



Supply Chain Risk Management

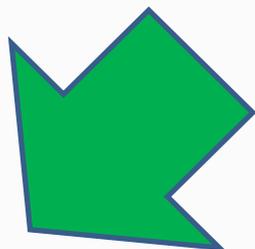
Operating ahead of the threat, not behind the vulnerabilities



Navigation in the Meeting Room



Notes box for audio information and other announcements

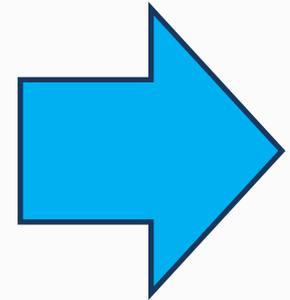


To enlarge the slide, click on the Full Screen button. To get out of Full Screen view, select Full Screen again. You will need to be out of Full Screen view to enter question responses.

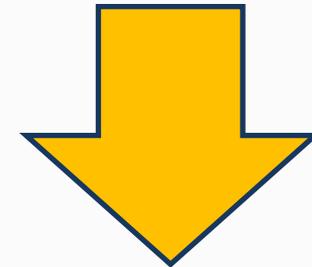


Navigation in the Meeting Room

Q&A box for entering questions to the presenters

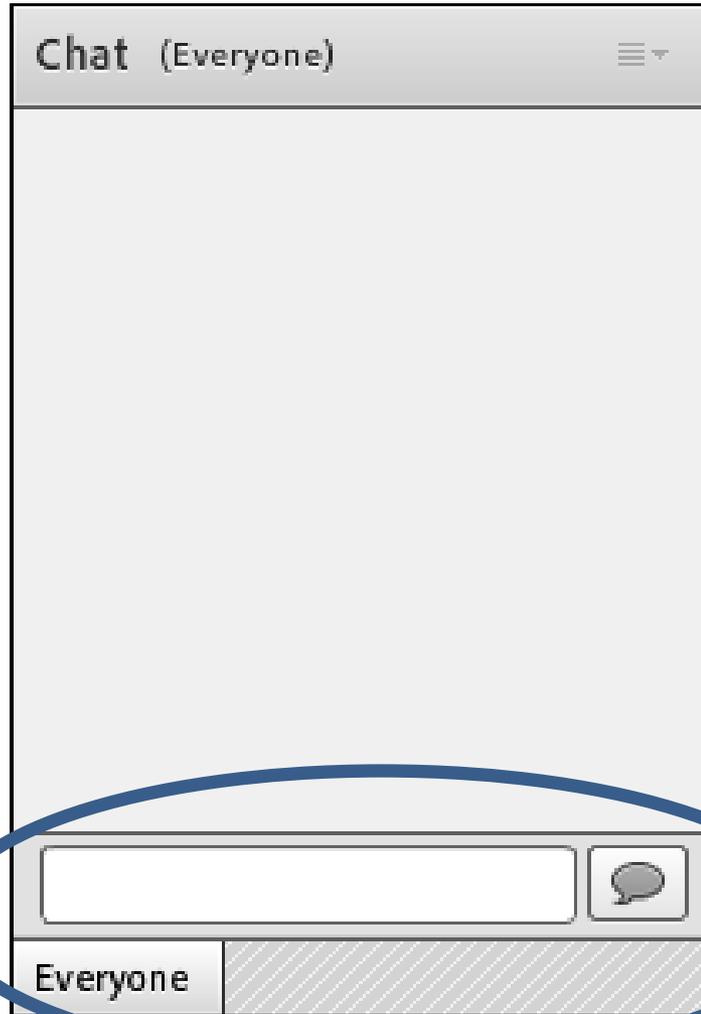


File share box to download resources relevant to today's presentation





Example of a Chat Question





Supply Chain Risk Management

Operating ahead of the threat, not behind the vulnerabilities



Agenda

- Introduction
- Supply Chains
- How is risk evaluated?
- Threat as an Element of Risk
- U.S. Government Requirements
- DoD Elements Involved with SCRM
- Summary





Supply Chain Threats

“Our adversaries are very active in trying to introduce material into the supply chain...to collect [intelligence] and disrupt U.S. military operations”

Mr. Shedd, Deputy Director, Defense Intelligence Agency



Adversary Activity

- The Air Force reported an unknown number of counterfeit aircraft parts had been fastened into U.S. military weapons systems after infiltrating supply depots.
- In 2010, the FBI seized \$143 million of counterfeit Cisco network hardware.
- While probing DoD's vulnerability to counterfeit parts, the GAO identified problems with microprocessors used in F-15 flight control computers, oscillators used for Global Positioning Systems navigation on more than 4,000 Air Force and Navy systems.



