



# Principles of Supply Chain Risk Management (SCRM)

Van Poindexter  
Professor of Production and Logistics Management  
DAU, South Region



# The supply chain

The supply chain is the distributed and interconnected web of people, processes, technology, information, and resources that creates and delivers a product or service



Dependence on ICT, commercialization, and globalization trends



# SCRM – What is it?...why do we need it?

**Supply chain risk management (SCRM)** is "the implementation of strategies to manage both everyday and exceptional risks along the **supply chain** based on continuous **risk** assessment with the objective of reducing vulnerability and ensuring continuity".

Wieland, A., Wallenburg, C.M., 2012. [Dealing with supply chain risks: Linking risk management practices and strategies to performance](#). International Journal of Physical Distribution & Logistics Management, 42(10).



# Areas to explore/consider

- SCRM is a cyber-issue, but also consider these:
  - SCRM certainly includes IT/cyber vulnerabilities
  - DMSMS
  - Counterfeit Parts
  - vanishing vendors (particularly at the lower tiers of the supply chain), globalization,
  - unintended consequences of high velocity "just in time" supply chains,
  - weather
  - labor unrest
  - national unrest that disrupts critical resources
  - terrorism, etc.
- Additive Manufacturing site - <https://acc.dau.mil/am>

# ICT global supply chain complexity

- Supply chains comprise interconnected webs around the world
- Components that end up in any ICT product have their own supply chains



Sabotage and espionage in the supply chain environment

# Threats to ICT components

- Supply chains offer adversaries attack vectors for cyber exploitation and manipulation
- ICT components are susceptible to both intentional and unintentional threats



Sabotage and espionage in the supply chain environment

# Vulnerabilities of ICT components

- Software and hardware are increasingly complex and interdependent
- Manufacturers use components from unknown sources
- Software developers create software from code created by third-party and unknown sources



Sabotage and espionage in the supply chain environment



# INSIGHT

September-October 2015 Vol. 13 No. 4

The Official Newsletter of the Defense Acquisition University

- 3 DAU's 13th Annual Corporate Recognition Awards
- 6 DAU Mentoring Program
- 12 Talent Management Planning
- 14 Due Dates for the Calendar Year 2016 Tuition Assistance Program
- 15 2015 Acquisition Insight Focus Days
- 17 PEO EIS Navy Tailored Training Focuses on Leadership
- 18 Five DAU Members Attended 4th Estate Acquisition Leadership Challenge II
- 21 Major Takeaways: Increasing Productivity
- 22 Better Outcomes Through Customization

## Cybersecurity

Recent cybersecurity breaches, such as the Office of Personnel Management breach that reportedly affected more than 21 million government employees, have brought cybersecurity to the forefront in the DoD. While our networks and critical infrastructure face grave danger in the cybersecurity arena, perhaps a misunderstood and even bigger issue is the cybersecurity threat faced by all acquisition programs, from aircraft, to tanks, to guided missiles. Indeed, any program or system that communicates digitally is vulnerable to the cybersecurity threat. Cybersecurity affects all acquisition career fields, and it is a design consideration that must be addressed throughout the program life cycle.

In response to the growing cybersecurity threat and relat-

many acquisition programs are struggling to follow these new policies and address programmatic cybersecurity challenges. The DoD is looking to DAU and other organizations to meet massive acquisition cybersecurity training needs.

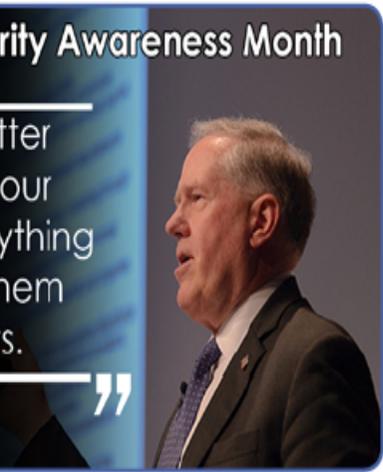
According to its Vision Statement, DAU seeks to "Enable the Defense Acquisition Workforce to

### National Cybersecurity Awareness Month

“ We must do a better job of protecting our systems and everything associated with them from cyber threats.

