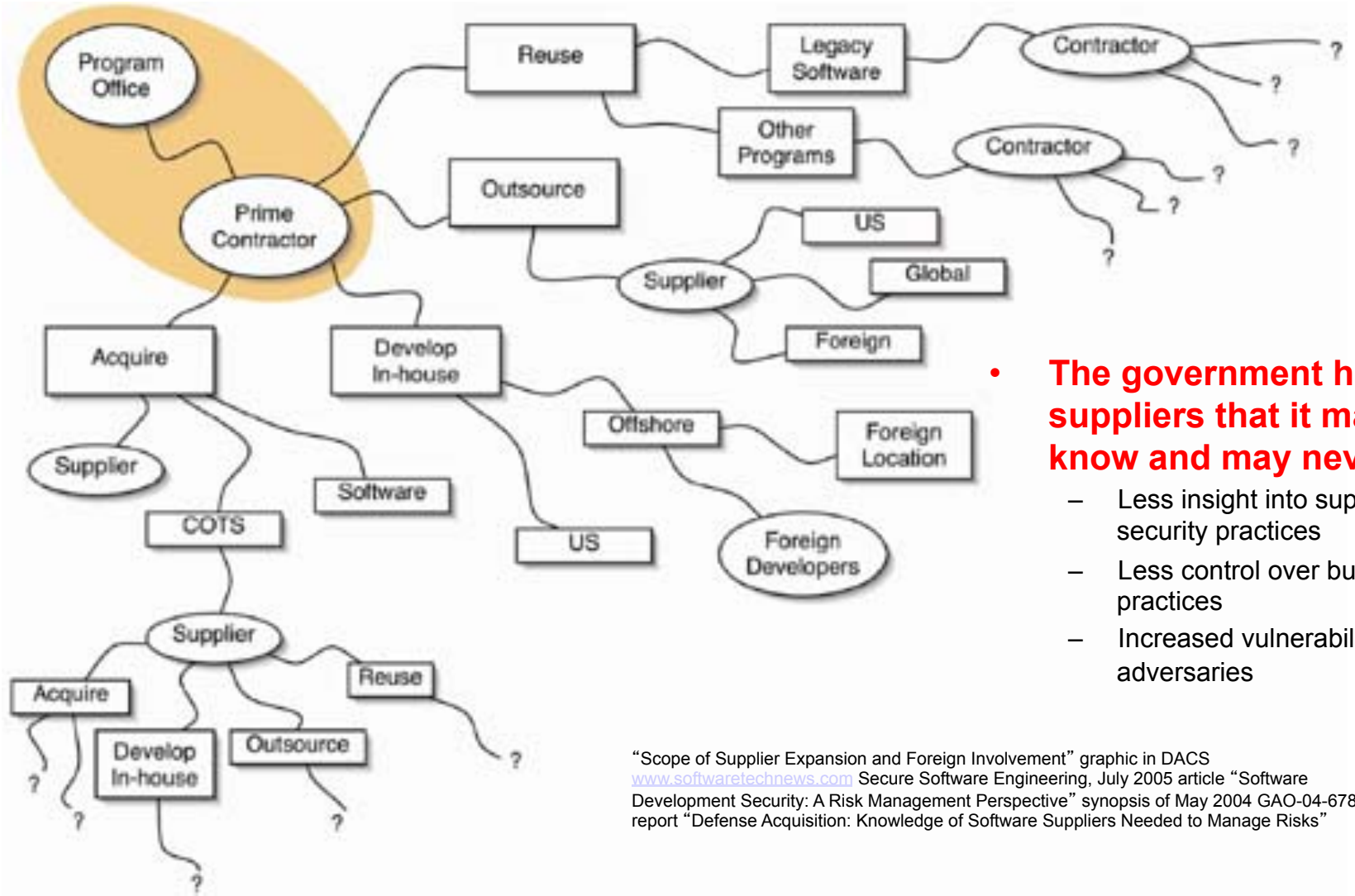
Supply Chain Risk Management (SCRM):

Managing Enterprise Risk
when
Outsourcing (HW, SW & Services)

Don Davidson,
Chief Outreach-Governance-Science-Standards,
in Lifecycle Cyber Security Risk Management (LCSRM)
Deputy DoD-CIO for Cyber Security

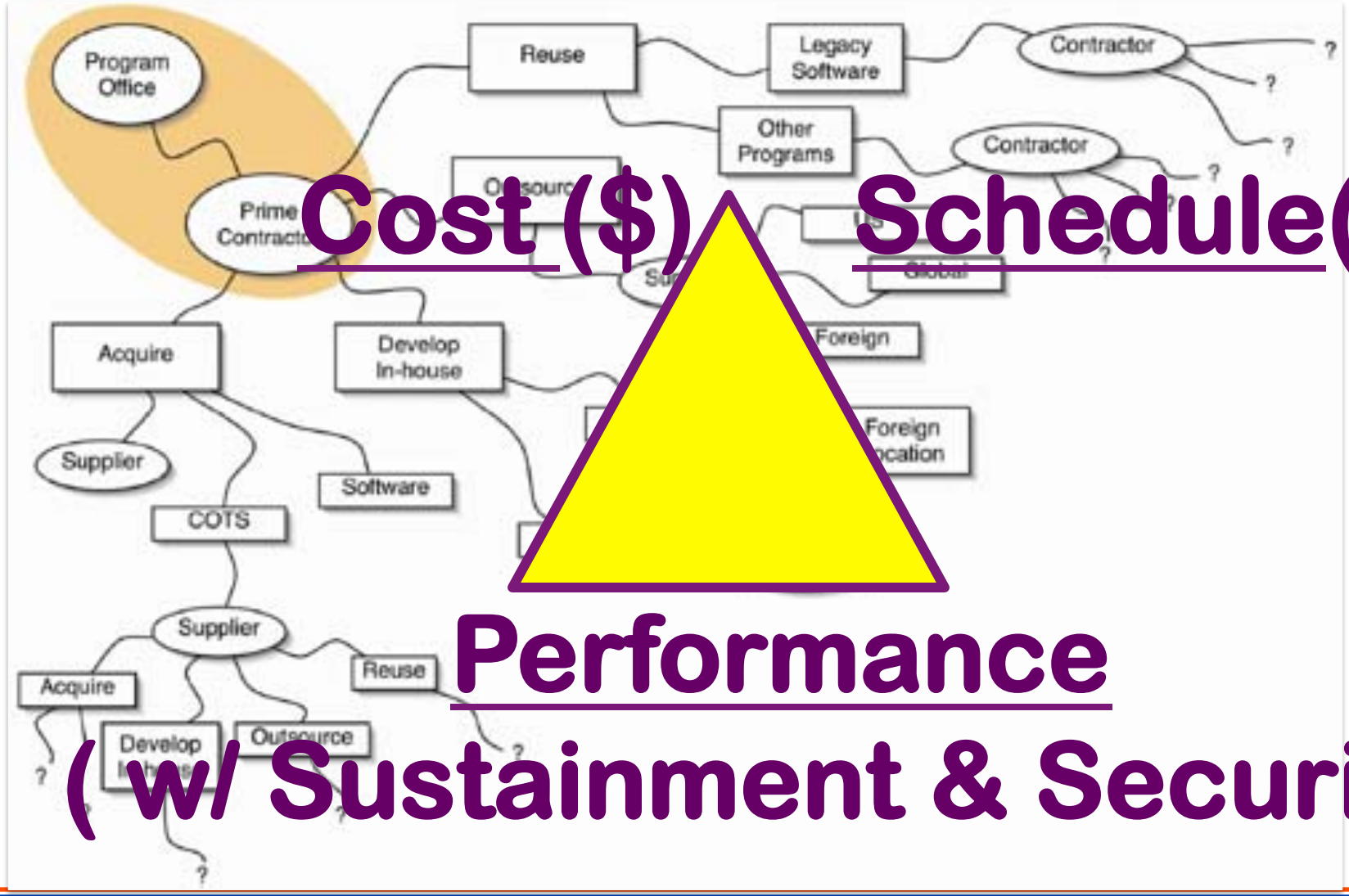
Globalization is good, but it brings challenges



- **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 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"

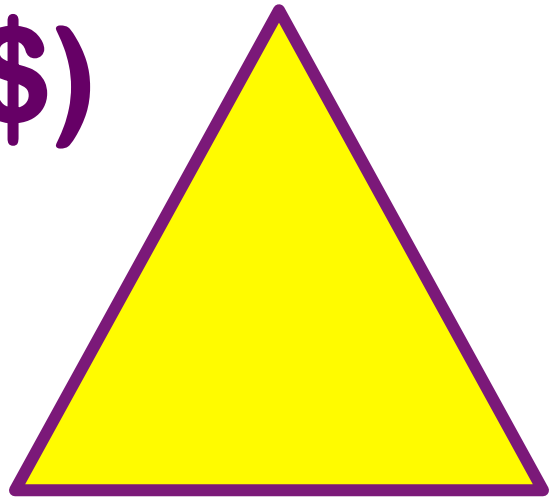
Globalization is good, but it brings challenges



… and Performance side of the TRADESPACE tends to be too near-term focused & mostly about AVAILABILITY

Cost ($)

