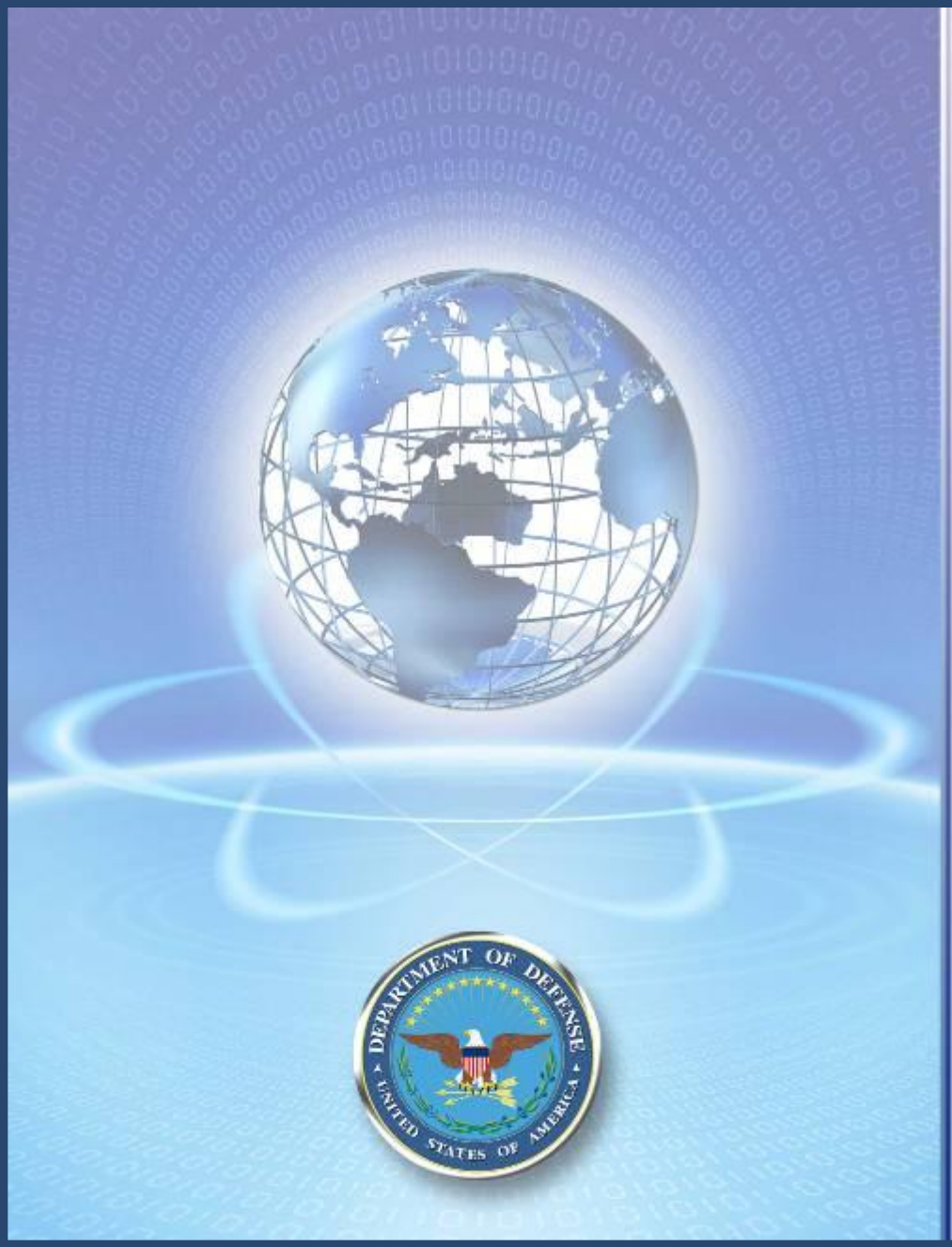


CNCI-SCRM

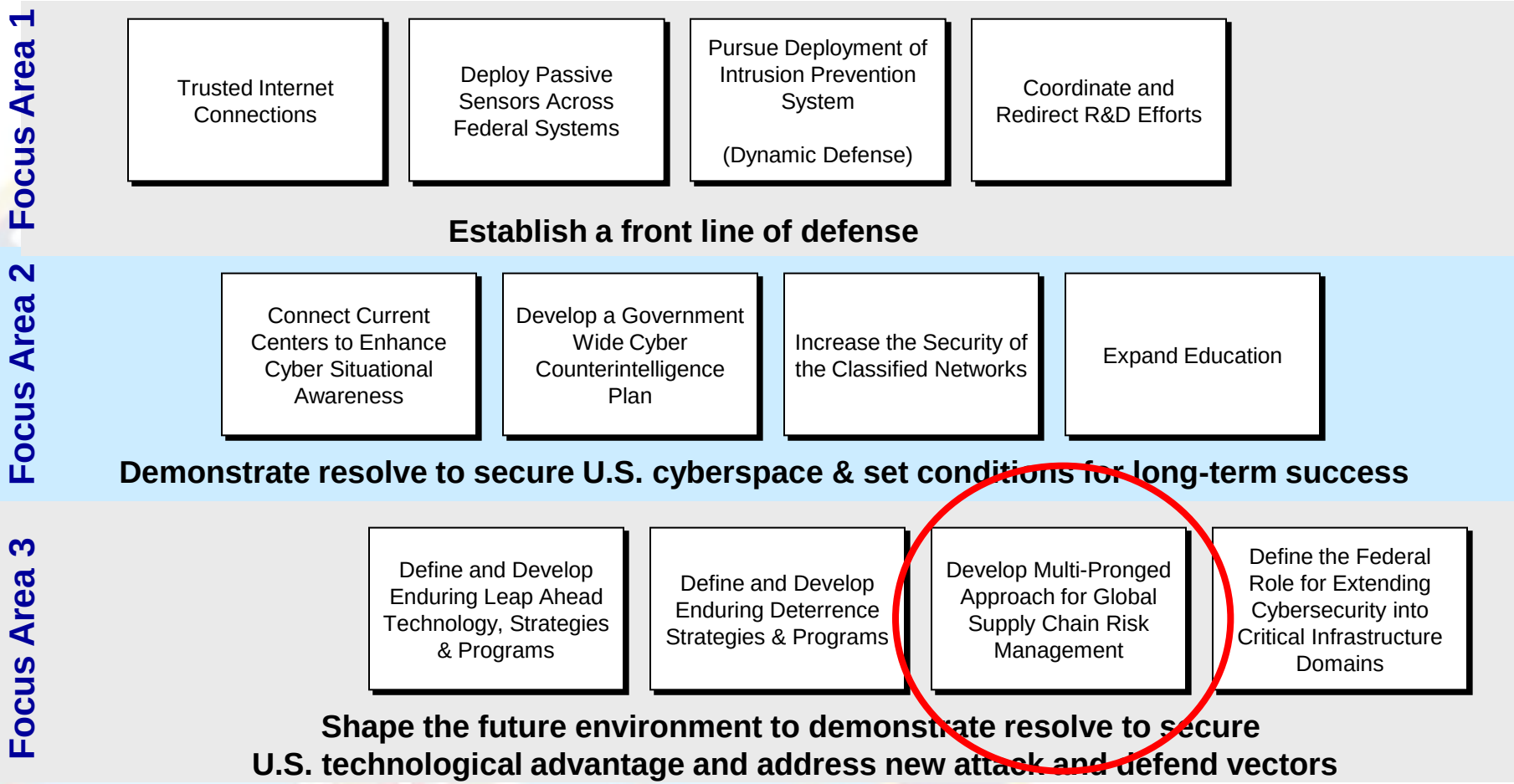
US Comprehensive National Cybersecurity Initiative – Supply Chain Risk Management

"UNDERSTANDING the CHALLENGES from OUTSOURCING"

