Counterintelligence Webinar Series:

Supply Chain Risk Management

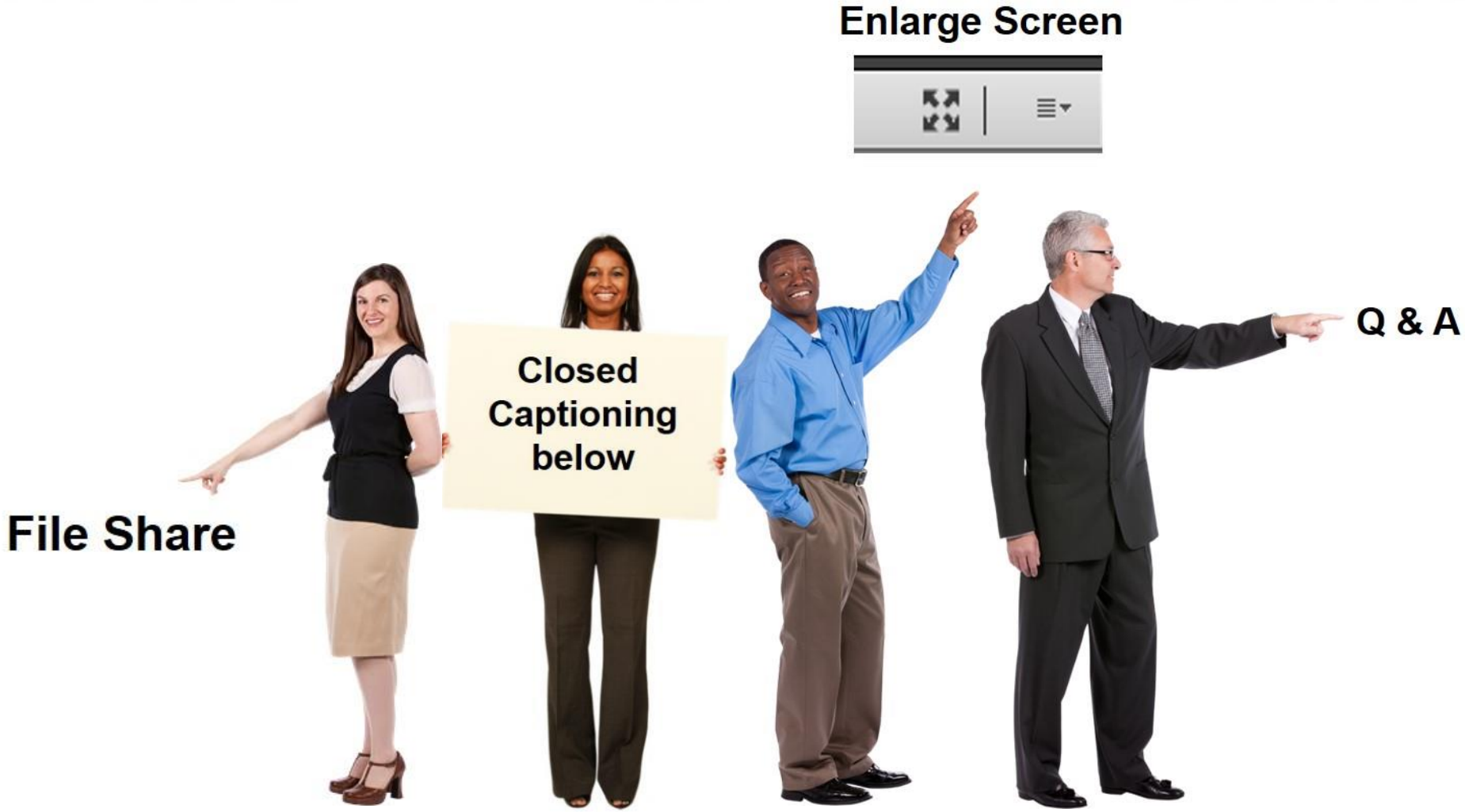
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