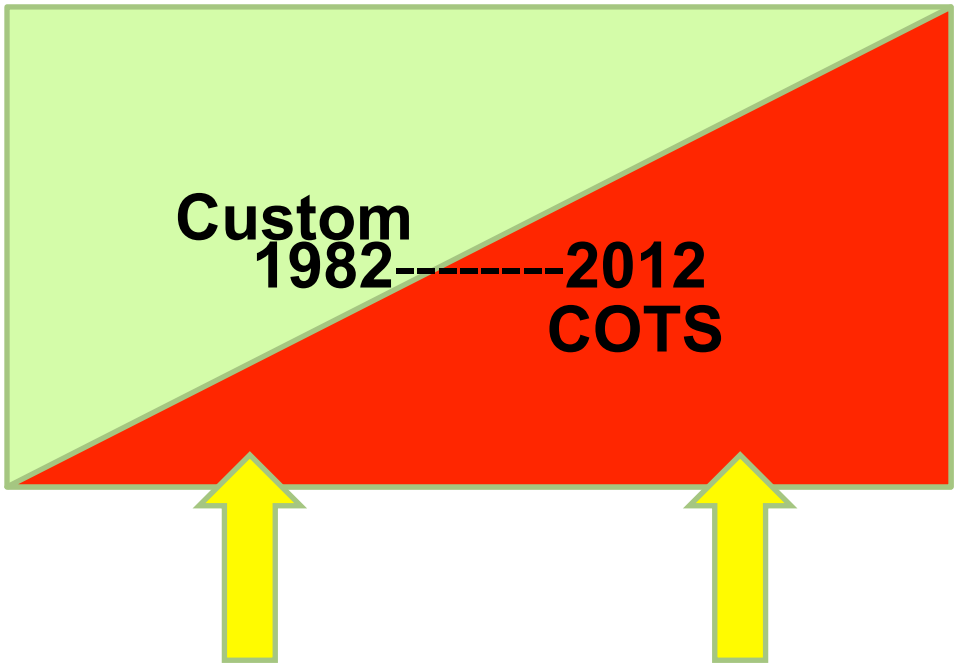
Sched (t)



Performance

(to include Confidentiality, Integrity & Availability)

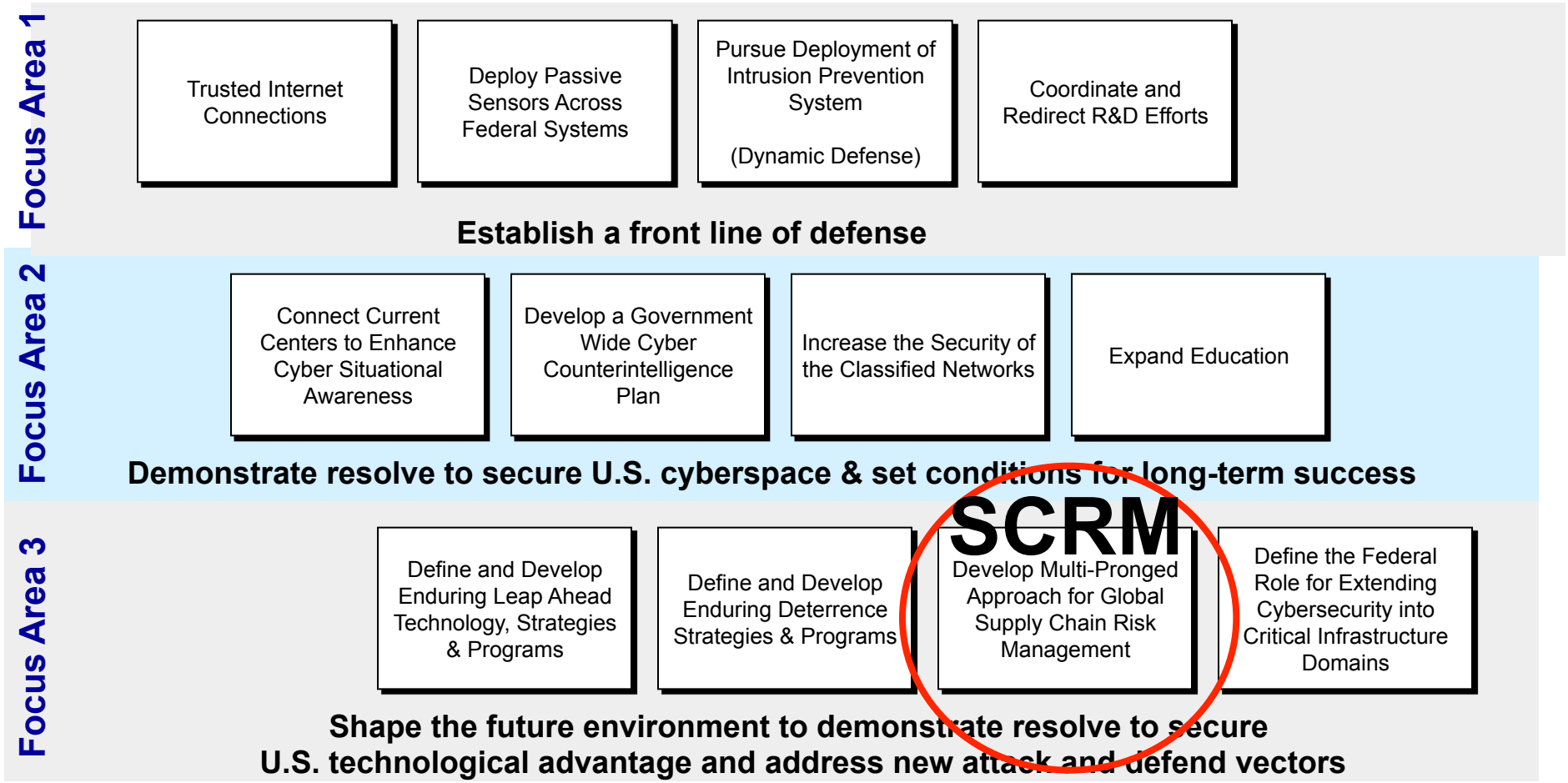
…and…we are all increasingly Dependent on COTS products



"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

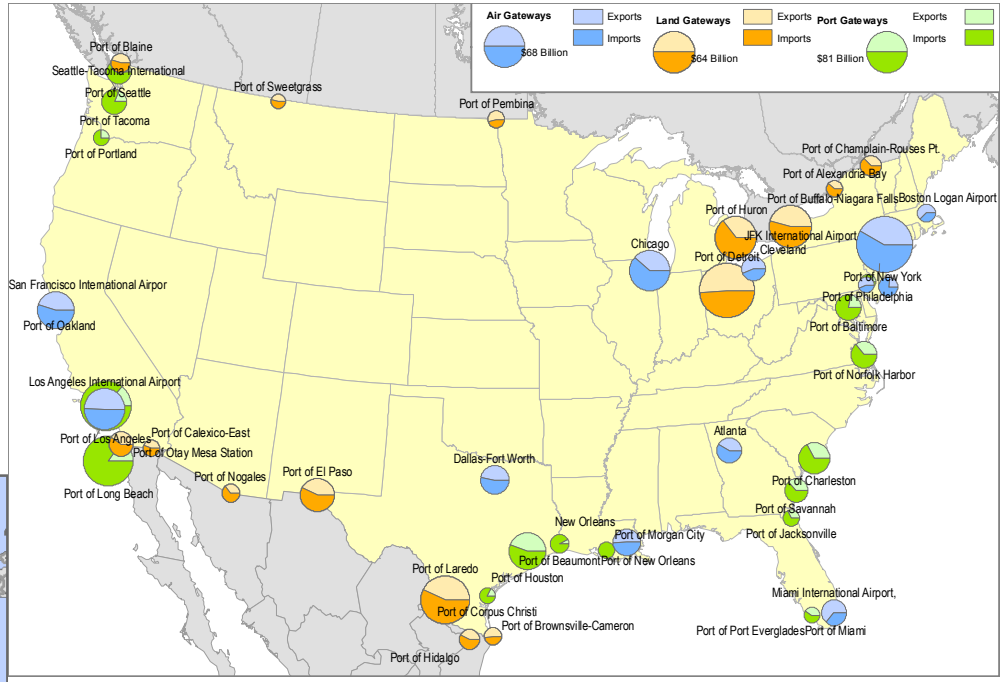
Comprehensive National Cybersecurity Initiative (CNCI)



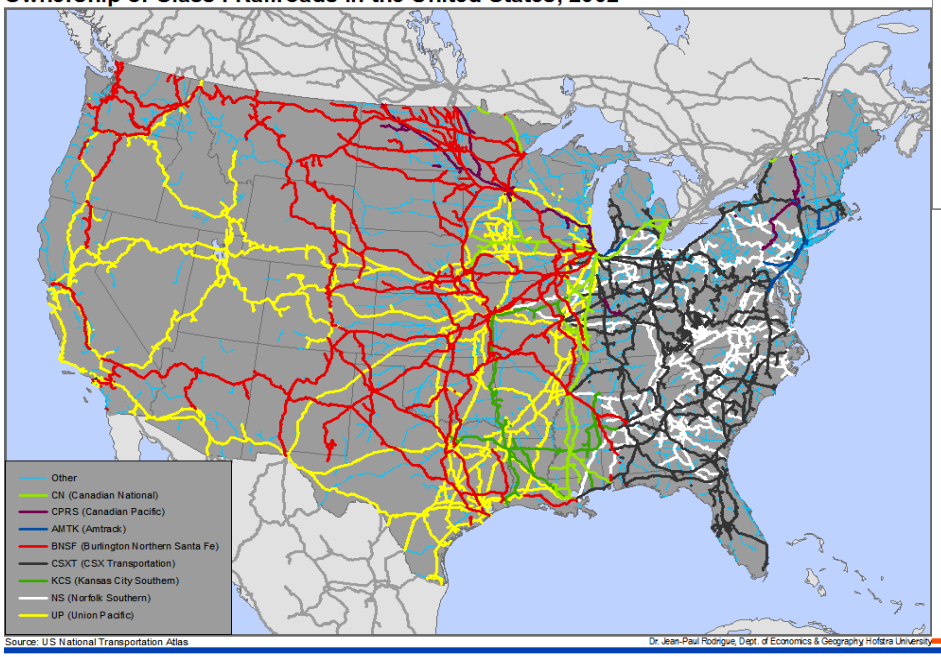
Supply Chain: PERSPECTIVES

Supply Chain SECURITY

- Nodes of
  storage & throughput
- Lines of
  transport (& communication)