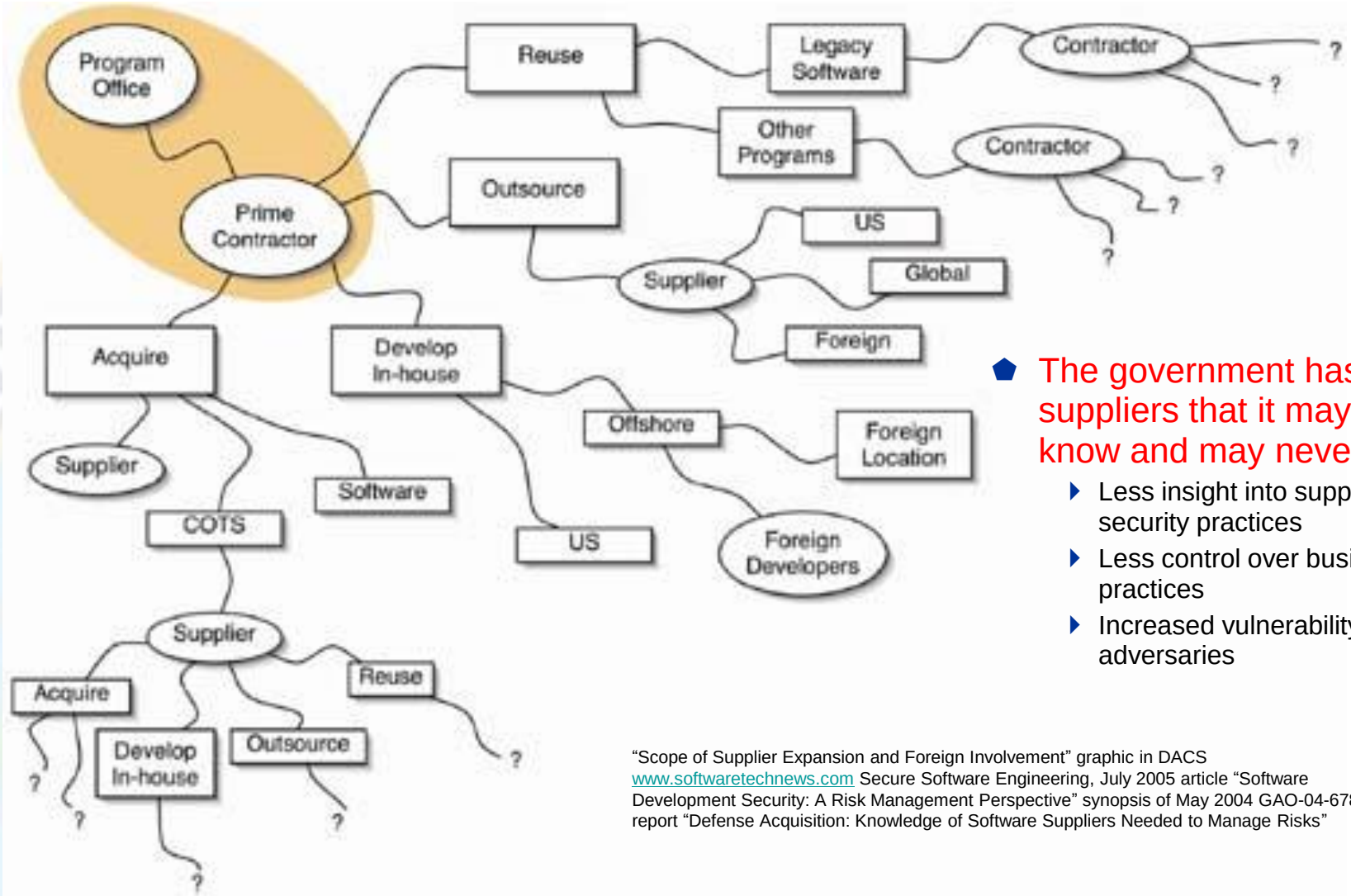
Mr. Donald Davidson,
Chief, Outreach & Standardization
Trusted Mission Systems & Networks
(formerly Globalization Task Force, GTF)
OASD (NII) / DoD CIO

Don.Davidson@osd.mil

Comprehensive National Cybersecurity Initiative (CNCI)