TODAY'S SESSION

Hosts:

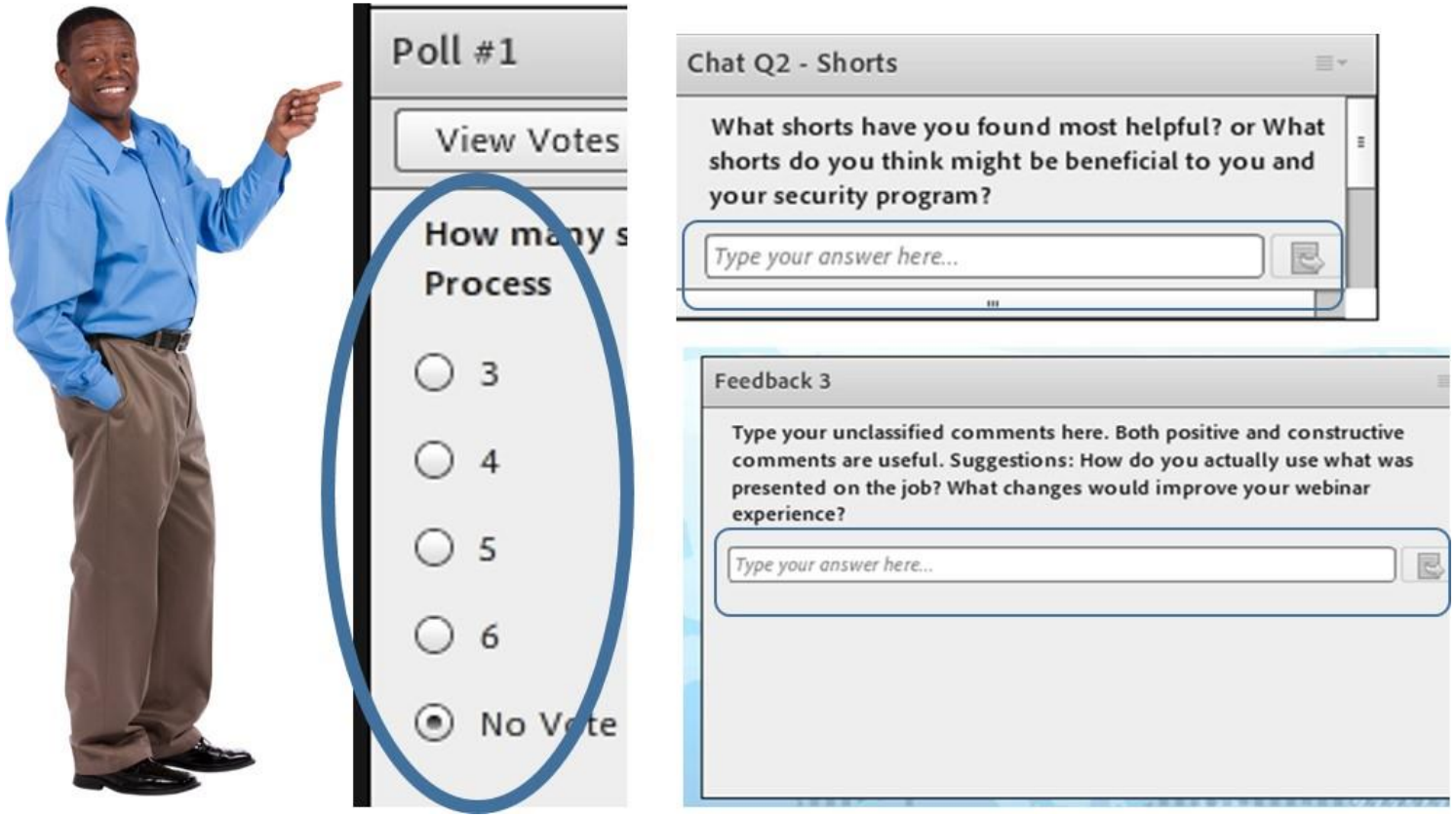
- Ed Kobeski, CDSE Counterintelligence (CI)
- Mark Zahner, DCSA CI Special Agent

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.