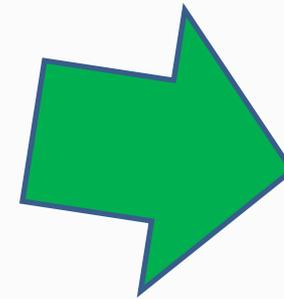
Introduction

- Globalization creates opportunity for foreign intelligence entities (FIE) to operate in a new battle space.
- The Department of Defense (DoD) is reliant on companies with global supply chains.
- The U.S. Government and DoD are focused on mitigating risks to supply chains.
 - U.S. Law
 - Defense Federal Acquisition Regulation
 - Intelligence Community Directives



Chat Question 1

What is Supply Chain Risk?



Enter your response in the Chat box.



What is Supply Chain Risk?

Supply Chain Risk: The risk that adversaries will insert malicious code into or otherwise subvert the design, manufacturing, production, distribution, installation, or maintenance of information and communications technology (ICT) components that may be used in DoD systems to gain unauthorized access to data, to alter data, to disrupt operations, or to interrupt communications.

Directive Type Memorandum (DTM) 09-016



What is Supply Chain Risk Management?

Supply Chain Risk Management: The management of supply chain risk whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., packaging, handling, storage, and transport).

DTM 09-016



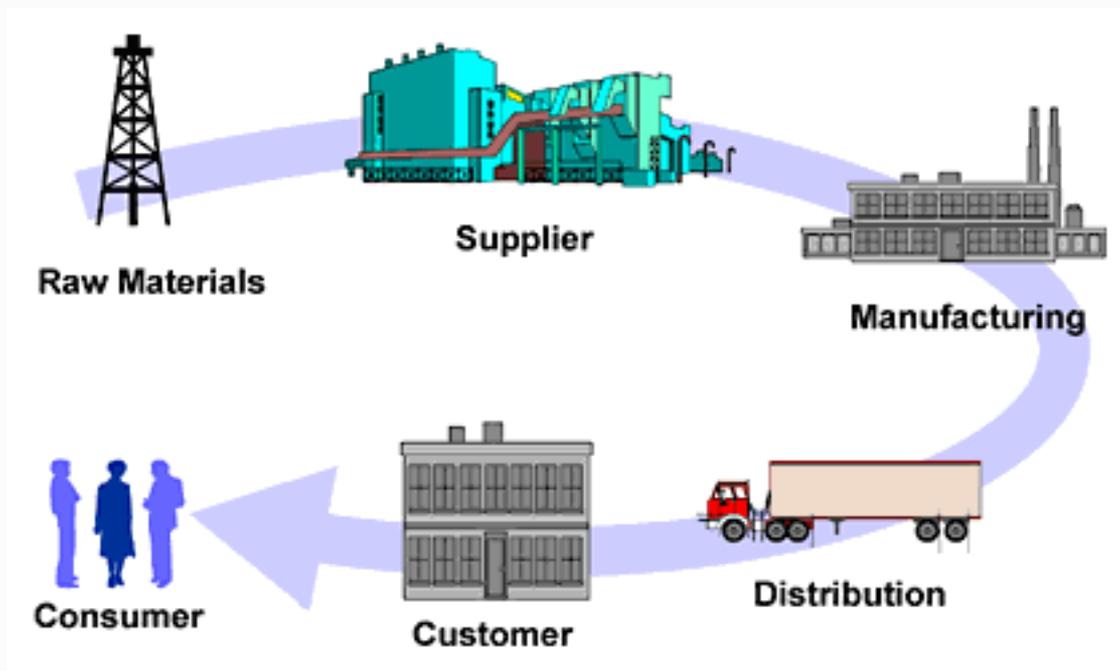
Intelligence Community Directive 731

Supply chain risk management is the 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 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.