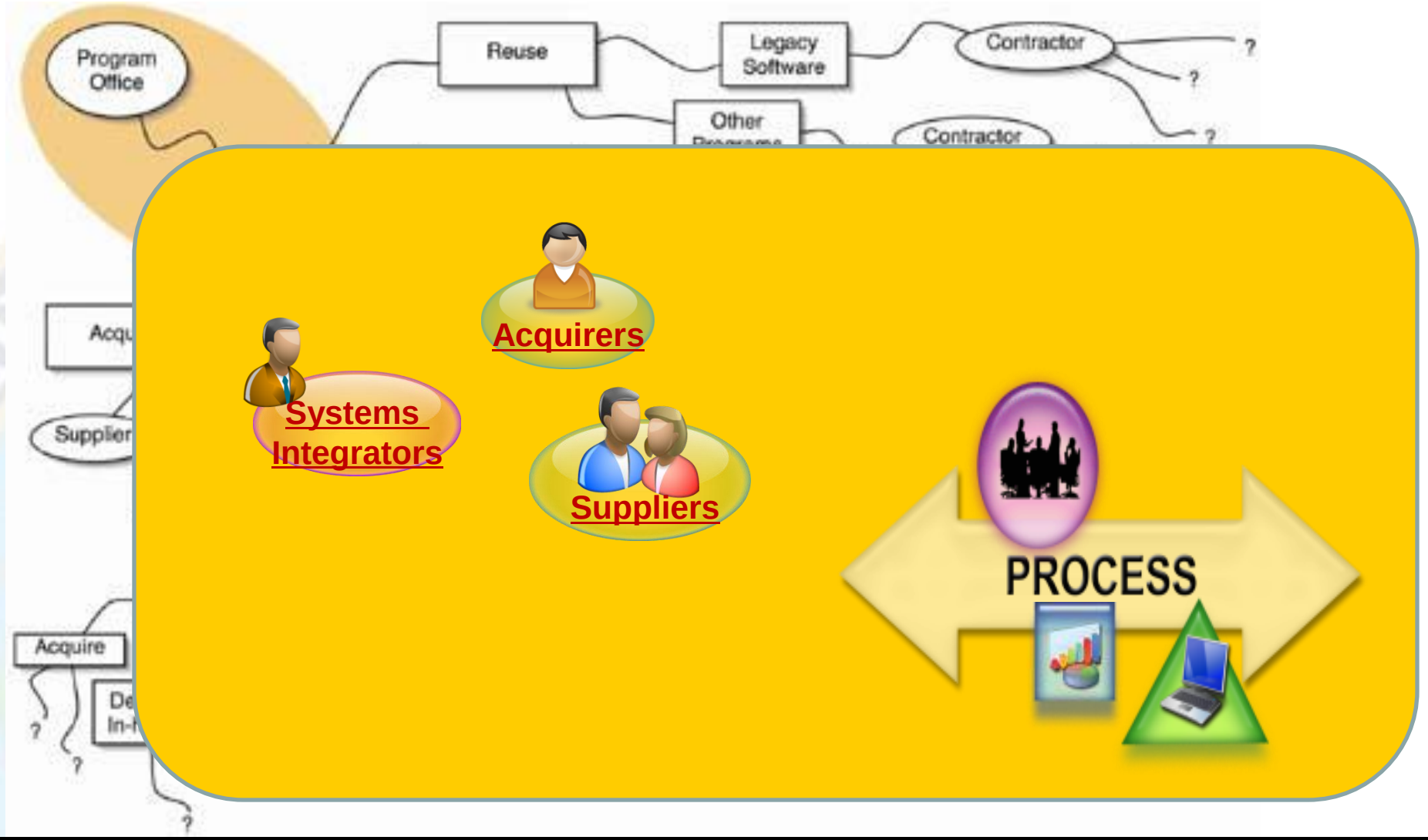
Globalization brings challenges to DoD…



- 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 brings challenges to DoD…



Today's Reality of our Increased Dependency Requires an Increased Confidence in our ICT

- Dependencies on technology are greater then ever

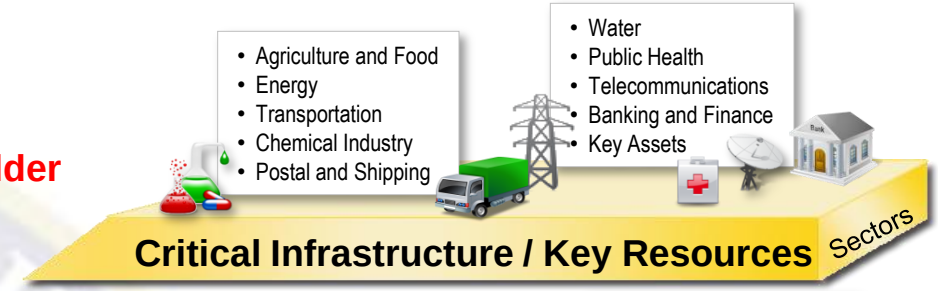
-- Possibility of disruption is greater than ever because hardware/software is vulnerable