AGENDA

- What is a Supply Chain?
- What are the risks to my Supply Chain?
- How can Risk Management help protect my Supply Chain?
- Questions

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. The Facility Security Officer's Job, not mine

D. An '80s Hair Metal Band

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. The Facility Security Officer's Job, not mine

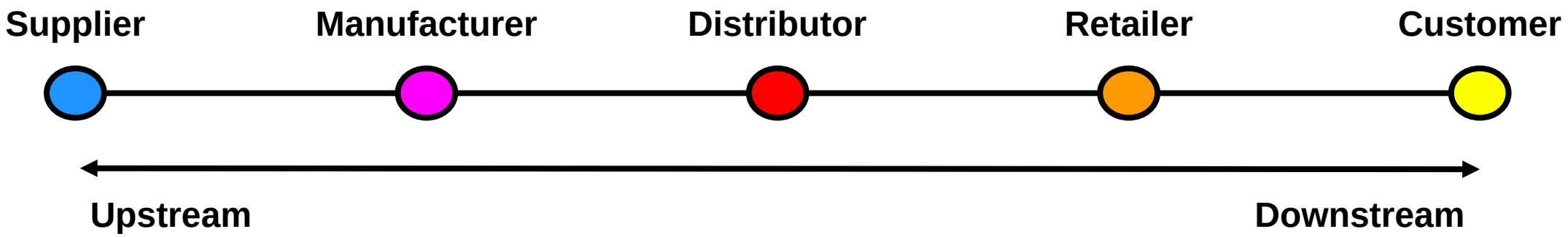
D. An '80s Hair Metal Band

WHAT IS A SUPPLY CHAIN?

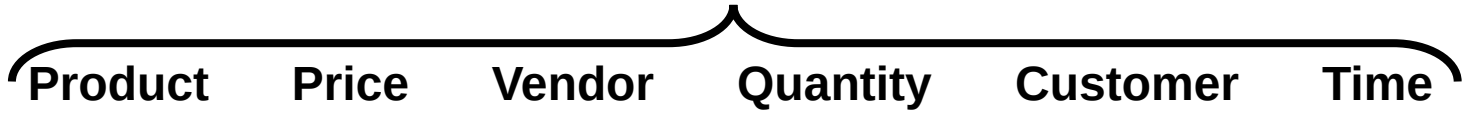
A system of organizations, people, activities, information, and resources involved in moving a product or service from supplier to customer. Supply chain activities involve the transformation of natural resources, raw materials, and components into a finished product that is delivered to the end customer.

SUPPLY CHAIN MANAGEMENT

Supply Chain Management: Oversight of the manufacturing, distribution, and transportation of a product from raw material to finished good



Matching supply and demand for profitability of goods and services requires the right:



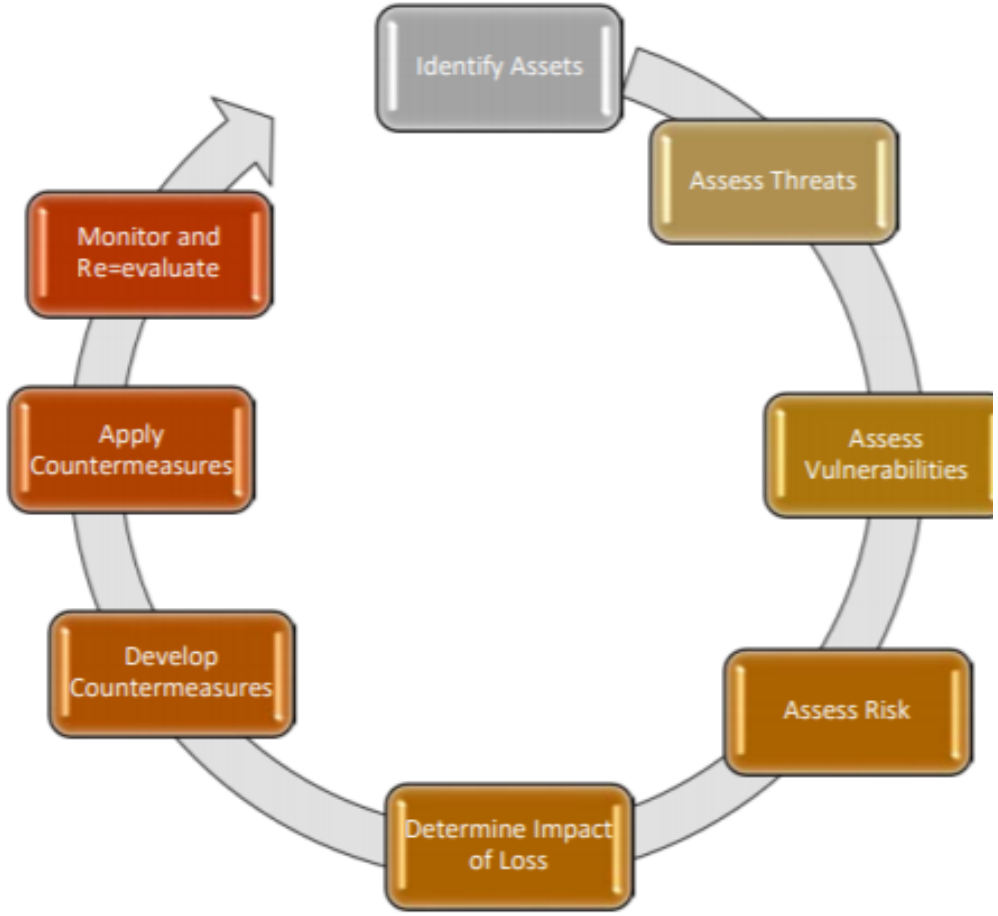
SUPPLY CHAIN RISK MANAGEMENT (SCRM)

A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats, whether presented by the supplier, the supplied product and its subcomponents, or the supply chain.

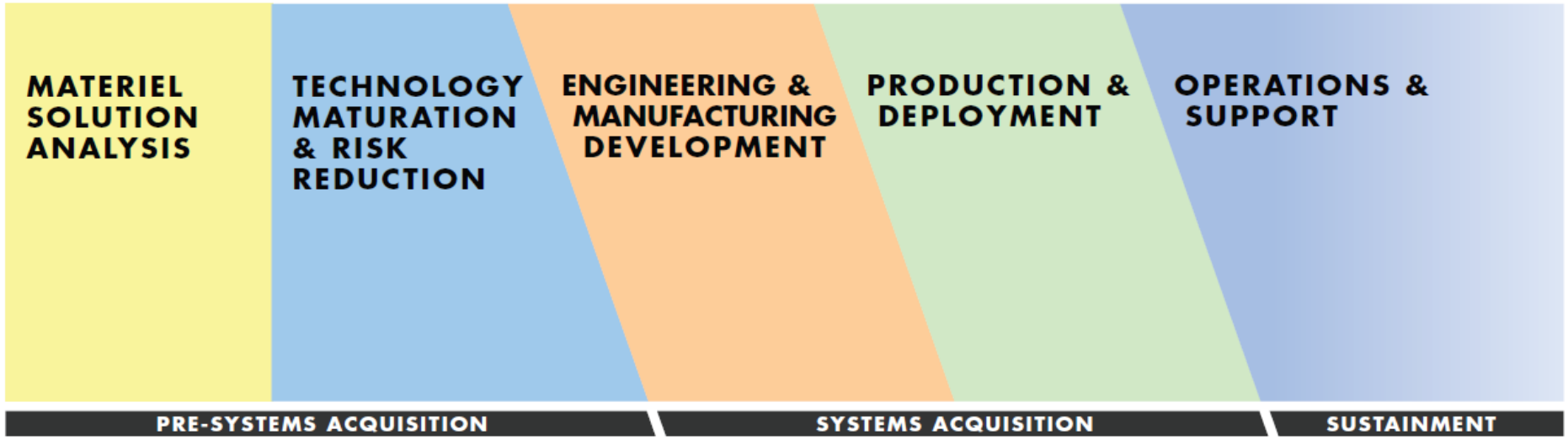
RISK MANAGEMENT PROCESS

Risk management is a multi-step process that provides a framework for collecting and evaluating information to:

- Identify assets
- Assess threats
- Assess vulnerabilities
- Determine impact of loss, damage, or compromise of assets
- Assess risks
- Develop countermeasures
- Apply countermeasures
- Monitor and re-evaluate



SCRM THREATS: THE ACQUISITIONS CYCLE



Foreign Intelligence Entity Methods of Operation

- Exploitation of Supply Chain
- Exploitation of Business
- Exploitation of Insider Access
- Exploitation of Cyber Operations
- Resume Submissions
- RFI/Solicitation
- Exploitation of Experts
- Attempted Acquisition of Technology
- Surveillance
- Theft
- Exploitation of Relationships
- Search/Seizure
- Exploitation of Security Protocols

LIFECYCLE

Supply Chain Risks exist across all phases of the life cycle

- CONCEPT
- DESIGN
- MANUFACTURE
- INTEGRATION
- DEPLOYMENT
- MAINTENANCE
- RETIREMENT

Some Methods of Supply Chain Disruption Include:

- Cyber intrusions on corporate systems and/or unwitting suppliers
- Co-opted suppliers
- Traditional Insider Threat methods
- Partnerships with criminal enterprises or adoption of their methods
- Governmental control over foreign suppliers
- Development of front companies (CONUS and OCONUS)

AUDIENCE POLL QUESTION #2

Which is a Supply Chain Threat?

A. Counterfeit Goods

B. War and Political Unrest

C. Cost Volatility

D. Tampering with Materiel

E. All of the Above

F. A and D Only

AUDIENCE POLL QUESTION #2

Which is a Supply Chain Threat?

A. Counterfeit Goods

B. War and Political Unrest

C. Cost Volatility

D. Tampering with Materiel

E. All of the Above

F. A and D Only

POTENTIAL METHODS OF INTRUSION

COUNTERFEIT	MALICIOUS INSERTION	TAMPERING	QUALITY ESCAPE	RELIABILITY FAILURE	EMERGING THREATS
Other than genuine and new devices from the legally authorized source, including relabeled, recycled, cloned, defective, out-of-spec, etc.	Insertion of malicious code/defect to enable attacks or cause mission failure; includes logic bombs, Trojan kill switches, & backdoors for control and access	Unauthorized extraction of intellectual property using reverse engineering, cyber means, embedded systems security weaknesses, etc.	Defect via mistake or negligence during design, production, and post production handling. May introduce a deficiency, vulnerability, &/or degrade life cycle performance	Mission failure in field due to factors unique to military and aerospace environment factors, such as particle strikes, device aging, hot spots, electro magnetic pulse, etc.	New threats, counterfeit trends, security attacks, and trust issues that combine two or more threats.

SIGNS OF A COMPROMISED SUPPLY CHAIN

- Exhibits functionality that was outside the original design
- A device, or multiple devices, from a lot that exhibits a unique error or failure
- Employees violating security protocols for handling of components or introducing non-compliant components
- Dealers offering rare or out of production components at low prices
- Dealers offering short lead times for large orders of components
- Shipping containers show signs of tampering

COUNTERMEASURES (1 OF 2)

- Periodically change procedures
- Educate your workforce & vendors on the importance of reporting suspicious anomalies
- Develop clear and detailed incident response procedures
- Investigate suspicious anomalies
- Maintain an incident tracking repository for analysis of historical data
- Encourage supplier site visits by CI personnel for CI Awareness Training
- Conduct Self-assessments
- Diversify product selection when possible

COUNTERMEASURES (2 OF 2)

