply Chain Resources**

- Department of Defense resources
- Department of Homeland Security resources
- UK National Cyber Security Centre resources

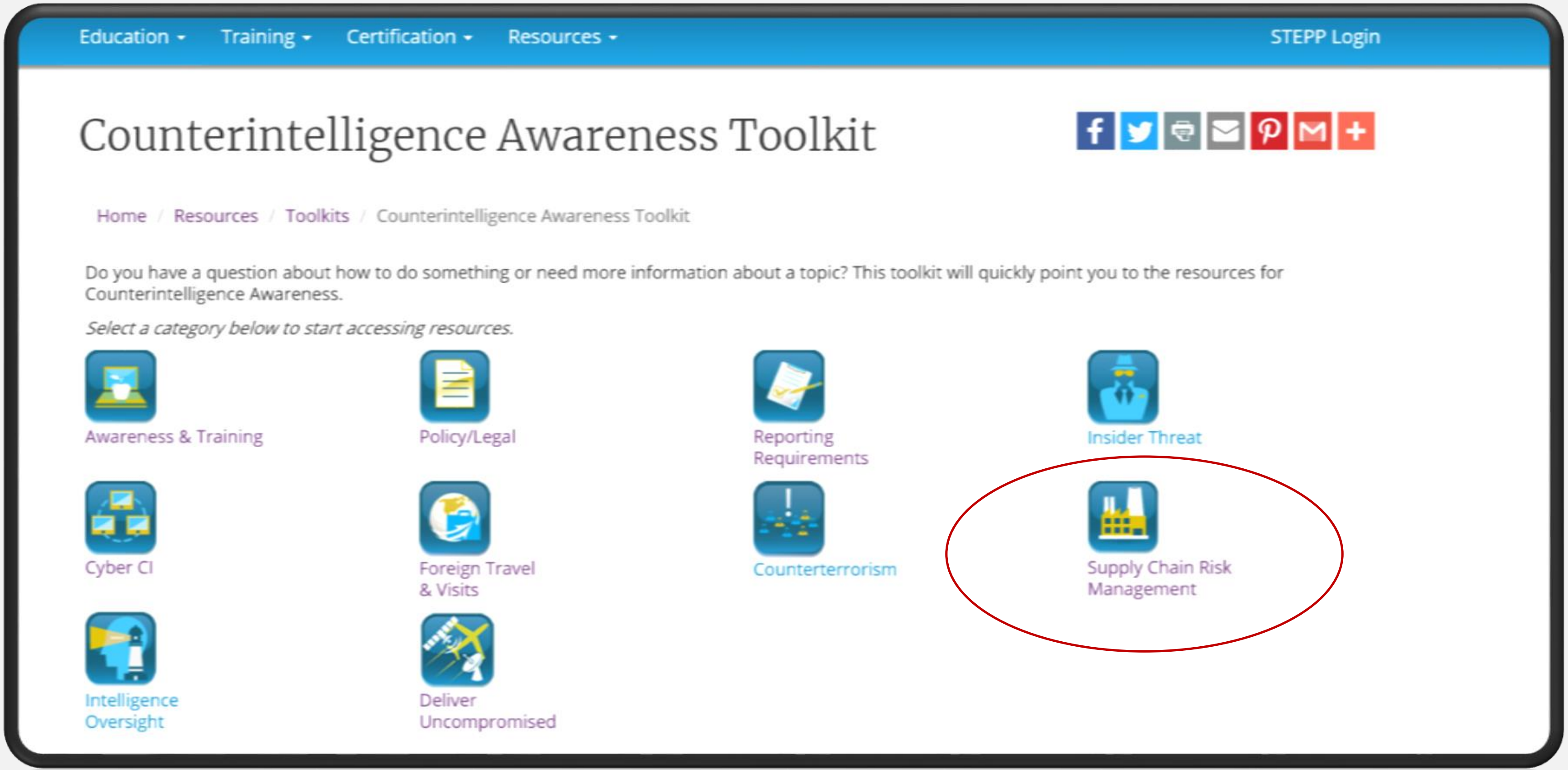
Additional Resources

- (New) National Cyber Strategy of the United States - September 2018 (PDF)
- National Security Strategy 2017 (PDF)
- National Counterintelligence Strategy 2016 (PDF)
- Supply Chain Risk Management Practices for Federal Information Systems and Organizations (PDF)
- Supply Chain Risk Management CNSSD 505