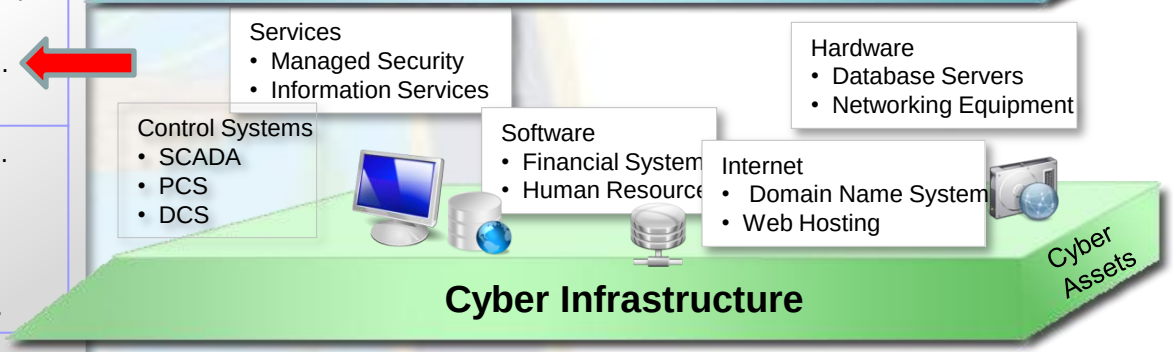
--- Loss of confidence alone can lead to stakeholder actions that disrupt critical business activities

Internet users in the world: 1,766,727,004
E-mail messages sent today: 215, 674, 475, 422
Blog Posts Today: 458, 972
Google searches Today: 2,302,204,936

Who is behind data breaches?	**74%** resulted from external sources (+1%). **20%** were caused by insiders (+2%). **32%** implicated business partners (-7%). **39%** involved multiple parties (+9%).
How do breaches occur?	**7%** were aided by significant errors (<>). **64%** resulted from hacking (+5%). **38%** utilized malware (+7%. **22%** involved privilege misuse (+7%). **9%** occurred via physical attacks (+7%).

** Source – 2009 Verizon Data Breach Investigations Report*





ASD(NII) / DoD CIO

DASD(IIA) / DoD-CISO

TMSN
Mitch Komaroff

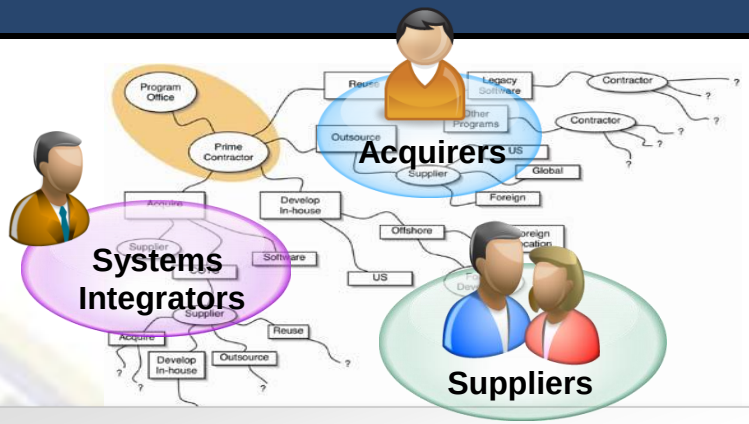
- Jenine Alston
  Policy+
- Annette Mirsky
  Pilots+
- Joe Wassel
  Criticality+
- Don Davidson
  Standards+
- Pat Sullivan
  CFIUS