- Continuously vet your vendors
- Stay apprised of vendor ownership changes
- Practice “need to know” with vendors
- Limit access to critical systems
- Educate yourself on how vendors protect your data on their networks
- Consistently use anti-tamper & tracking technology
- Pay close attention to shipping schedules
- Know who’s touching your materials/shipments
- Use trusted U.S. manufacturers, builders, & installers where possible
- Consideration of CI Awareness Training requirement in contracts

REPORTING

The introduction of counterfeit or malicious products or materials into the supply chain to gain unauthorized access to classified information, to alter data, disrupt operations, or to interrupt communications related to classified contracts or cleared facilities constitutes a “suspicious contact” and is reportable by cleared companies to DCSA as per the National Industrial Security Program Operating Manual (NISPOM) (32 Code of Federal Regulations (CFR) Part 117).

AUDIENCE POLL QUESTION #3

What's Reportable?

A. Multiple Products from the Same Lot Experiencing Degraded Capability, Errors, and/or Premature Failure

B. Broken Chain of Custody from a Supplier

C. Purchased Software Pinging (trying to connect to) a Foreign Military's Internet Protocol (IP) Address

D. My Microelectronics Chasing Me Through the Facility With a Knife Shouting Red Rum!

E. All of the Above

AUDIENCE POLL QUESTION #3

What's Reportable?

A. Multiple Products from the Same Lot Experiencing Degraded Capability, Errors, and/or Premature Failure

B. Broken Chain of Custody from a Supplier

C. Purchased Software Pinging (trying to connect to) a Foreign Military's Internet Protocol (IP) Address

D. My Microelectronics Chasing Me Through the Facility With a Knife Shouting Red Rum!

E. All of the Above

EXAMPLES OF REPORTABLE ACTIVITY

- Devices that exhibit functionality that was outside the original design
- A device, or multiple devices from a lot, that exhibits a unique error or failure
- Inadvertent or deliberate attempts to break a trusted chain of custody
- Introduction of counterfeit components into a U.S. Government system during production
- Unauthorized personnel of any nationality accessing restricted areas of a cleared facility involved in the production of components for DOD systems
- Efforts by any individual, regardless of nationality, to compromise a cleared employee involved in manufacturing, assembling, or maintaining DOD systems

INTERACTIVE SELF ASSESSMENT

- Acquisition
- Design/Development
- Logistics
- Policy/Procedures

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

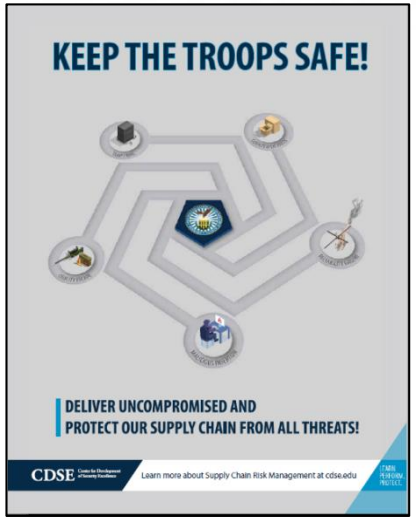
SCRM SELF-ASSESSMENT (1 OF 2)

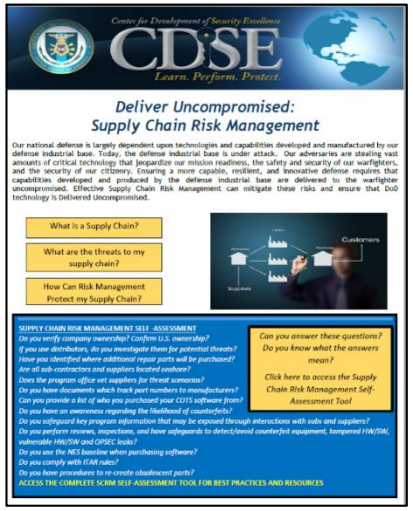
- Do you verify company ownership? Confirm U.S. ownership?
- If you use distributors, do you investigate them for potential threats?
- Have you identified where additional repair parts will be purchased?
- Are all subcontractors and suppliers located onshore?
- Does the program office vet suppliers for threat scenarios?