”

USD(AT&L) Frank Kendal



# Comprehensive National Cybersecurity Initiative (CNCI)

Focus Area 1

Trusted Internet Connections

Deploy Passive Sensors Across Federal Systems

Pursue Deployment Of Intrusion Prevention System  
(Dynamic Defense)

Coordinate And Redirect R&D Efforts

Establish A Front Line Of Defense

Focus Area 2

Connect Current Centers To Enhance Cyber Situational Awareness

Develop A Government Wide Cyber Counterintelligence Plan

Increase The Security Of The Classified Networks

Expand Education

Demonstrate Resolve To Secure U.S. Cyberspace & Set Conditions For Long-term Success

Focus Area 3

Define and Develop Enduring Leap Ahead Technology, Strategies & Programs

Define and Develop Enduring Deterrence Strategies & Programs

**SCRM**  
Develop Multi-pronged Approach For Global Supply Chain Risk Management

Define The Federal Role For Extending Cybersecurity Into Critical Infrastructure Domains

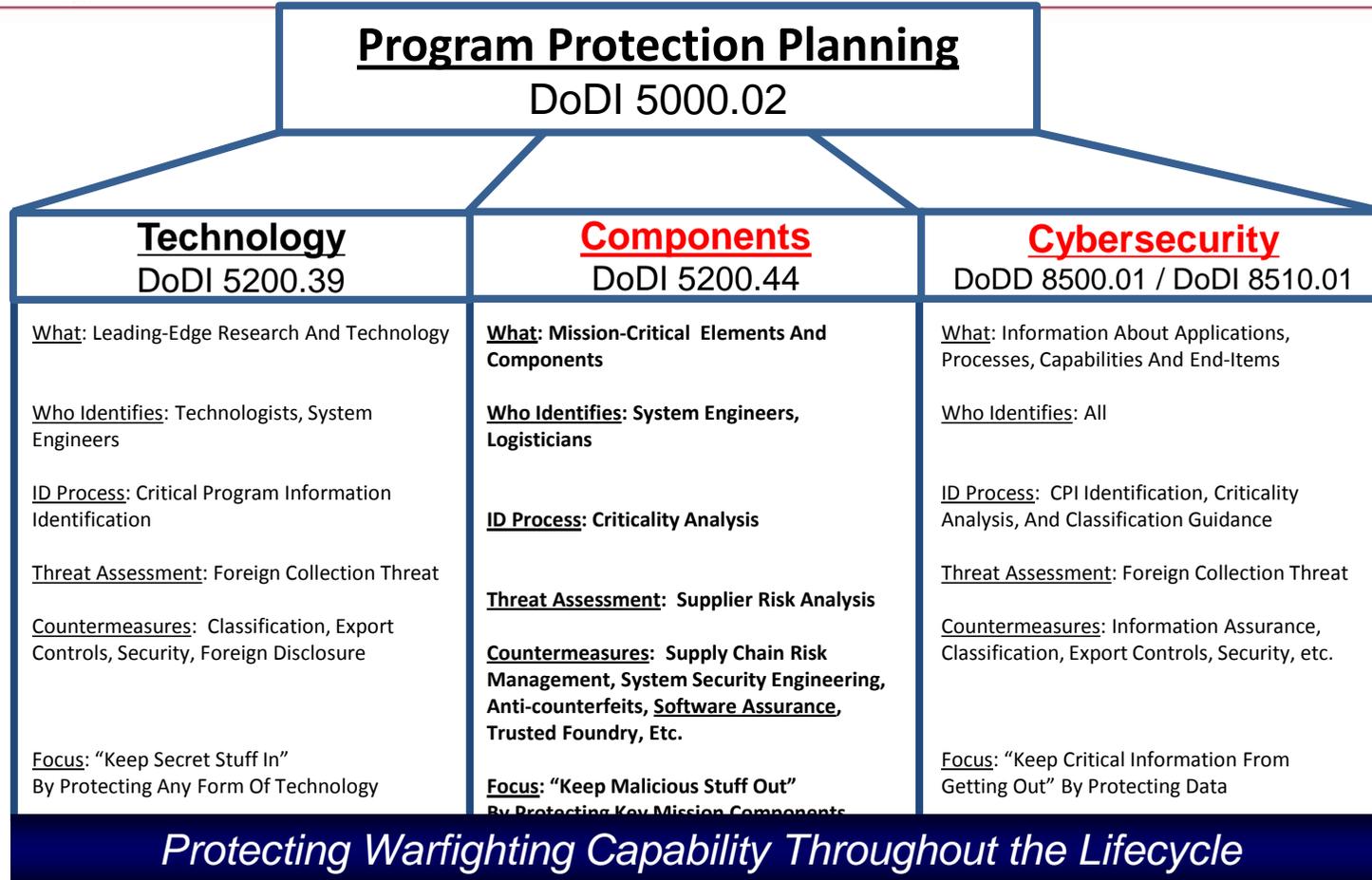
Shape The Future Environment To Demonstrate Resolve To Secure U.S. Technological Advantage And Address New Attack And Defend Vectors