Ownership of Class I Railroads in the United States, 2002



Source: U.S National Transportation Atlas

Dr. Jean-Paul Rodrigue, Dept. of Economics & Geography Hofstra University

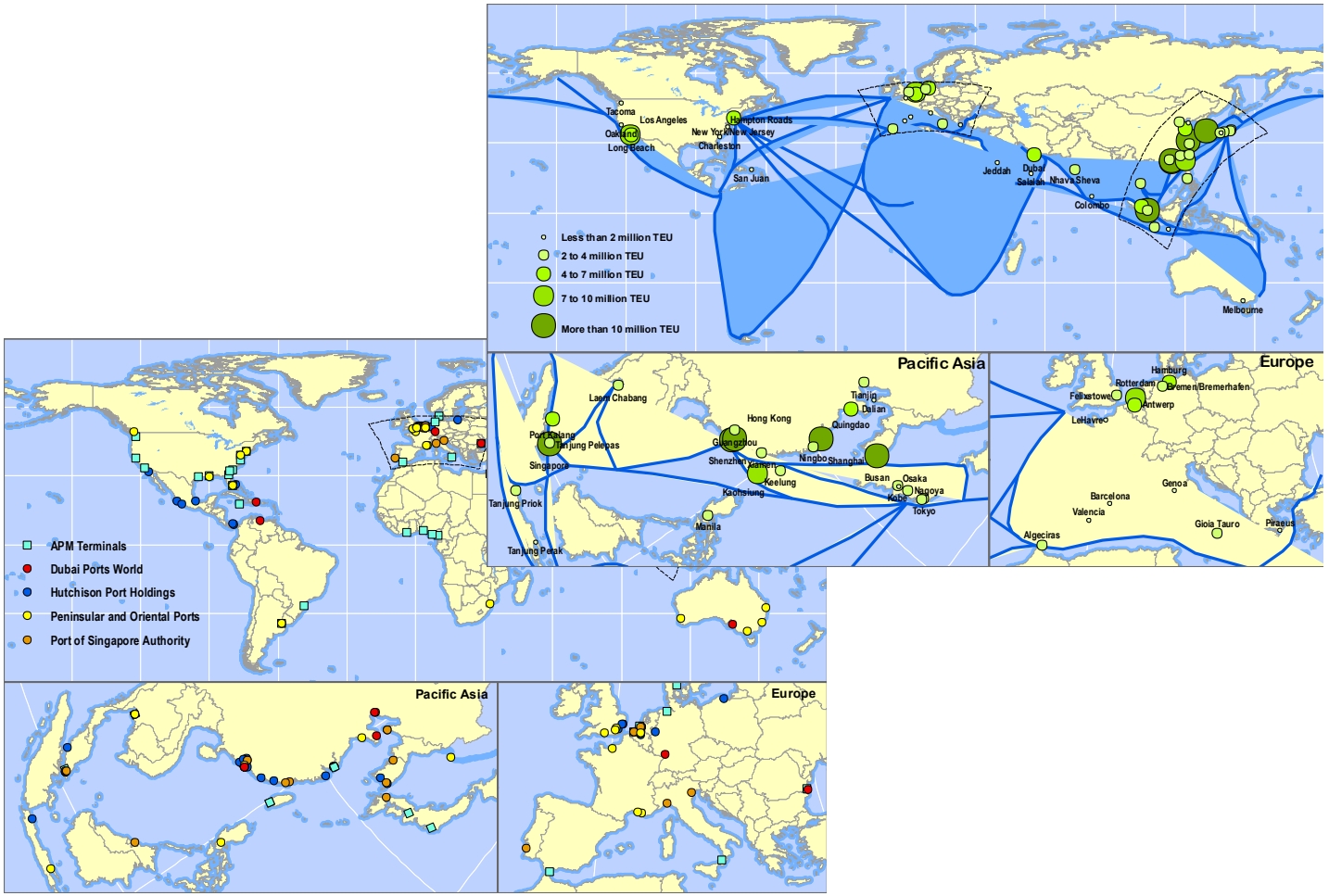
New 2012 US National Supply Chain SECURITY Strategy

Supply Chain: PERSPECTIVES

Supply Chain RESILIENCE

- Multi-sources
- Multi-nodes
- Multi-routes

- fix-on-the-fly (while doing , w/ no pause) … to continue to move product



Supply Chain: PERSPECTIVES

Product INTEGRITY

How do we improve our trust & confidence in HW, SW & Services we source from a global supply chain?

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		Now
Stand-alone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers
CPI (technologies)	>>>	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.)**

What Are We Protecting?

Program Protection Planning
DoDI 5000.02

* DoD is migrating from Information Assurance to Cybersecurity

Technology
DoDI 5200.39

What: Leading-edge research and technology

Who Identifies: Technologists, System Engineers

ID Process: Critical Program Information Identification

Threat Assessment: Foreign collection threat

Countermeasures: Classification, Export Controls, Security, Foreign Disclosure

Focus: "Keep secret stuff in" by protecting any form of technology

Components
DoDI 5200.44

What: Mission-critical elements and components

Who Identifies: System Engineers, Logisticians

ID Process: Criticality Analysis

Threat Assessment: Supplier Risk Analysis

Countermeasures: Supply Chain Risk Management, System Security Engineering, Anti-counterfeits, **software assurance**, Trusted Foundry, etc.

Focus: "Keep malicious stuff out" by protecting key mission components

Information*
DoDD 8500.01 / DoDI 8510.01

What: Information about applications, processes, capabilities and end-items

Who Identifies: All

ID Process: CPI identification, criticality analysis, and classification guidance

Threat Assessment: Foreign collection threat

Countermeasures: Information Assurance, Classification, Export Controls, Security, etc.

Focus: "Keep critical information from getting out" by protecting data

Protecting Warfighting Capability Throughout the Lifecycle

CNCI-SCRM

&

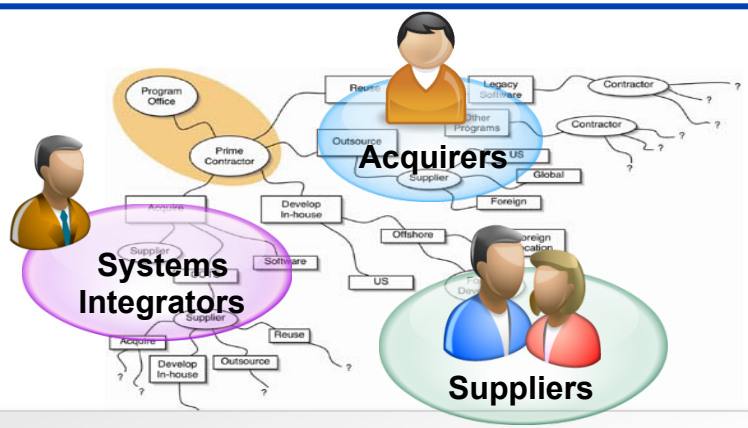
“commercially acceptable global sourcing standards”

Product Assurance
TRADESPACE

$

Unique Requirements

Higher COST can buy Risk Reduction



SCRM Standardization and Levels of Assurance will enable ***Acquirers*** to better communicate requirements to **Systems Integrators** & ***Suppliers***, so that the "supply chain" can demonstrate good/ best practices and enable better overall risk measurement and management.