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

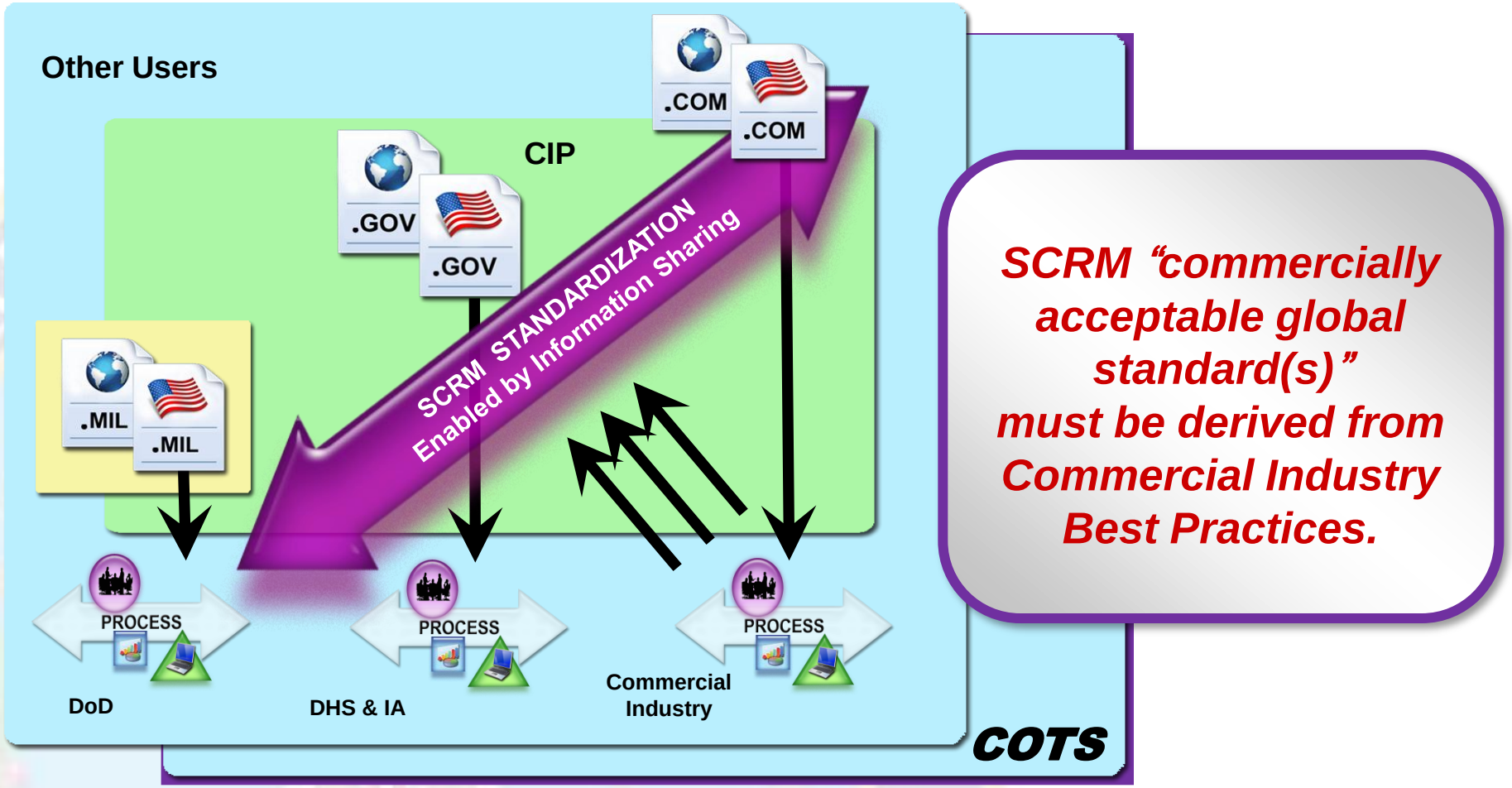
Slippery Slope / Unmeasurable Reqts