CNCI Signed in 2008 by President Bush >> DOD Strategy for Trusted Systems and Networks (TSN)





# So What is DOD doing about it?





# DoDI 5200.44

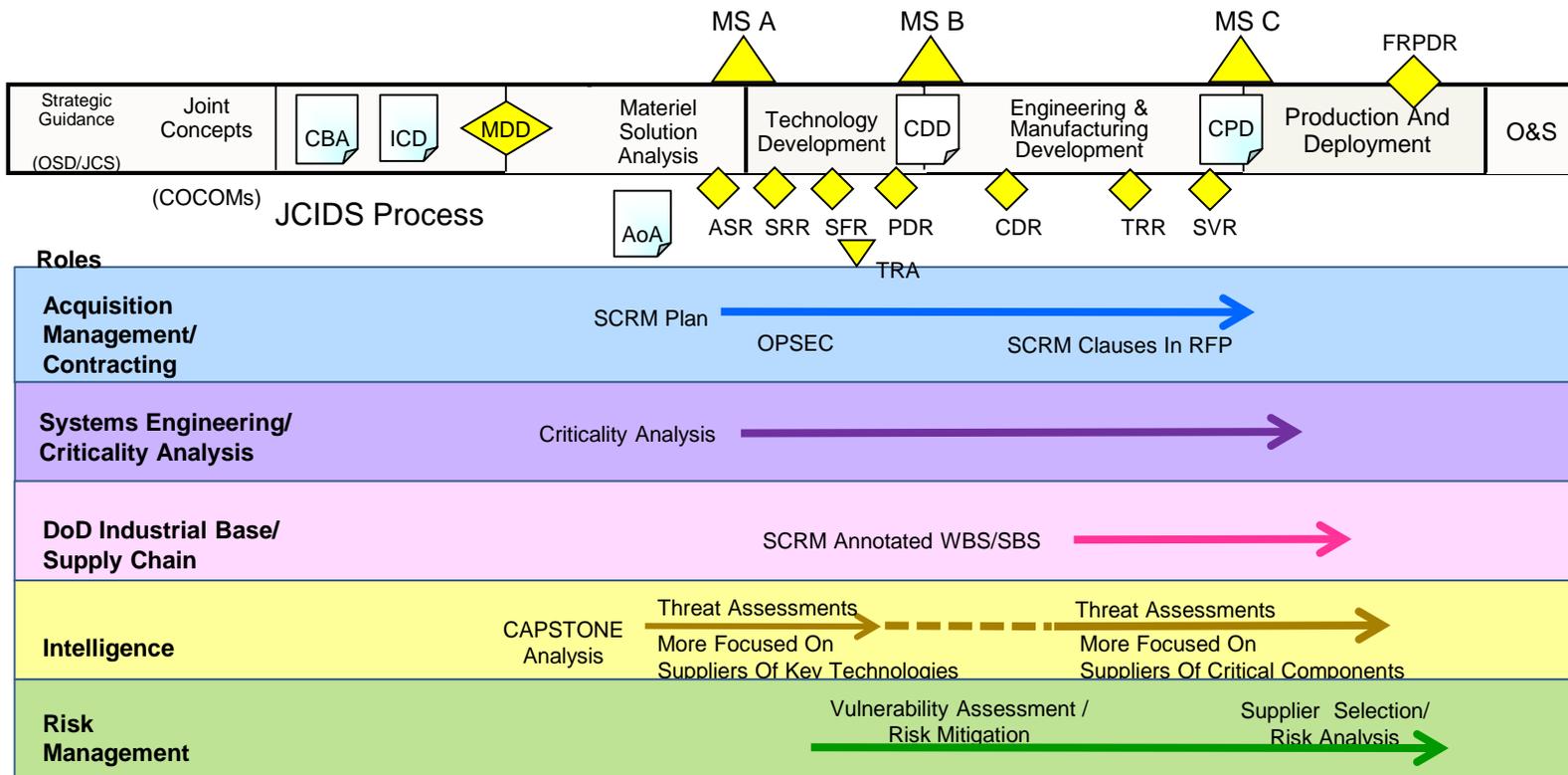
## Trusted Systems And Networks

• **Purpose:** Minimize The Risk That Warfighting Capability Will Be Impaired Due To Vulnerabilities In System Design Or Subversion Of Mission Critical Functions Or Components