COTS products

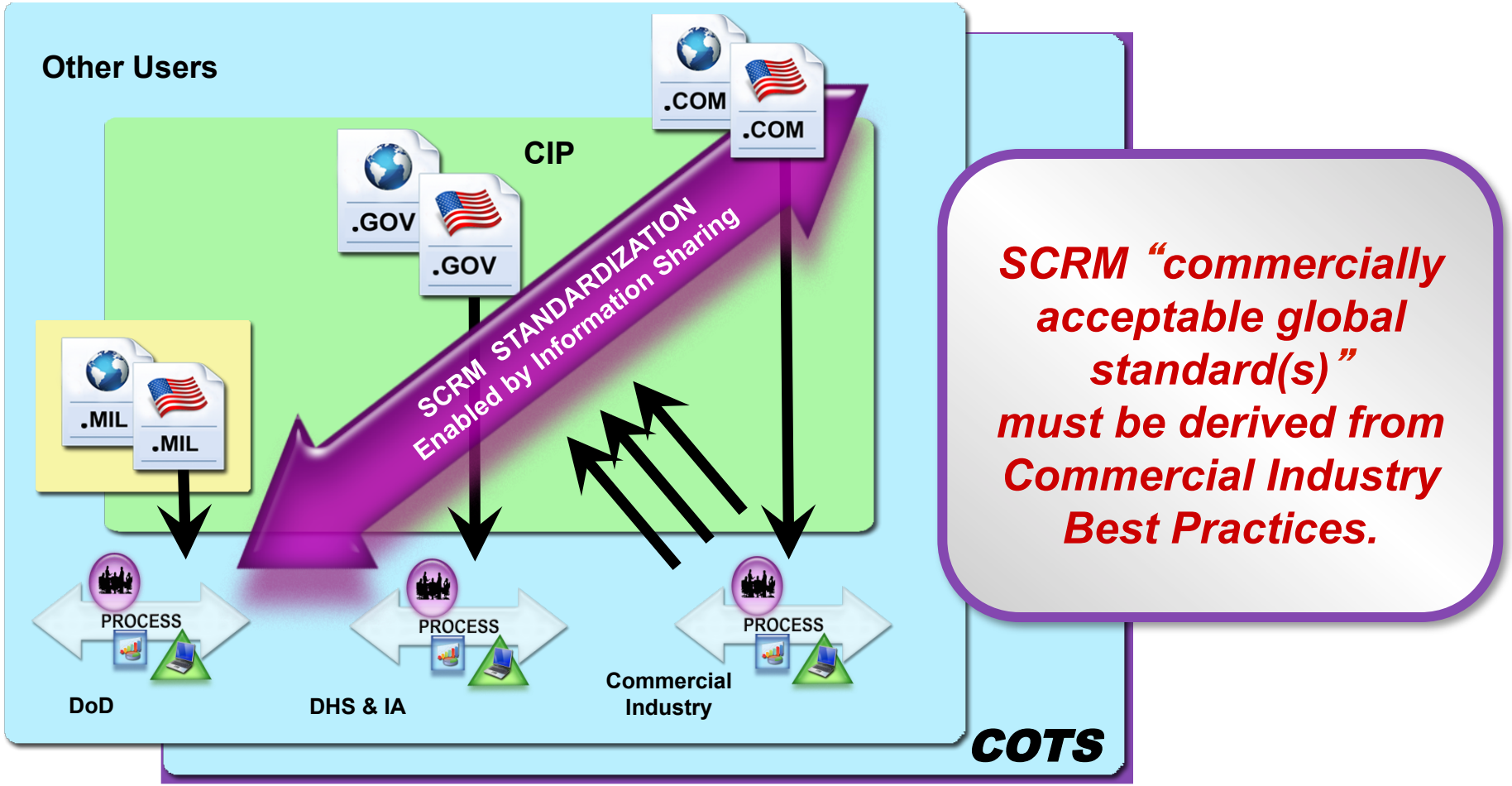
Slippery Slope / Unmeasurable Reqts

Lower Cost usually means Higher RISK

Risk

SCRM Stakeholders

US has vital interest in the global supply chain.

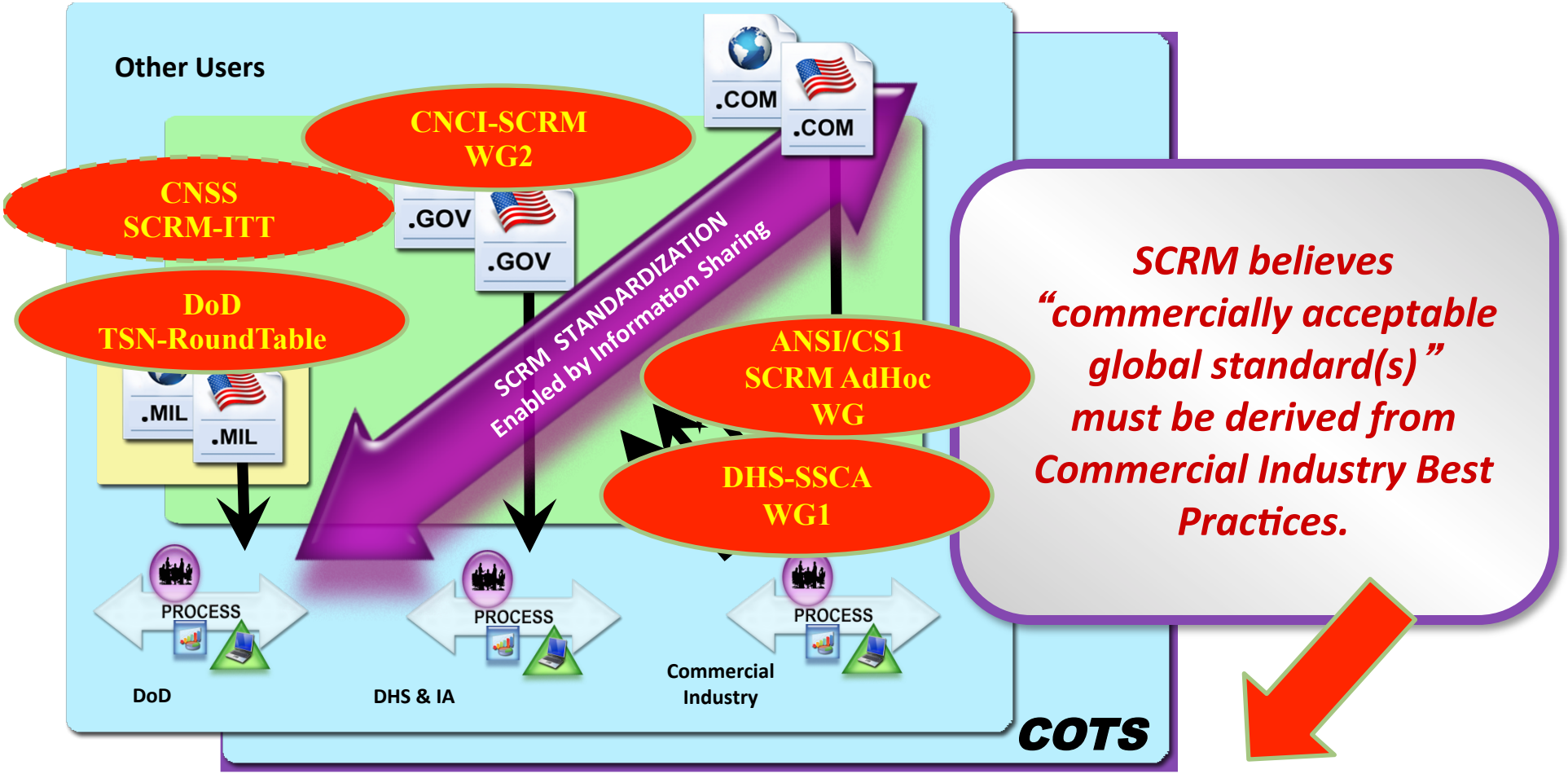


SCRM "commercially acceptable global standard(s)" must be derived from Commercial Industry Best Practices.

SCRM Standardization Requires Public-Private Collaborative Effort

SCRM has a Landscape of activities

US has vital interest in the global supply chain.

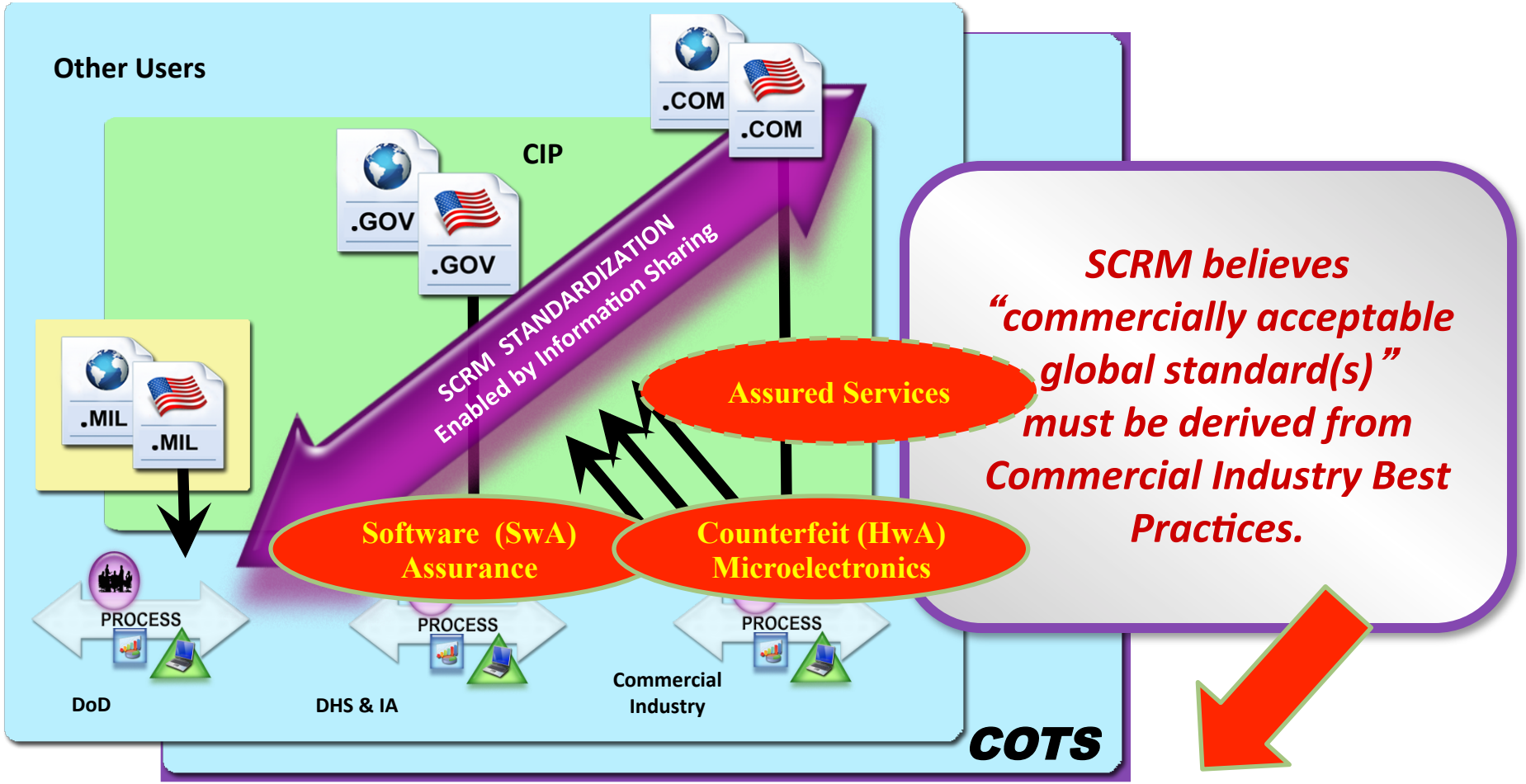


SCRM believes "commercially acceptable global standard(s)" must be derived from Commercial Industry Best Practices.