Intelligence Community Directive 731



From Beginning to End



Credit: Weber State University, Student Association of Supply Chain Management

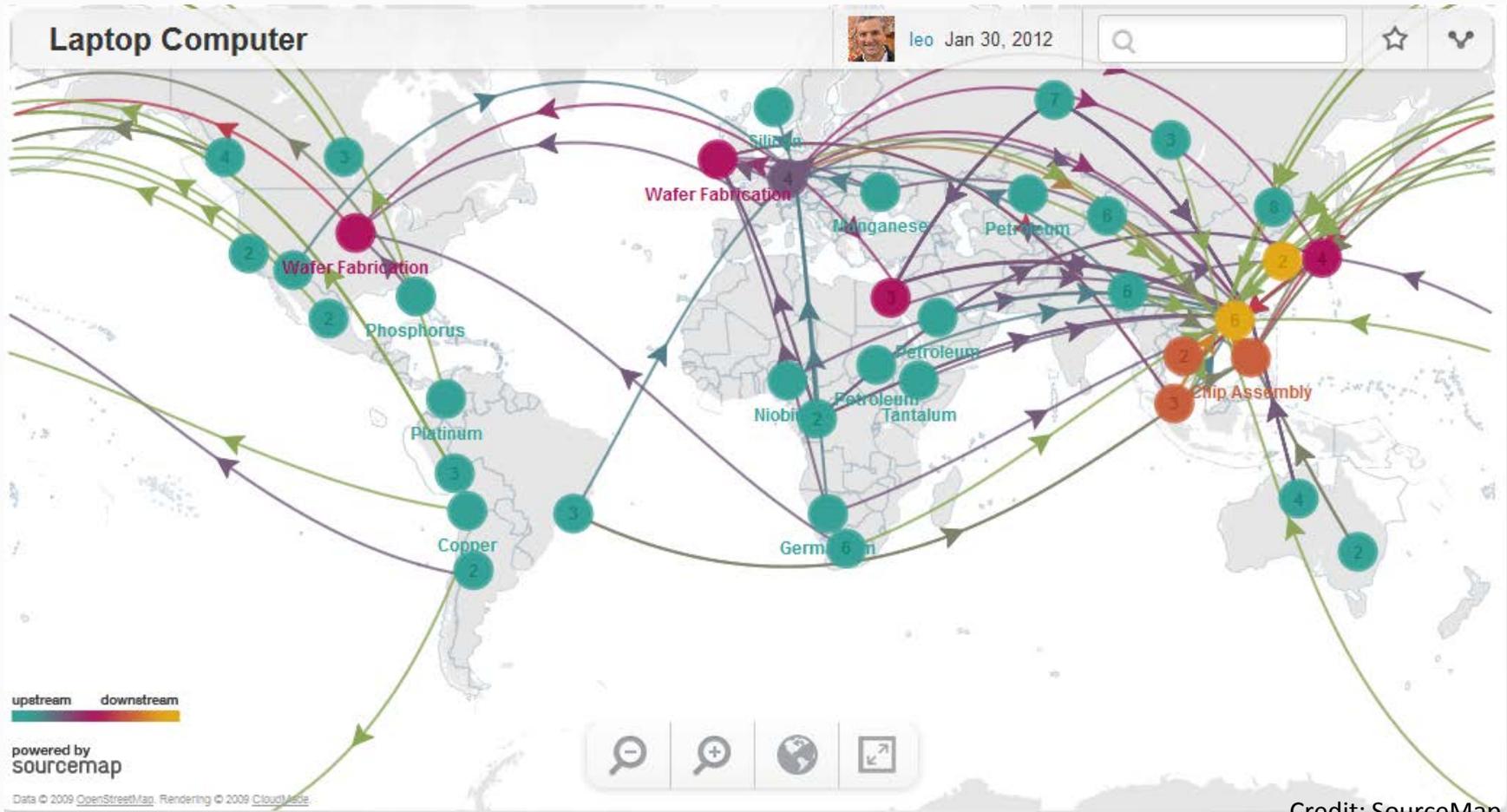


Dell Headquarters





A Laptop Supply Chain



Credit: SourceMap



Information Flow in Supply Chains

Upstream: From raw materials to consumer

- Production statuses, production outputs, inventory levels, delivery schedules

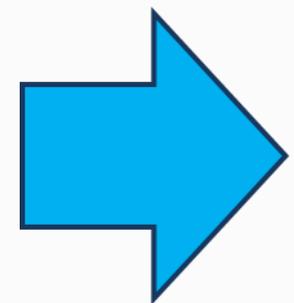
Downstream: From consumer to raw materials

- Contracts, orders, return requests, personal information, payments



Chat Question 2

How do we evaluate risks associated with the global supply chain?