- **Scope:** All DoD Information Systems And Weapons Systems That Are Or Include:
  1. National Security Systems As Defined By Section 3542 Of Title 44;
  2. Mission Assurance Category (MAC) I Systems; Or
  3. Other DoD Information Systems That The DoD Component's Acquisition Executive Or Chief Information Officer Determines Are Critical To The Direct Fulfillment Of Military Or Intelligence Missions
  
- **Key Effects:**
  - **Manage Risk Of Critical Function And Component Compromise Throughout Lifecycle**
    - Criticality Analysis Is The Systems Engineering Process For Focusing Activities
    - Mitigations: SCRM, Software Assurance, Secure Design
  - **Use All-Source Intelligence Analysis To Inform Procurement Decisions**
  - **Codify Trusted Foundry Requirement For DoD-Unique ASICs**
  - **Detect Vulnerabilities Within Hardware And Software Through Test And Evaluation, Including Developmental, Acceptance, And Operational Testing**
  - **Document Planning And Accomplishments In PPP And IA Strategy**
  - **Establishes Focal Points In All DoD Components**
    - Conduit To Enterprise Risk Management Capabilities (e.g. DIA SCRM TAC)
    - Offers Guidance On Mitigation

# Ex. - AMRDEC Capability Aligns With SCRM Across The System Lifecycle

www.DAU.mil





## Input Analysis Results:

### Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF1	Processor X	II	Redundancy
	CF2	SWModule Y	I	Performance
Mission 2	CF3	SWAlgorithm A	II	Accuracy
	CF4	FPGA123	I	Performance

### Vulnerability Assessment Results

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploitability	System Impact (I, II, III, IV)	Exposure
Processor X	Vulnerability 1	Low	II	Low
	Vulnerability 4	Medium		Low
SWModule Y	Vulnerability 1	High	I	High
	Vulnerability 2	Low		Medium
	Vulnerability 3	Medium		Low
	Vulnerability 6	High		Low
SWAlgorithm A	None	Very Low	II	Very Low
FPGA123	Vulnerability 1	Low	I	High
	Vulnerability 23	Low		High

### Threat Analysis Results

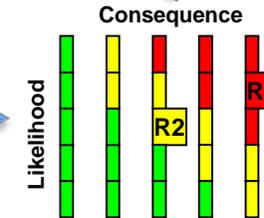
Supplier	Critical Components (HW, SW, Firmware)	TAC Findings
Supplier 1	Processor X	Potential Foreign Influence
	FPGA123	Potential Foreign Influence
Supplier 2	SWAlgorithm A	Supplier Vulnerabilities
	SWModule Y	Supplier Vulnerabilities

**Risk Mitigation And Countermeasure Options**

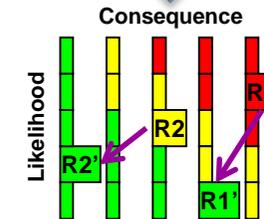
Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