- Defense Science Board (DSB) Task Force Report on Cyber Supply Chain
- DNI ICD 731 Supply Chain Risk Management 20131207 (PDF)
- DNI ICD 731-01 Supply Chain Criticality Assessment 20151002 (PDF)
- DNI ICD 731-02 Supply Chain Threat Assessments 20160517 (PDF)
- DNI ICD 731-03 Supply Chain Information Sharing (PDF)

RELATED LINKS

CDSE Center for Development of Security Excellence

CDSE SCRM TRAINING



Counterintelligence Awareness Toolkit

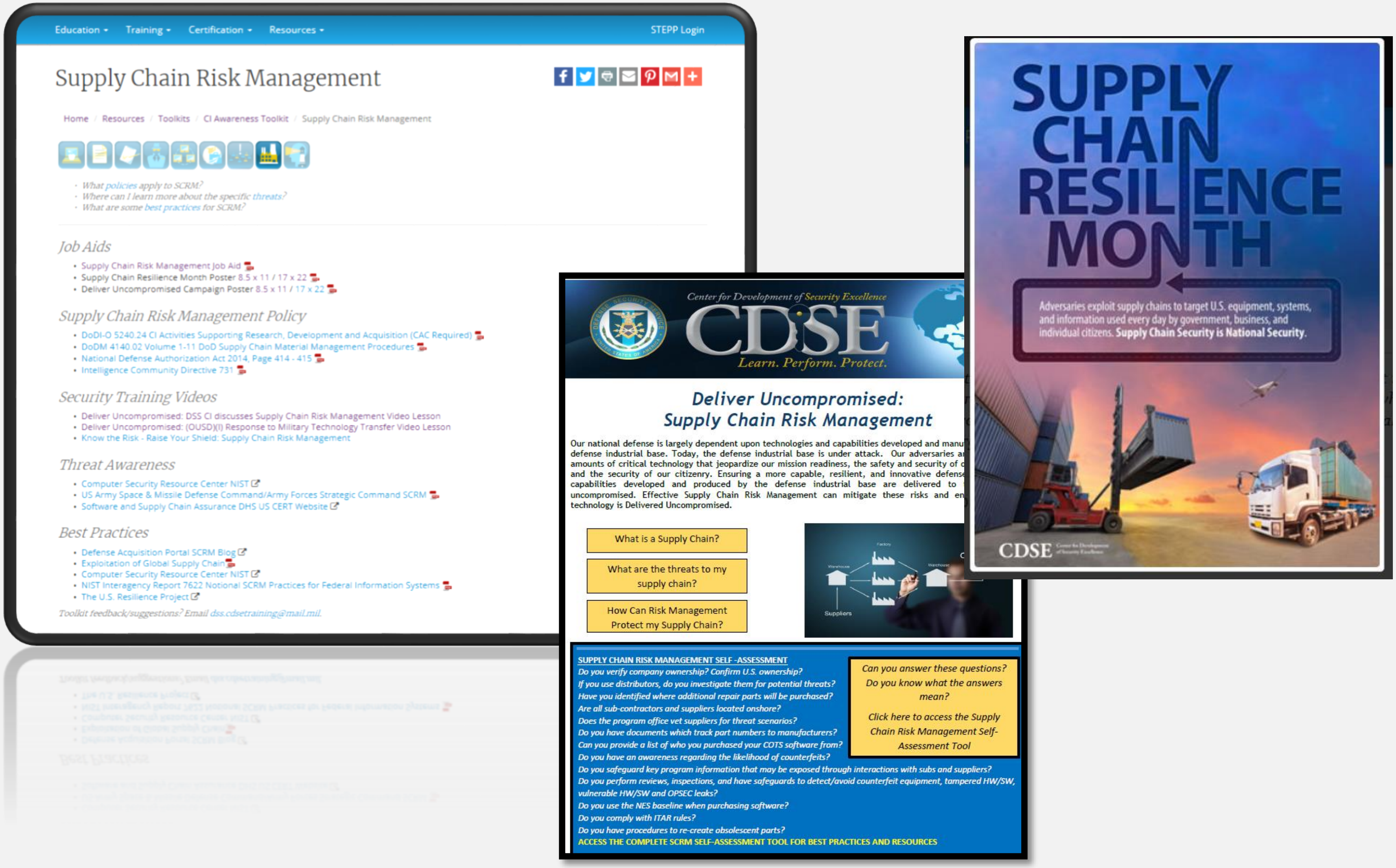
Home / Resources / Toolkits / Counterintelligence Awareness Toolkit