SCRM Standardization Requires Public-Private Collaborative Effort

SCRM has a Landscape of activities & must address Counterfeits & Software

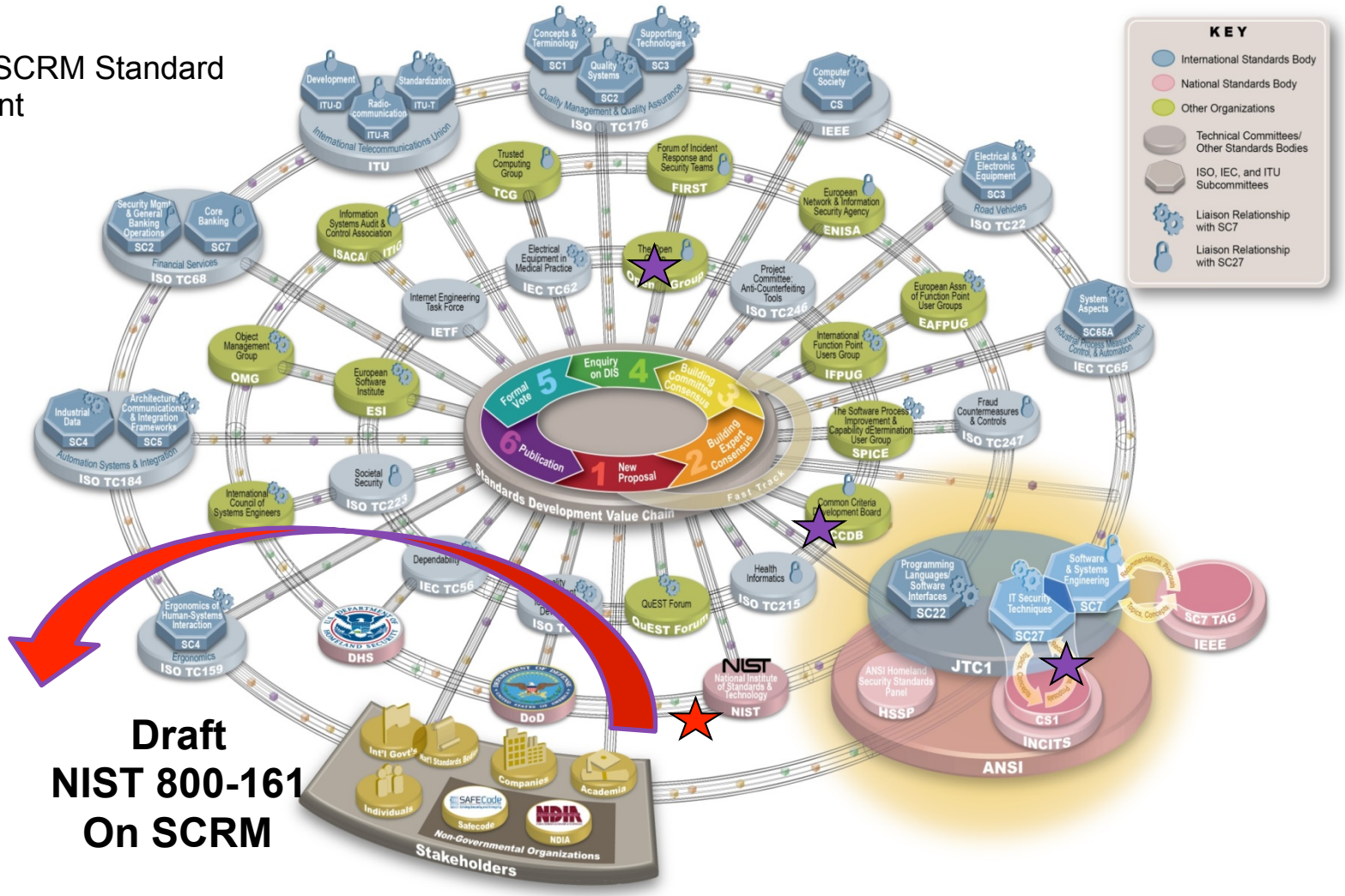
US has vital interest in the global supply chain.