## Initial Risk Posture



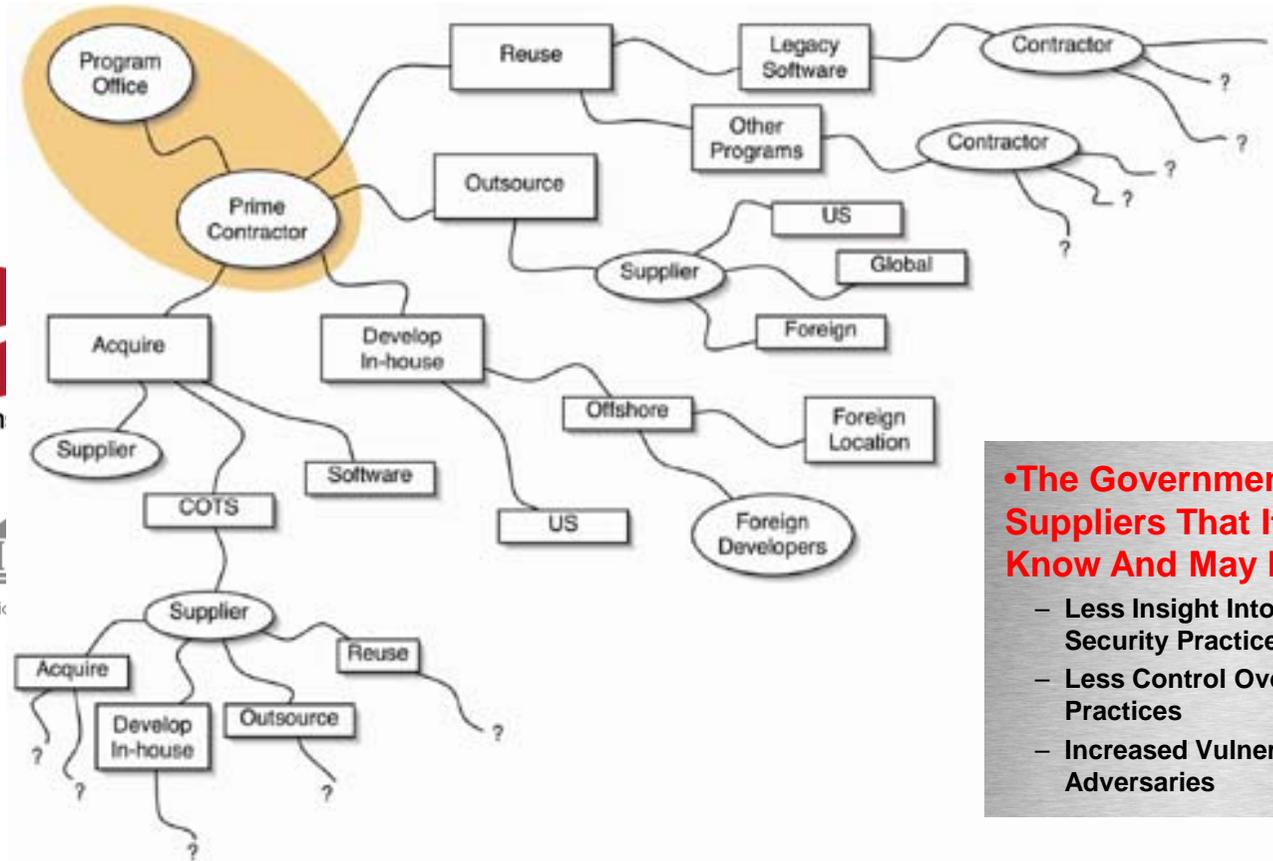
## Risk Mitigation Decisions



# Managing risk

- Risks to the ICT global supply chain, like the risk of contracting the flu, require an assessment of threat and vulnerability, likelihood and potential impact, and the risks associated with critical components, systems, and networks
- Supply chain risks, like exposure to the flu virus, are inevitable and cannot be eliminated, so they must be managed
- Things like globalization, commercialization, JIT, etc. are all good, but introduce their own forms of risk

# Globalization Is Good, But It Brings Challenges



Defen



Foundatic

**•The Government Has Suppliers That It May Not Know And May Never See**

- Less Insight Into Suppliers' Security Practices
- Less Control Over Business Practices
- Increased Vulnerability To Adversaries

"Scope Of Supplier Expansion And Foreign Involvement" Graphic In DACS [www.softwaretechnews.com](http://www.softwaretechnews.com) Secure Software Engineering, July 2005 Article "Software Development Security: A Risk Management Perspective" Synopsis Of May 2004 GAO-04-678 Report "Defense Acquisition: Knowledge Of Software Suppliers Needed To Manage Risks"