Do you have a question about how to do something or need more information about a topic? This toolkit will quickly point you to the resources for Counterintelligence Awareness.

Select a category below to start accessing resources.

CDSE Center for Development of Security Excellence

CDSE SCRM TRAINING



Supply Chain Risk Management

Home / Resources / Toolkits / CI Awareness Toolkit / Supply Chain Risk Management

- *What policies apply to SCRM?*
- *Where can I learn more about the specific threats?*
- *What are some best practices for SCRM?*

Job Aids

- Supply Chain Risk Management Job Aid
- Supply Chain Resilience Month Poster 8.5 x 11 / 17 x 22
- Deliver Uncompromised Campaign Poster 8.5 x 11 / 17 x 22

Supply Chain Risk Management Policy

- DoDI-O 5240.24 CI Activities Supporting Research, Development and Acquisition (CAC Required)
- DoDM 4140.02 Volume 1-11 DoD Supply Chain Material Management Procedures
- National Defense Authorization Act 2014, Page 414 - 415
- Intelligence Community Directive 731

Security Training Videos

- Deliver Uncompromised: DSS CI discusses Supply Chain Risk Management Video Lesson
- Deliver Uncompromised: (OUSD)(I) Response to Military Technology Transfer Video Lesson
- Know the Risk - Raise Your Shield: Supply Chain Risk Management

Threat Awareness

- Computer Security Resource Center NIST
- US Army Space & Missile Defense Command/Army Forces Strategic Command SCRM
- Software and Supply Chain Assurance DHS US CERT Website

Best Practices

- Defense Acquisition Portal SCRM Blog
- Exploitation of Global Supply Chain
- Computer Security Resource Center NIST
- NIST Interagency Report 7622 Notional SCRM Practices for Federal Information Systems
- The U.S. Resilience Project

Toolkit feedback/suggestions? Email dss.cdsetraining@mail.mil.

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 manu defense industrial base. Today, the defense industrial base is under attack. Our adversaries ar amounts of critical technology that jeopardize our mission readiness, the safety and security of c and the security of our citizenry. Ensuring a more capable, resilient, and innovative defense capabilities developed and produced by the defense industrial base are delivered to uncompromised. Effective Supply Chain Risk Management can mitigate these risks and en 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?