SCRM Standardization Requires Public-Private Collaborative Effort

The ICT SCRM Standard Development Organization Landscape

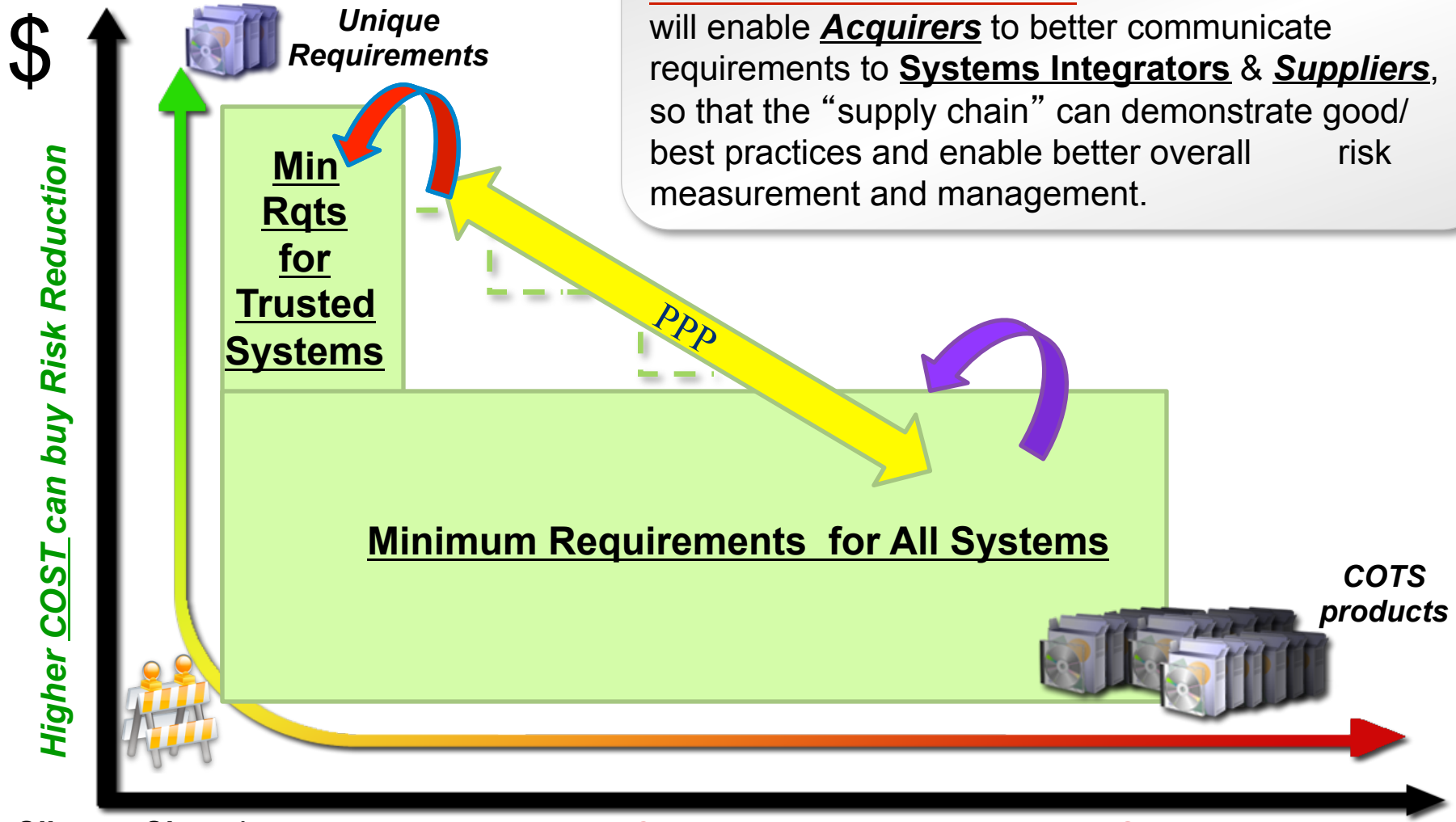
★ Active ICT SCRM Standard Development



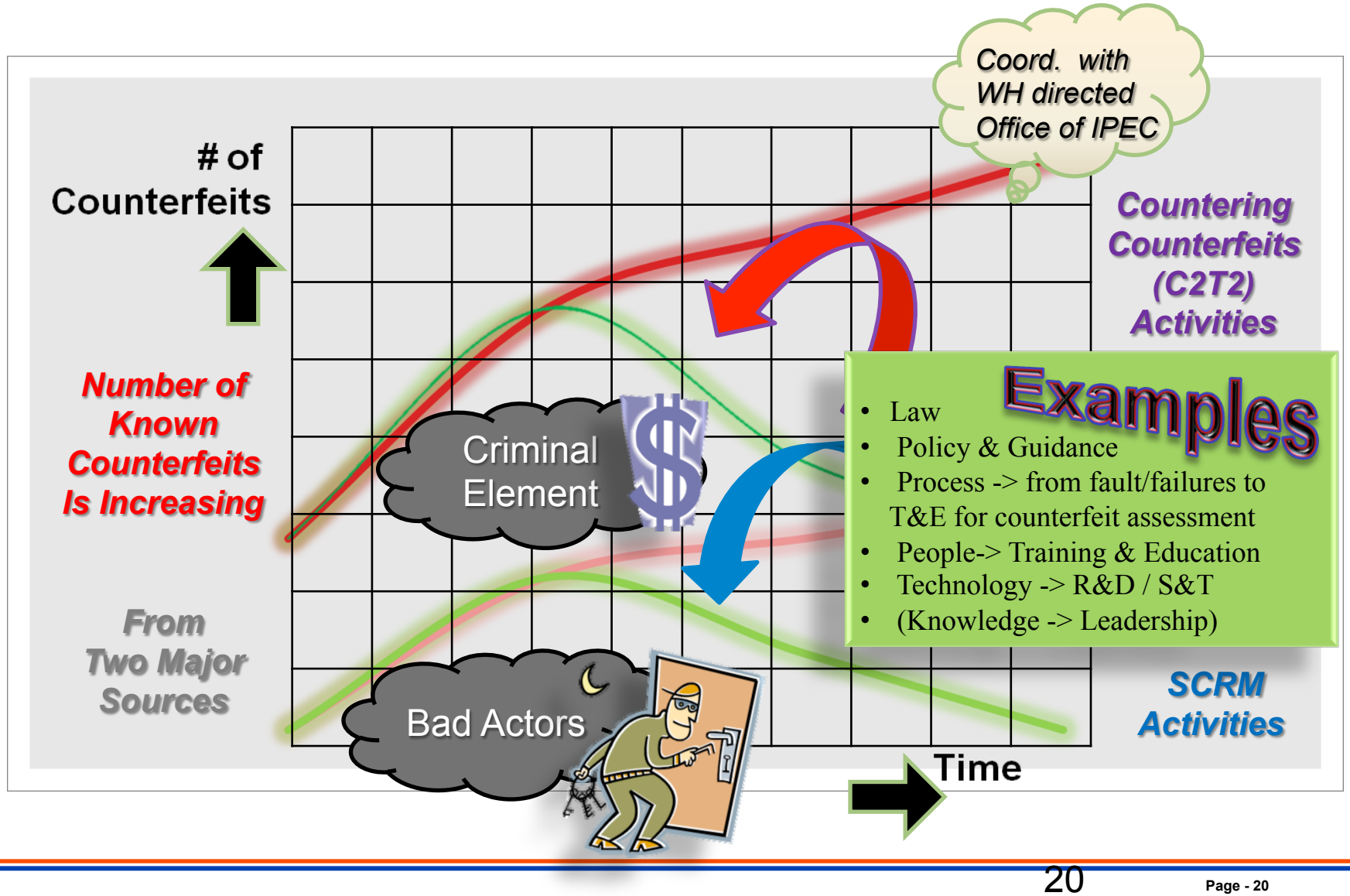
Draft NIST 800-161 On SCRM

…GSA-DoD IT-Acq Report …SSCA in Dec'14

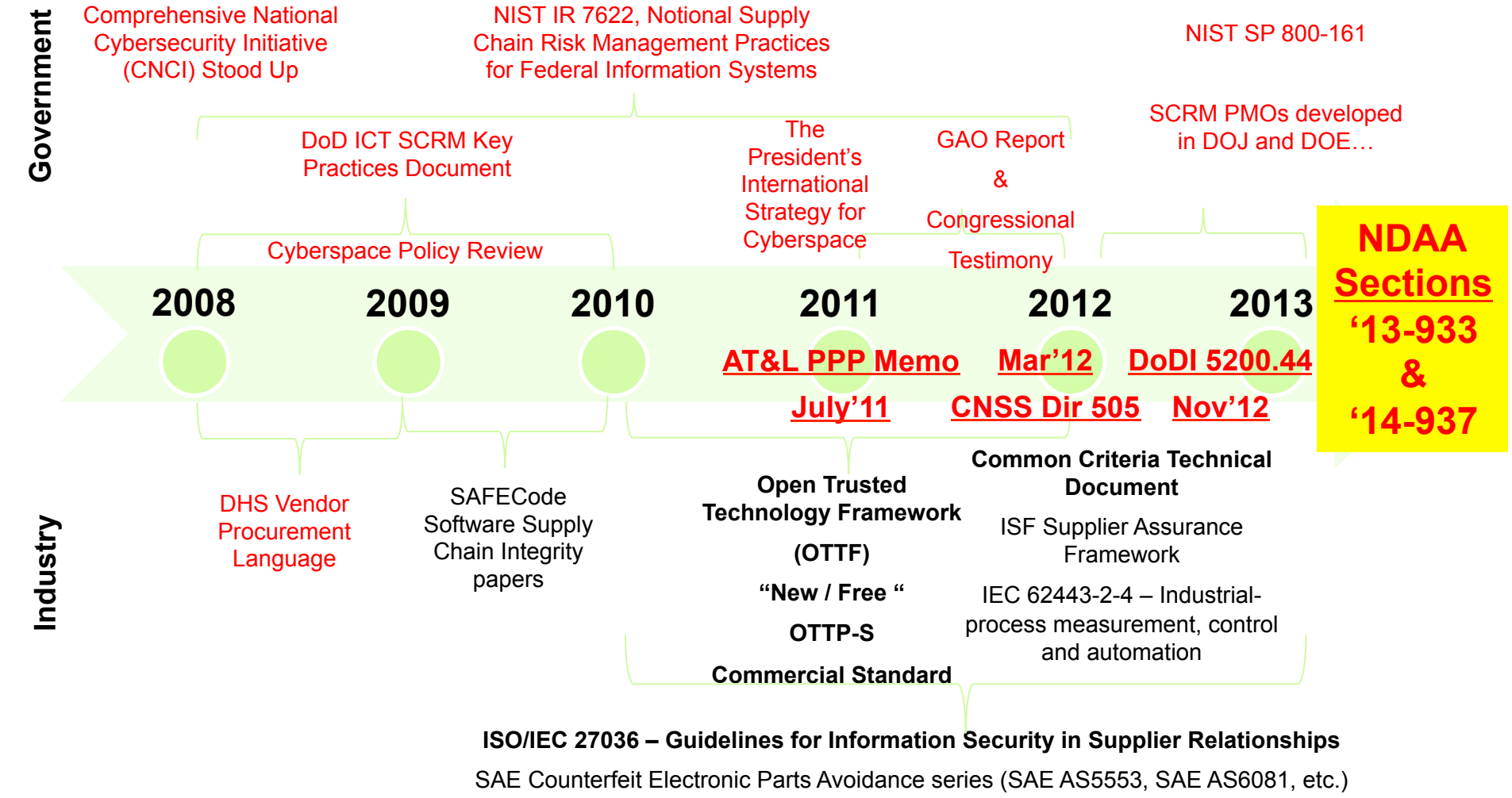
SCRM Standardization and Levels of Assurance will enable ***Acquirers*** to better communicate requirements to **Systems Integrators** & ***Suppliers***, so that the "supply chain" can demonstrate good/ best practices and enable better overall risk measurement and management.



Countering Counterfeits Strategic Concept



Existing and Emerging SCRM Practices and Standards



Adopted from
Nadya Bartol / UTC.org

Commercial SCRM Developments & Standards

Lots ongoing- this is a representative list (not all inclusive)

- **TheOpenGroup's Trusted Technology Forum (OTTF): Trusted Technology Provider Standard (OTTP-S)**

  https://www2.opengroup.org/ogsys/catalog/C139... and Accreditation Process

- **Supply Chain Technical Working Group (CCTWG) "approved" by Common Criteria Development Board (CCDB) to advise CCDB & development of new CC "Protection Profiles" that will replace EALs**

  https://cc-supplychain.teamlab.com/products/files/#408084

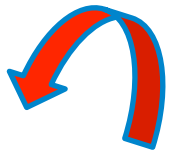
- **ISO 27036 on ICT Acquirer-Supplier Relationships (Parts 1-2-3) finalized Part 1 is FREE… (TMSN/ LCSRM leads US participation in ANSI CS1 SCRM adHoc WG)**

- **SAE- G19's AS5553 on Counterfeit Electronics… AS6171…**

- **SAFECode**

  http://www.safecode.org/index.php

Govt-SCRM-related Developments



- CNCI-SCRM still alive & well

- CNSS DIRECTIVE 505 on SCRM from Committee on National Security Systems (FOUO)
  http://csrc.nist.gov/news_events/index.html

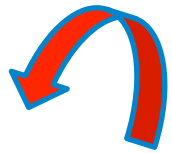
- "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks", GAO-12-361, Mar 23
  http://www.gao.gov/products/GAO-12-361

- NIST-IR 7622 & NIST 800-53 rev4 (US.gov-only participates in SCRM WG2)
  http://csrc.nist.gov/news_events/index.html---- new NIST SP-161 on SCRM

- DODI 5200.44 on Trusted Systems & Networks (Nov 2012)
- USD AT&L Memo on Program Protection Planning (PPP) July 2011
- Monthly TSN RoundTable Meetings & periodic TSN/PP Executive Council Meetings

- NEW EO-CyberSecurity FRAMEWORK

Recent Evolution of Strategy & Policy



Counterfeit Microelectronics---L&MR lead

Who is working this (DoD, US,gov, public-private, standards)
& NDAA'12 Section 818… & NDAA'13 Section 833… **New DoDI 4140.67**

- **-Learn from Quality Assurance & Safety Critical Items Practices**
- **-Procurement & Acquisition-Contracts**
- **-Testing (life cycle doc, acceptance, follow-up analysis)**
- **-Reporting**
- **-WorkForce Development (training & education)**
- **-Standards**

Software Assurance---AT&L-SE lead

Who is working this (DoD, US,gov, public-private, standards)
& NDAA'11 Section 932 & **NDAA'13 Section 933 (SOAR, R&D, Liability)**

- **-Learn from Quality Assurance & Safety Critical Items Practices**
- **-Procurement & Acquisition-Contracts**
- **-Testing (life cycle doc, acceptance, follow-up analysis)**
- **-Reporting**
- **-WorkForce Development (training & education)**
- **-Standards**