SCRM SELF-ASSESSMENT (2 OF 2)

- Do you have documents which track part numbers to manufacturers?
- Can you provide a list of who you purchased your Commercial Off the Shelf (COTS) software from?
- Do you have an awareness regarding the likelihood of counterfeits?
- Do you use the National Institute of Science and Technology (NIST) baseline when purchasing software?
- Do you comply with ITAR rules?

RESOURCES





[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]

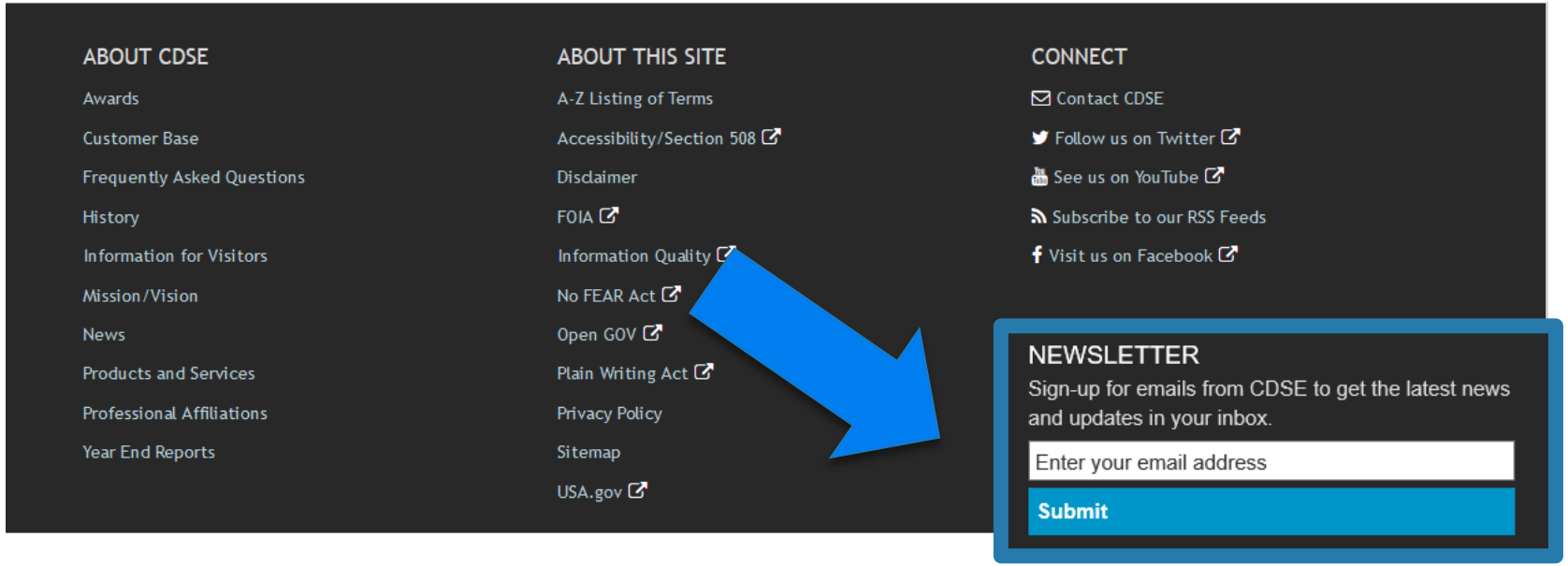
[Cybersecurity Supply Chain Toolkit]

[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!



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 14	Meet the DITMAC: An Overview of Analysis & Mitigation, the Enterprise Program Management Office, Unauthorized Disclosure Program Management Office, and Performance & Metrics
April 29	Supply Chain Due Diligence
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

DCSA Hanover Field Office
Mark Zahner
mark.e.zahner.civ@mail.mil