Enter your response in the Chat box.



How do we evaluate the risks?

- Incorporation of all-source analysis into assessments
- Processes to assess threats from potential suppliers
- Processes to control the quality, configuration, and security
- Processes to detect the occurrence, reduce likelihood, and mitigate the consequences



Threat as an Element of Risk

Foreign Intelligence Entity (FIE)

Known or suspected person or group that conduct intelligence activities to

- Collect U.S. information
- Block or impair U.S. intelligence collection
- Influence U.S. policy
- Disrupt U.S. systems or programs





Government SCRM actions

Chinese telecom companies Huawei and ZTE

- U.S. blocks acquisitions, mergers, or take overs of U.S. firms and eliminates the technology from U.S. systems and programs
- UK recommends close monitoring
- Australia bans bids on government contracts
- India mandates testing of commercial products





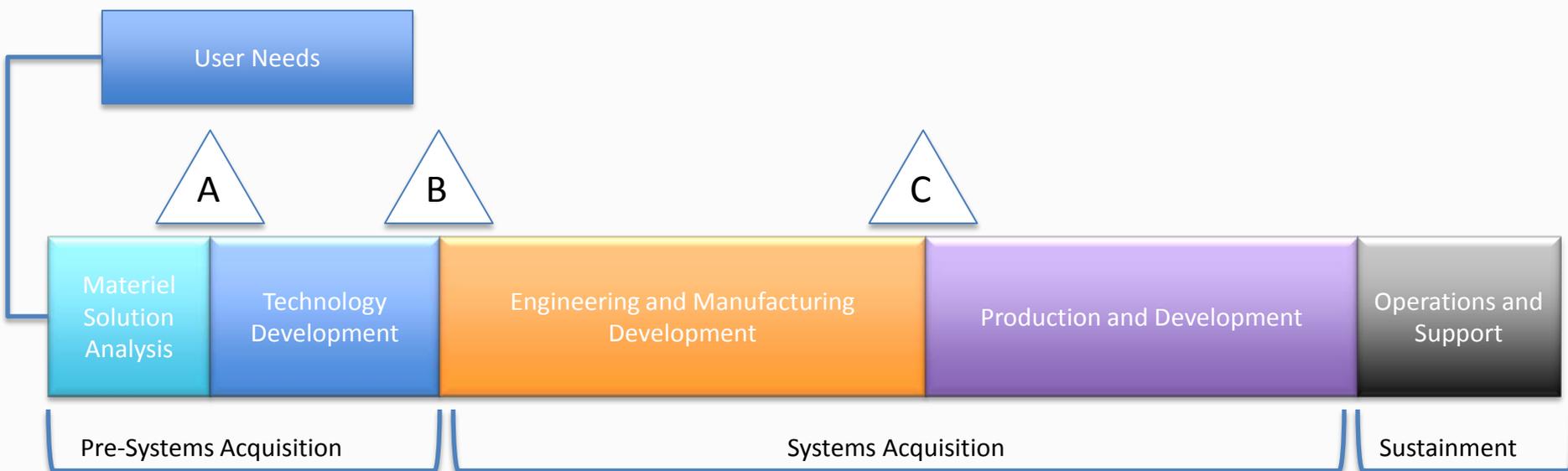
U.S. Government Requirements

- 2009 Comprehensive National Cyber Security Strategy
- 2011 National Defense Authorization Act (NDAA), Section 863
- 2012 NDAA, Section 818 (c) (3)
- Intelligence Community Directive 731, Supply Chain Risk Management





DoD Acquisition Programs SCRМ





DoD Elements Involved with SCRM

- DIA Supply Chain Risk Management, Threat Analysis Center
- Defense Security Service – in partnership with Service and Defense Agencies