DoD's SCRM for TSNs

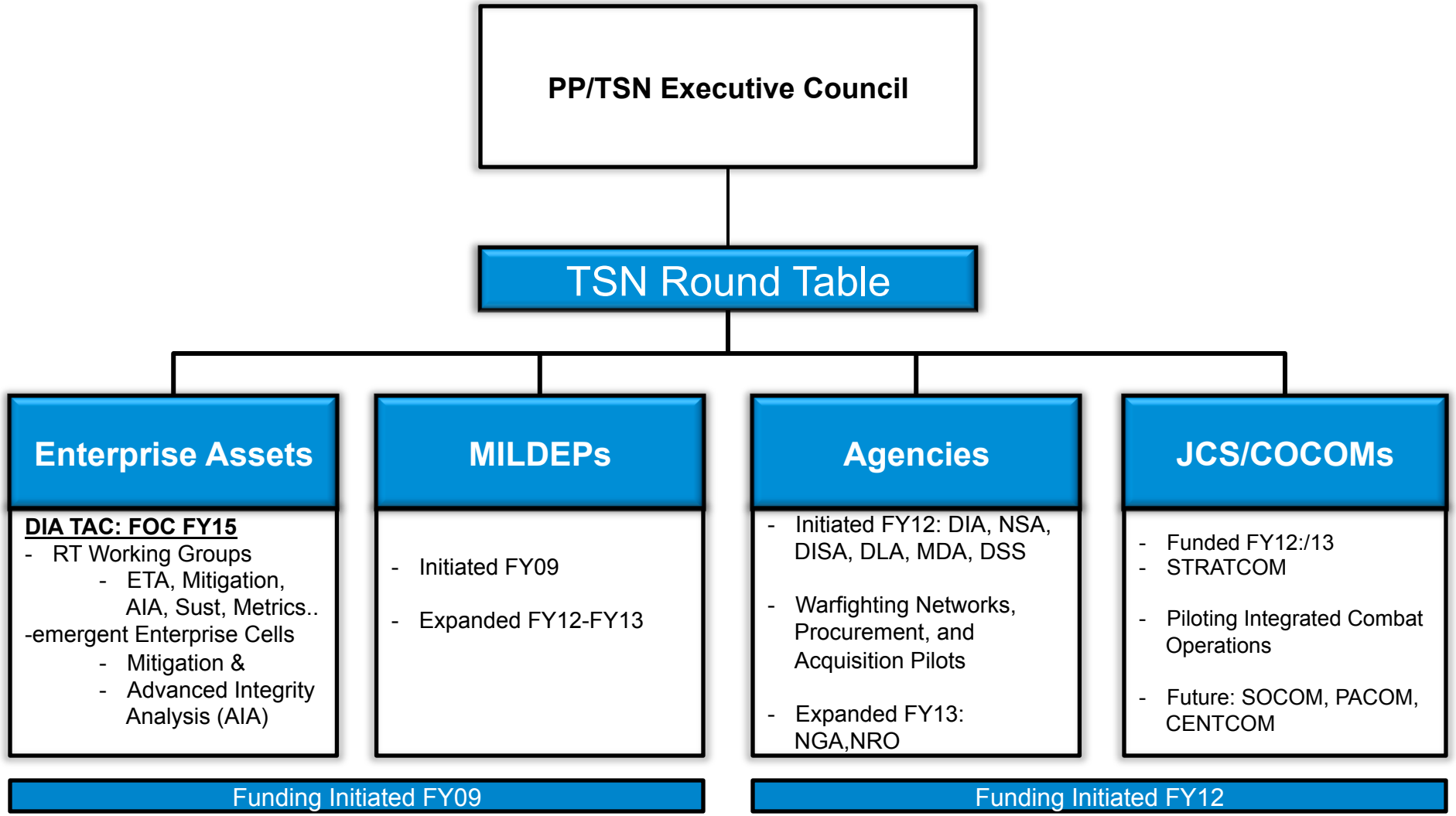
is more than

PPPs & DoD Acquisition,

It's about Cyber Risk in the Lifecycle

(what is centralized & decentralized)

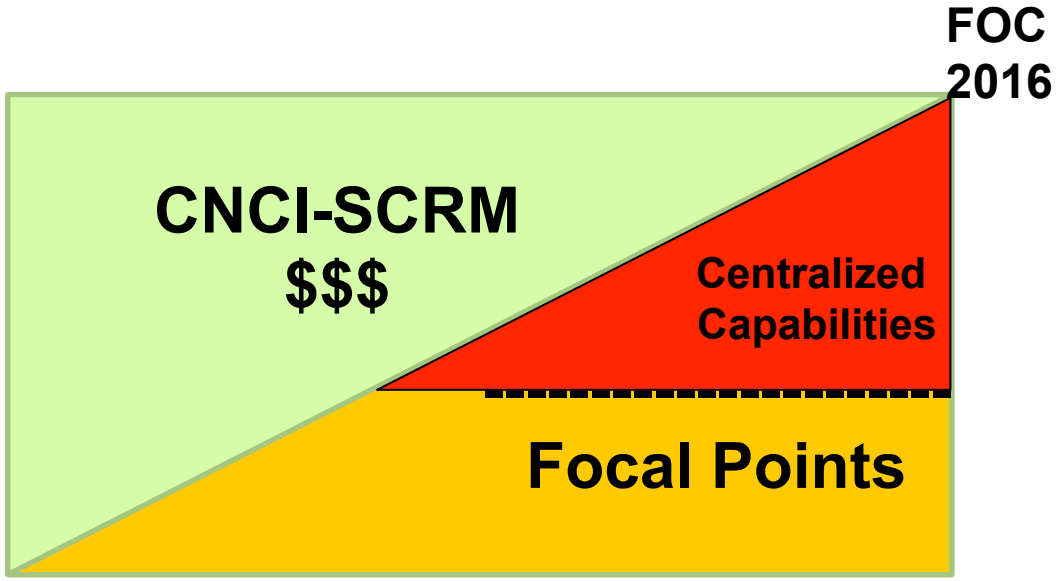
TSN Governance



TSN RT Participants

- **Focal Points**

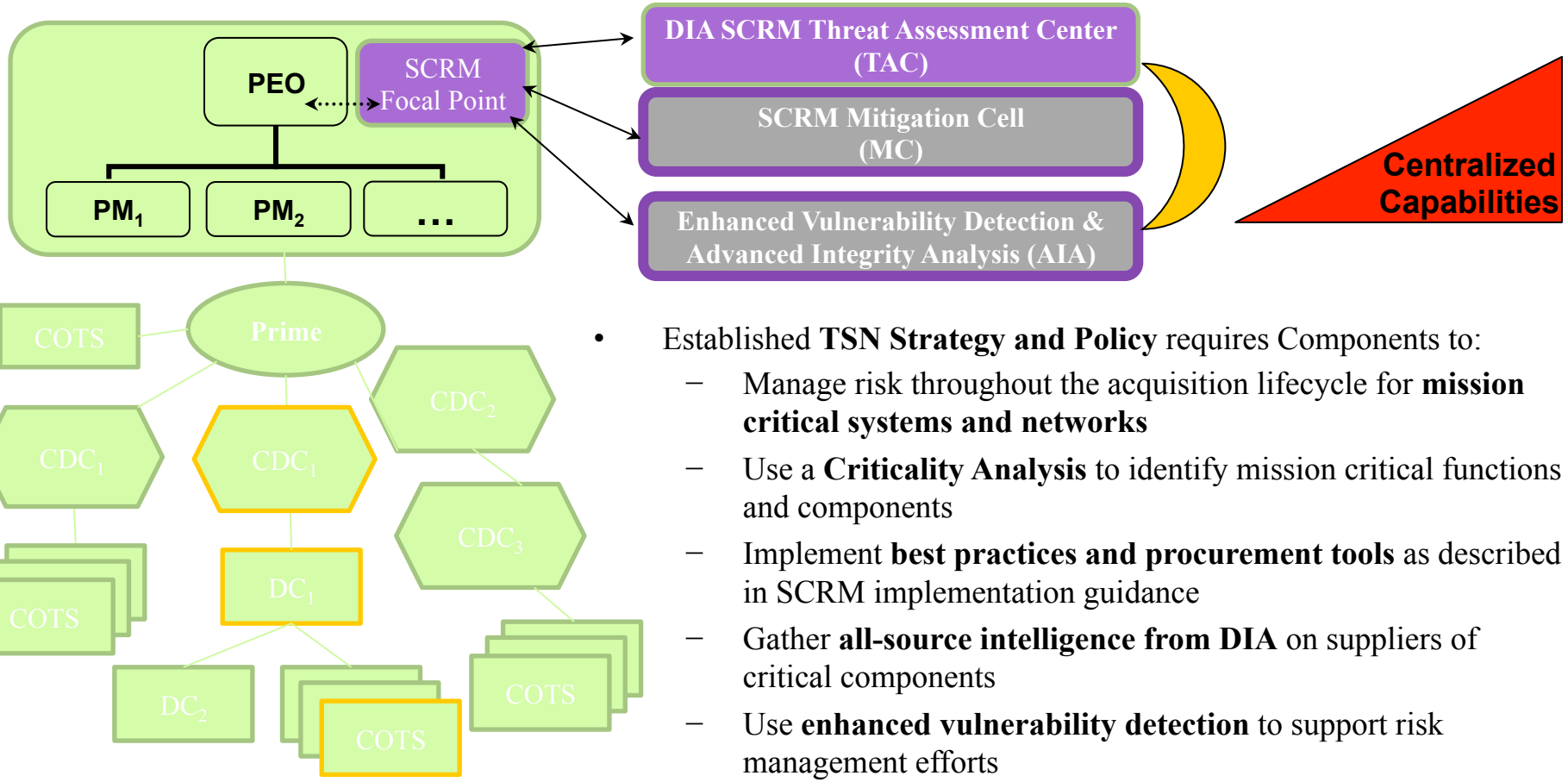
- **Stakeholders**



People----------FTEs / ETA*
Process----------TAC*, Mitigation*, Sustainment*
Tools/Technology---HwA & SwA Testing, AIA*
Metrics----------Methods to Measure & Manage Risk