# U.S. influence on industry

- The U.S. Government is a large user of commercial ICT, but it no longer has the largest share of the market
- While DoD is concerned about the security and integrity of ICT components, other purchasers are more concerned about the logistical aspects of the supply chain
- In response to global market forces and consumerism, DoD is playing a role in developing industry standards



i n v e n t



Dependence on ICT, commercialization, and globalization trends

# Commercialization and globalization

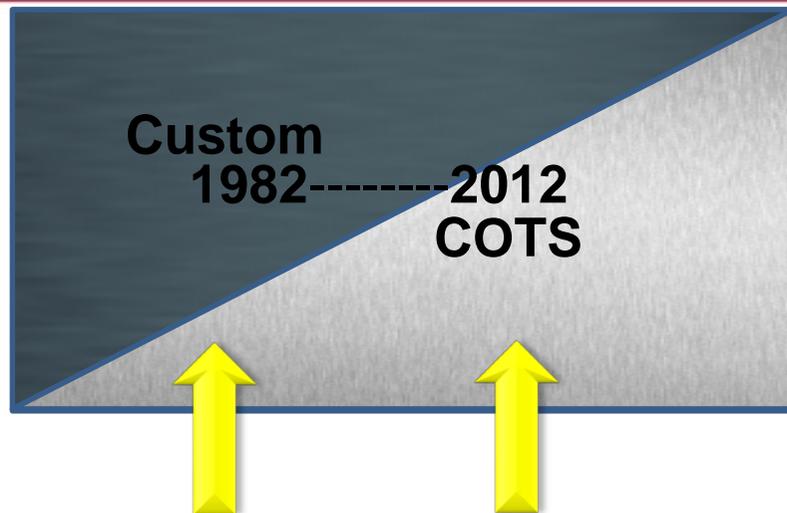
- The bulk of U.S. Government ICT is obtained from global and commercial suppliers
- Commercial products can be purchased at lower cost and increase access to innovation and operational efficiency
- Commercial product risk (e.g., tampering and counterfeit components) is increased by foreign or unknown sourcing



Dependence on ICT, commercialization, and globalization trends



# DOD's Supply Chain Commercialization



*"This is a trend the department has frankly been willing to recognize more in policy than in practice...I'd hazard a guess that 25 years ago, 70 percent of the goods and services the department procured were developed and produced exclusively for the military. Today, that ratio has reversed. Seventy percent of our goods and services are now either produced for commercial consumption or with commercial applications in mind. And it's backed by a largely commercial-based supply chain."*

*– Mr Brett Lambert, DASD for Manufacturing and Industrial Base Policy*



# Ensuring Confidence In Defense Systems

- ***Threat: Nation-state, Terrorist, Criminal, Or Rogue Developer Who:***
  - Gain Control Of Systems Through Supply Chain Opportunities
  - Exploit Vulnerabilities Remotely
- ***Vulnerabilities***
  - All Systems, Networks, And Applications
  - Intentionally Implanted Logic
  - Unintentional Vulnerabilities Maliciously Exploited (e.g., Poor Quality Or Fragile Code)
- ***Traditional Consequences: Loss Of Critical Data And Technology***
- ***Emerging Consequences: Exploitation Of Manufacturing And Supply Chain***
- ***Either Can Result In Corruption; Loss Of Confidence In Critical Warfighting Capability***

## ***Today's Acquisition Environment Drives The Increased Emphasis:***

### Then

Stand-alone Systems

Some Software Functions

Known Supply Base

CPI (Technologies)

### Now

>>> Networked Systems

>>> Software-intensive

>>> Prime Integrator, Hundreds Of Suppliers

>>> CPI And Critical Components



# DOD Strategy For Trusted Systems And Networks/SCRM

- 1. Understand System Criticality And Prioritize Limited Resources**
  - Focus On National Security Systems: Mission Critical Systems (MAC I) And Classified Networks
- 2. Within Priority Systems, Strengthen Systems Security Engineering Practices To Identify And Protect Mission Critical Functions And Their Critical Components**
- 3. For Critical Components, Utilize All-source Supply Chain Threat Assessments From DIA SCRM Threat Assessment Center To Inform Risk Management Strategies**
- 4. Manage Risk To Critical Components Throughout The Acquisition Lifecycle Through Acquisition *Program Protection* And SCRM By:**
  - Proactive SCRM Key Practices To Strengthen Acquisition Operations Security
  - Trusted Supply Chain For DoD Unique Application Specific Integrated Circuits (ASICs)
  - Employ Technical Mitigations And Enhanced Vulnerability Detection
- 5. Partner With Industry To Drive Security (Manufacturing, Engineering, Test And Evaluation, etc.)**