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

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

ACCESS THE COMPLETE SCRM SELF-ASSESSMENT TOOL FOR BEST PRACTICES AND RESOURCES

Adversaries exploit supply chains to target U.S. equipment, systems, and information used every day by government, business, and individual citizens. **Supply Chain Security is National Security.**

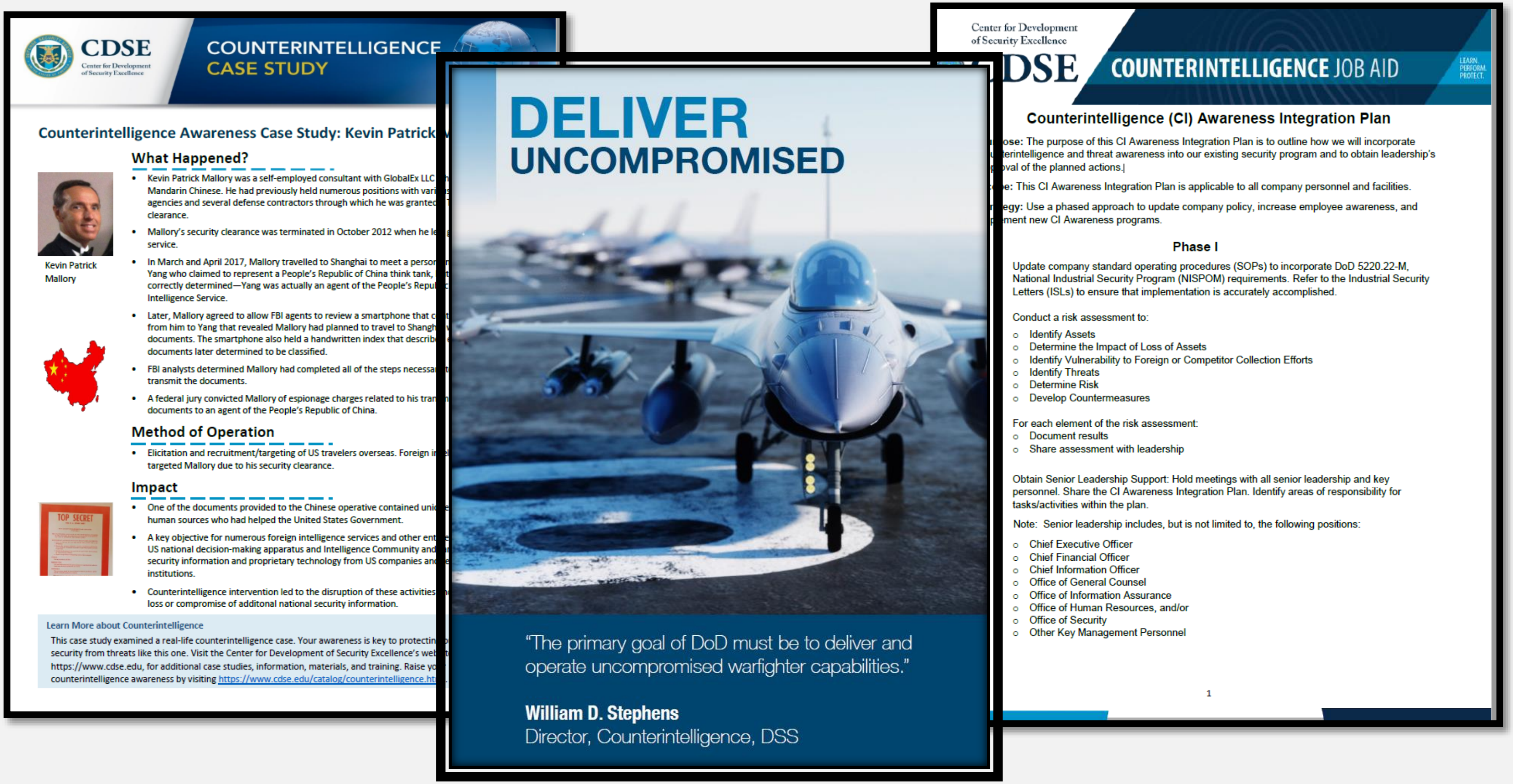
CDSE Center for Development of Security Excellence

NEW COUNTERINTELLIGENCE AWARENESS TRAINING

New course now available! CI117
PROTECTING ASSETS IN THE
NISP
(National Industrial Security Program)

CDSE Center for Development of Security Excellence

NEW COUNTERINTELLIGENCE AWARENESS TRAINING



CDSE Center for Development of Security Excellence

COUNTERINTELLIGENCE CASE STUDY

Counterintelligence Awareness Case Study: Kevin Patrick

What Happened?