_____*_TSN-RT Working Groups (WGs)_____

Trusted Systems and Networks Enterprise Capabilities

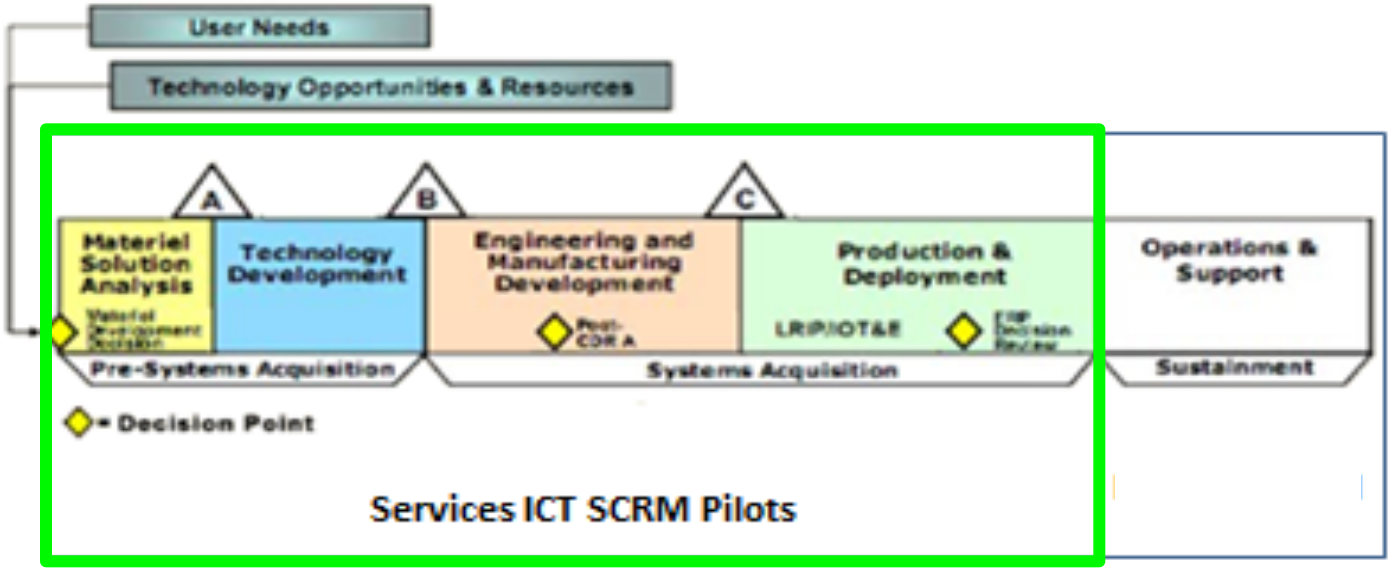


- Established **TSN Strategy and Policy** requires Components to:
  - Manage risk throughout the acquisition lifecycle for **mission critical systems and networks**
  - Use a **Criticality Analysis** to identify mission critical functions and components
  - Implement **best practices and procurement tools** as described in SCRM implementation guidance
  - Gather **all-source intelligence from DIA** on suppliers of critical components
  - Use **enhanced vulnerability detection** to support risk management efforts
  - Work with the **TSN Focal Points** and subject matter experts to develop and **implement mitigation strategies**

= Critical function or components = Unfunded activity = Critical function or components

SCRM in PPP & Sustainment

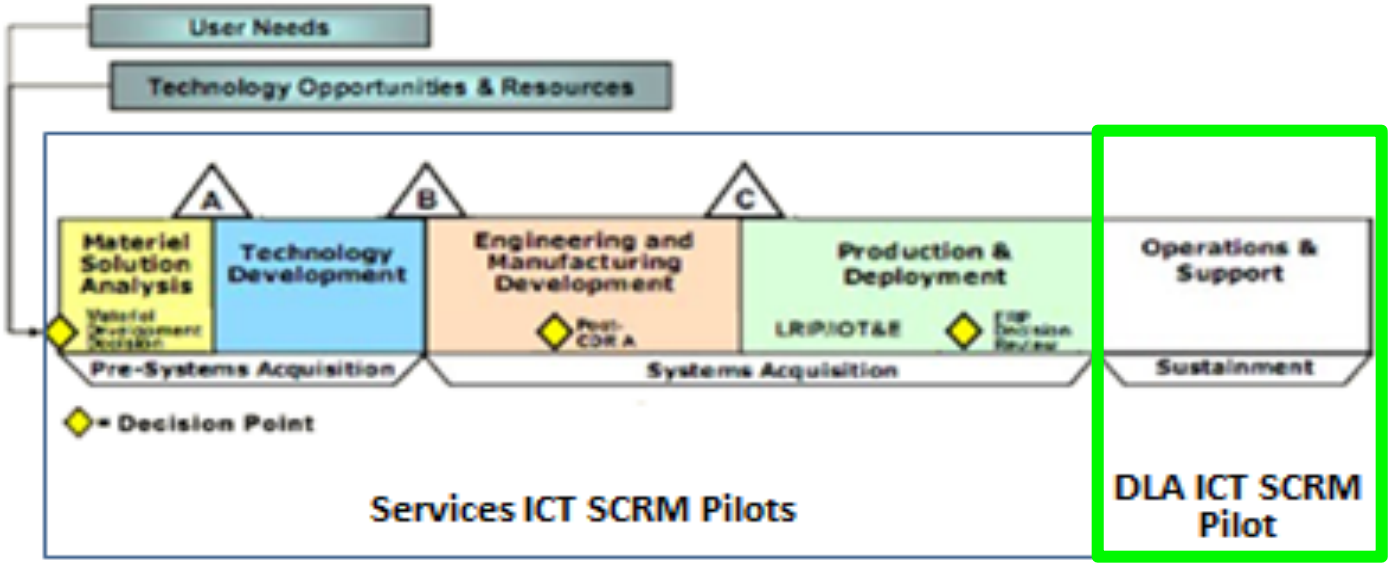
DoD 5000 Defense Acquisition System



- Focuses on Pre-Systems Acquisition and Systems Acquisition Phases (ACAT I programs)
- Emphasis is placed on the PPP through MS C and FRP

SCRM / PPP and DLA

DoD 5000 Defense Acquisition System



- DLA pilot focuses on the ICT components that support weapon systems throughout DoD
- The emphasis is on protecting fielded weapon systems

Transition from Acquisition to Sustainment

Acquisition Process

Logistics Reassignment Process

- Governed by DoD 4140.26M (Vol 2 & 4)
- Service defines <u>criticality of part, such as:</u>
  - Critical Flight Safety
  - Critical Application
- Service defines <u>Acquisition Strategy, such as</u>:
  - Sole source
  - Competitive bid

Sustainment Process

Lead Service

Service Engineering Support Activity (ESA) retains configuration control (Tech data)

DLA Priority

DLA accepts management of consumable items

DoD TSN Strategy

&

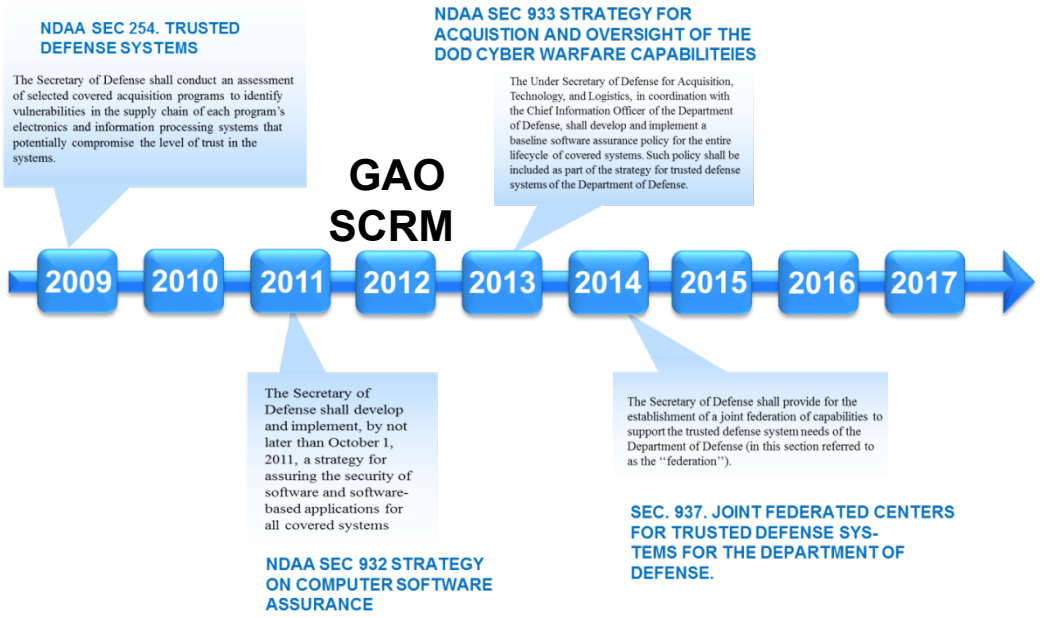
NDAAs

DoD TSN Strategy & NDAAs

(Still a work in progress)

- A *combination* of the assurance expertise, products, and services—and continued advancements within these areas—is required to help the DoD establish and institutionalize a culture of assurance-focused engineering and (ultimately) Designed-in Security.

- In response the DOD created The Trusted Systems and Networks Strategy which provides an overarching framework for the design and delivery of trusted systems addressing hardware assurance, software assurance, supply chain management, and supporting policy, engineering practices, and training and awareness.



"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

Risk Management Framework (RMF)

&

Cybersecurity Governance

RMF & Governance

Donald.R.Davidson4.civ@mail.mil

Don Davidson
Chief, Outreach, Science & Standards
LCSRM in DoD-CIO

Comprehensive National Cybersecurity Initiative (CNCI)