Lower Cost usually means Higher RISK

Risk

SCRM Stakeholders

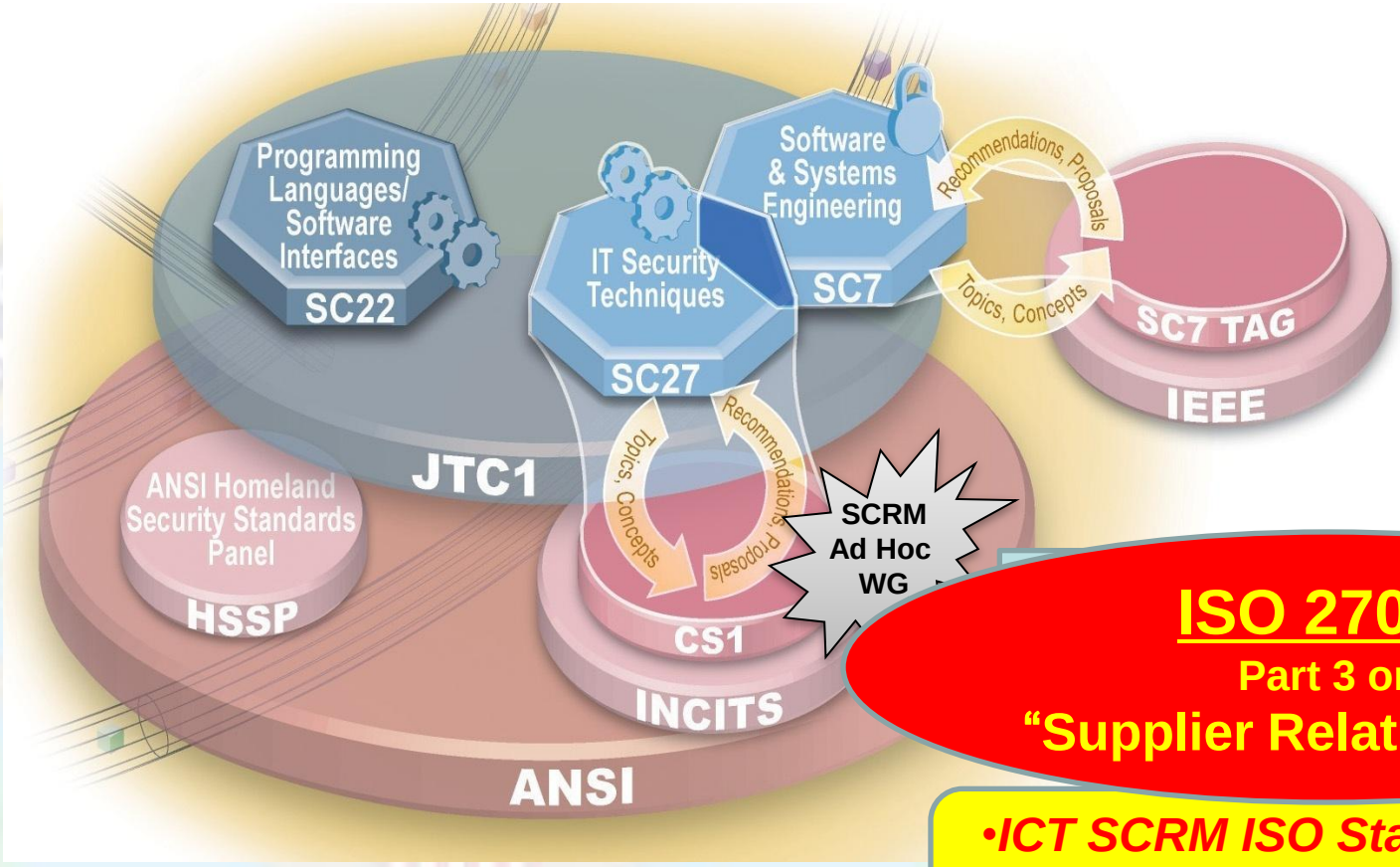
US has vital interest in the global supply chain.