Kevin Patrick Mallory

- Kevin Patrick Mallory was a self-employed consultant with GlobalEx LLC Mandarin Chinese. He had previously held numerous positions with vari agencies and several defense contractors through which he was grante clearance.
- Mallory's security clearance was terminated in October 2012 when he le service.
- In March and April 2017, Mallory travelled to Shanghai to meet a person Yang who claimed to represent a People's Republic of China think tank, correctly determined—Yang was actually an agent of the People's Repub Intelligence Service.
- Later, Mallory agreed to allow FBI agents to review a smartphone that c from him to Yang that revealed Mallory had planned to travel to Shangh documents. The smartphone also held a handwritten index that describ documents later determined to be classified.
- FBI analysts determined Mallory had completed all of the steps necessa transmit the documents.
- A federal jury convicted Mallory of espionage charges related to his tran documents to an agent of the People's Republic of China.

Method of Operation

- Elicitation and recruitment/targeting of US travelers overseas. Foreign i targeted Mallory due to his security clearance.

Impact

- One of the documents provided to the Chinese operative contained uni human sources who had helped the United States Government.
- A key objective for numerous foreign intelligence services and other ent US national decision-making apparatus and Intelligence Community and security information and proprietary technology from US companies an institutions.
- Counterintelligence intervention led to the disruption of these activities loss or compromise of additonal national security information.

Learn More about Counterintelligence

This case study examined a real-life counterintelligence case. Your awareness is key to protectin security from threats like this one. Visit the Center for Development of Security Excellence's web https://www.cdse.edu, for additional case studies, information, materials, and training. Raise yo counterintelligence awareness by visiting https://www.cdse.edu/catalog/counterintelligence.ht

DELIVER UNCOMPROMISED

"The primary goal of DoD must be to deliver and operate uncompromised warfighter capabilities."

William D. Stephens
Director, Counterintelligence, DSS

Center for Development of Security Excellence
DSE COUNTERINTELLIGENCE JOB AID
LEARN. PERFORM. PROTECT.

Counterintelligence (CI) Awareness Integration Plan

ose: The purpose of this CI Awareness Integration Plan is to outline how we will incorporate terintelligence and threat awareness into our existing security program and to obtain leadership's oval of the planned actions.

e: This CI Awareness Integration Plan is applicable to all company personnel and facilities.

egy: Use a phased approach to update company policy, increase employee awareness, and ement new CI Awareness programs.

Phase I

Update company standard operating procedures (SOPs) to incorporate DoD 5220.22-M, National Industrial Security Program (NISPOM) requirements. Refer to the Industrial Security Letters (ISLs) to ensure that implementation is accurately accomplished.

Conduct a risk assessment to:

- Identify Assets
- Determine the Impact of Loss of Assets
- Identify Vulnerability to Foreign or Competitor Collection Efforts
- Identify Threats
- Determine Risk
- Develop Countermeasures

For each element of the risk assessment:

- Document results
- Share assessment with leadership

Obtain Senior Leadership Support: Hold meetings with all senior leadership and key personnel. Share the CI Awareness Integration Plan. Identify areas of responsibility for tasks/activities within the plan.

Note: Senior leadership includes, but is not limited to, the following positions:

- Chief Executive Officer
- Chief Financial Officer
- Chief Information Officer
- Office of General Counsel
- Office of Information Assurance
- Office of Human Resources, and/or
- Office of Security
- Other Key Management Personnel

1

CDSE Center for Development of Security Excellence

Counterintelligence Awareness Training POC:

Rebecca Morgan
(410) 689-1294
Email: Rebecca.a.morgan22.civ@mail.mil