# Supply Chain Linkage Attack Vectors

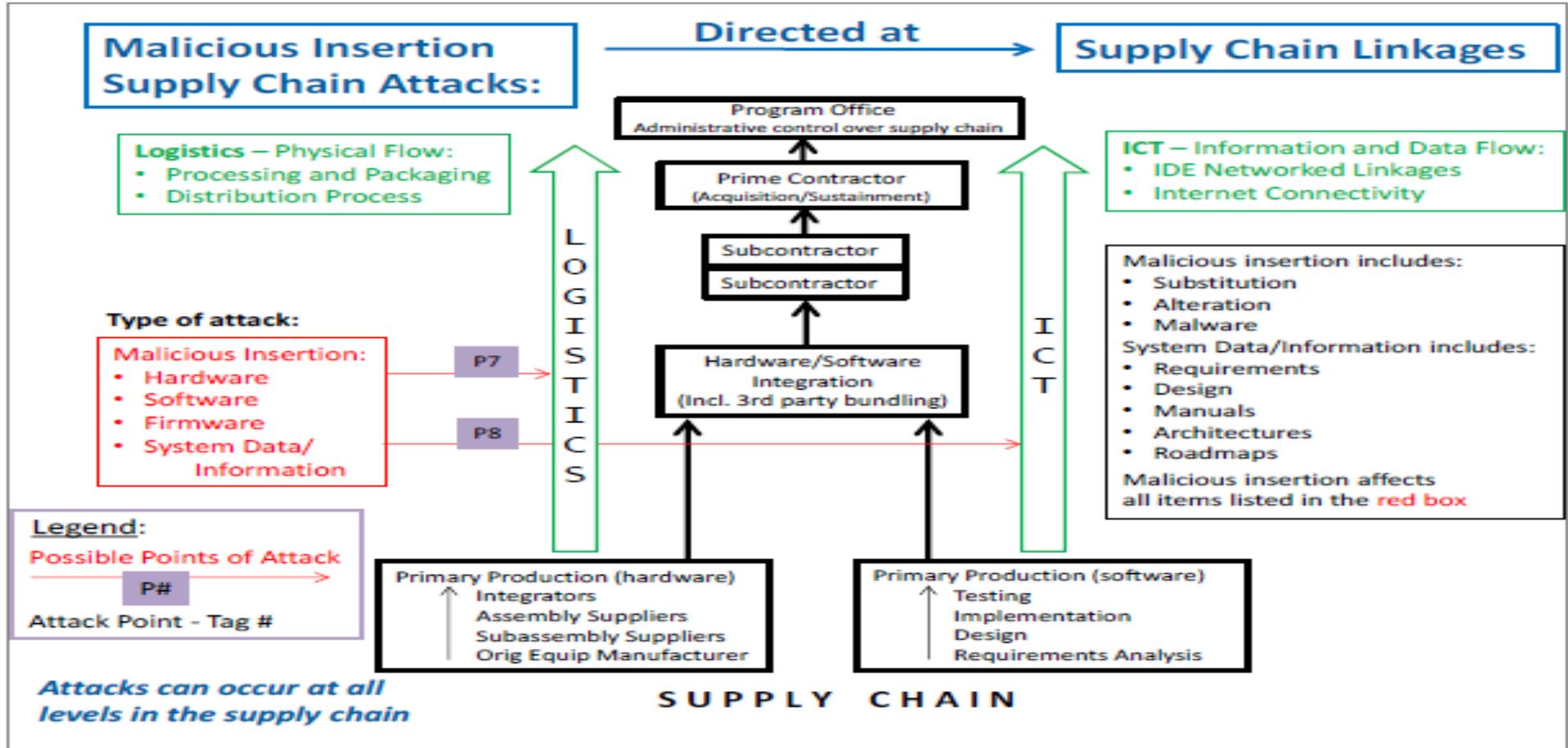


Figure 2. Points of Attack – Supply Chain Linkages



## How do we solve this?

- Partnering with Suppliers – it's in both our best interests
- Do the hard things first – Hon. Mr Frank Kendall contends that DOD activities are inherently risk averse and therefore advocates focusing on the big rocks, and not just the low-hanging fruit, to show they are moving the ball down the field
- Treat risks like issues – requires identification, planning, mitigation, and investment (dollars, people, time)



## DAU is on a sprint to get word out

---

- Three articles discussing cybersecurity and SCRM
- Infusing cybersecurity awareness in current courseware
- DAU South has hired two cybersecurity faculty