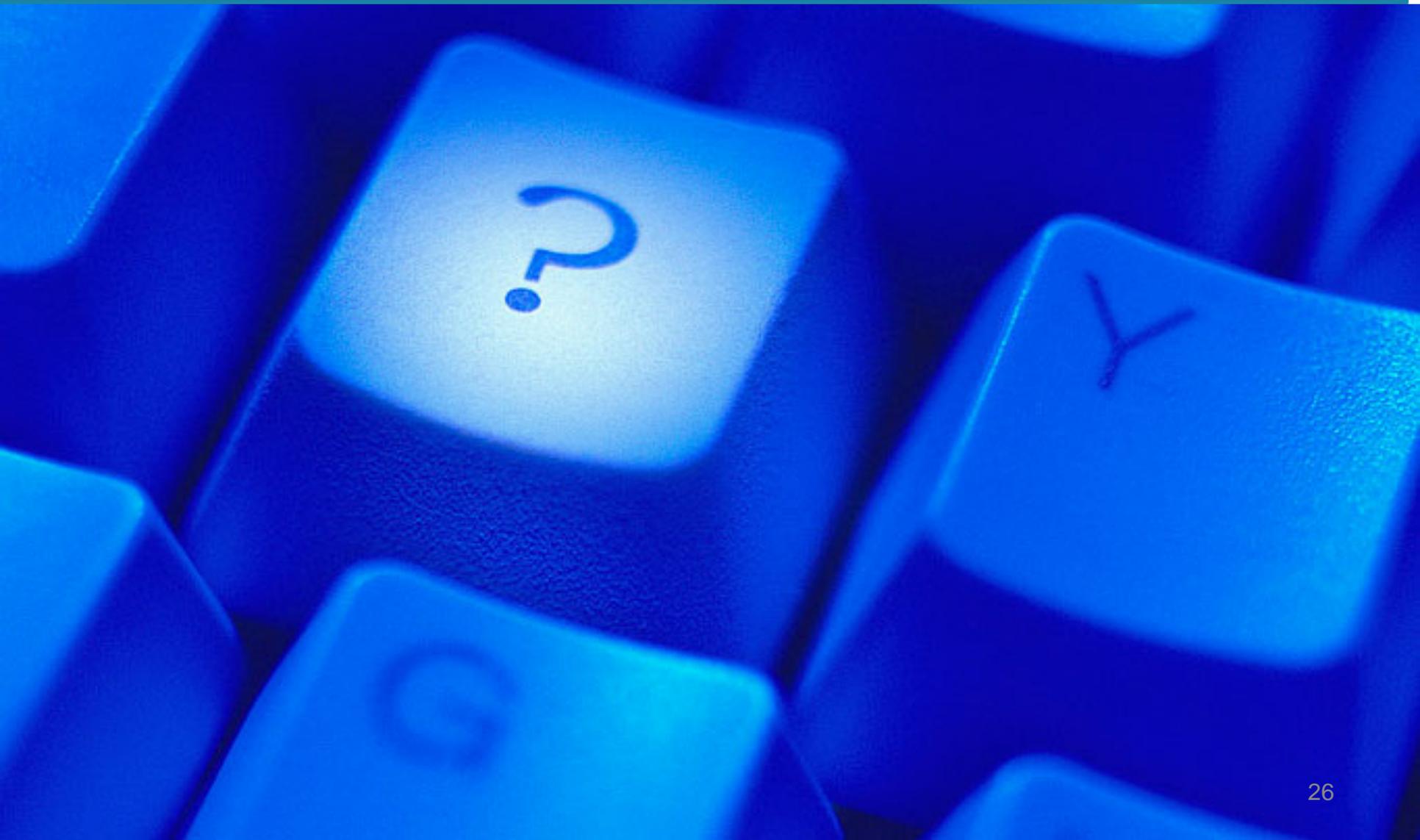


Summary

- SCRM is a proactive approach to identifying risk before it can impact a defense acquisition program
- Good SCRM reduces uncertainty
- The DoD is focused on mitigating supply chain risk for national security systems and major weapon systems
- Numerous DoD organizations play a role in informing decision makers on supply chain risk



Questions





Survey





Contacts and Resources

Contact CDSE at

counterintelligence.training@dss.mil

CI Training:

<http://www.cdse.edu/catalog/counterintelligence.html>

CI Products:

http://www.dss.mil/isp/count_intell/index.html