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

SCRM Standardization Requires Public-Private Collaborative Effort

ISO 27036: Information technology – Security techniques –Information Security for Supplier Relationships



ISO 27036

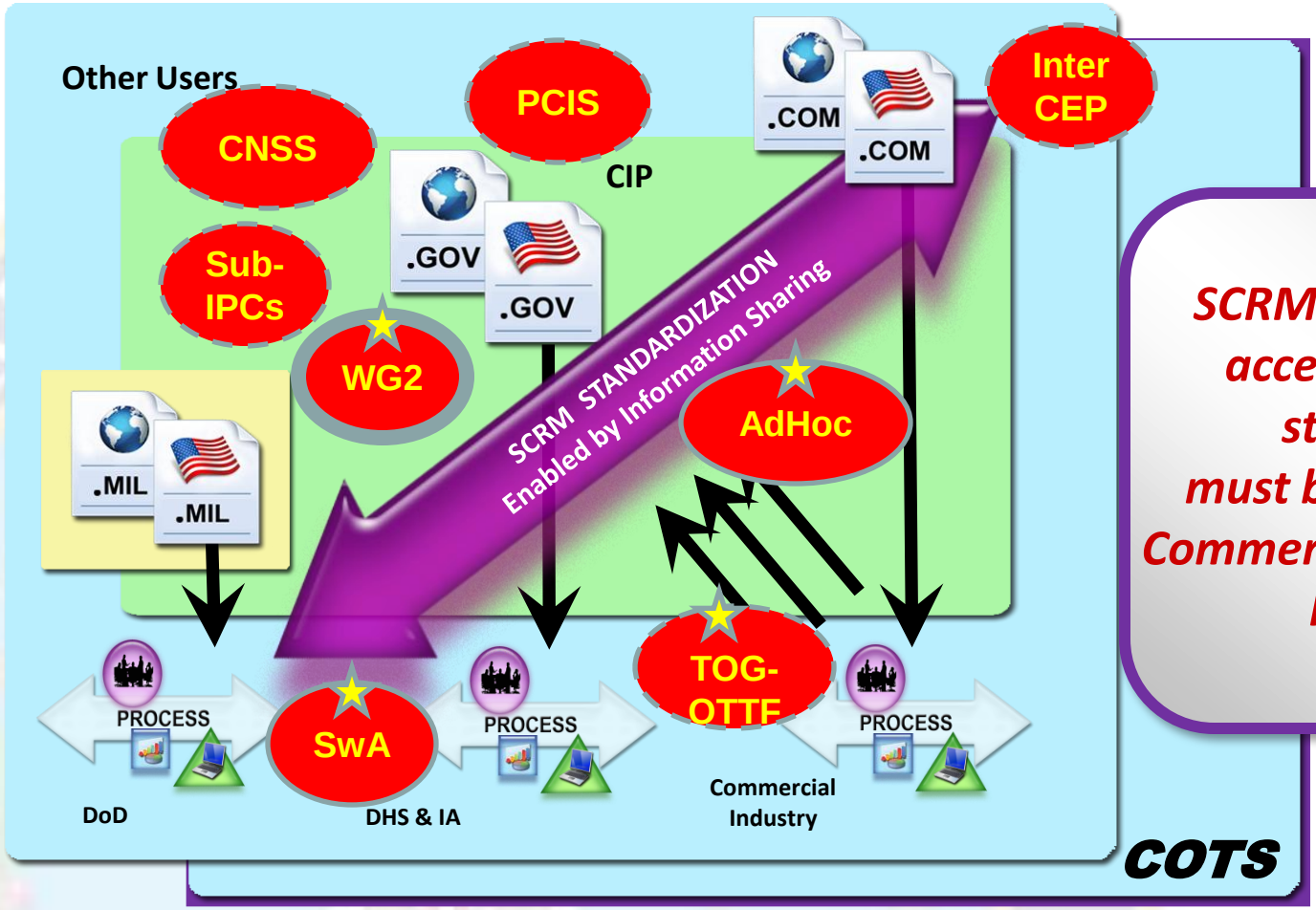
Part 3 on

"Supplier Relationships"

- *ICT SCRM ISO Standard*
- *Development 2010-2013*
- *Adoption 2013-2016*

SCRM Landscape of activities

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

Collecting Data: "*Understanding the Challenges*"

- Assessing Cyber Supply Chain Security Vulnerability within the US Critical Infrastructure--- Jon Oltsik (ESF)
- IT Supply Chain Research on Industry Perspectives--- Sandy Boysen (UMD)
- Software Supply Chain Risk Management from Products to Systems of Systems--- Carol Woody (SEI)
- Critical Code Model for Supply Chain issues---

  Bill Scherlis (CMU)

CYBERSECURITY

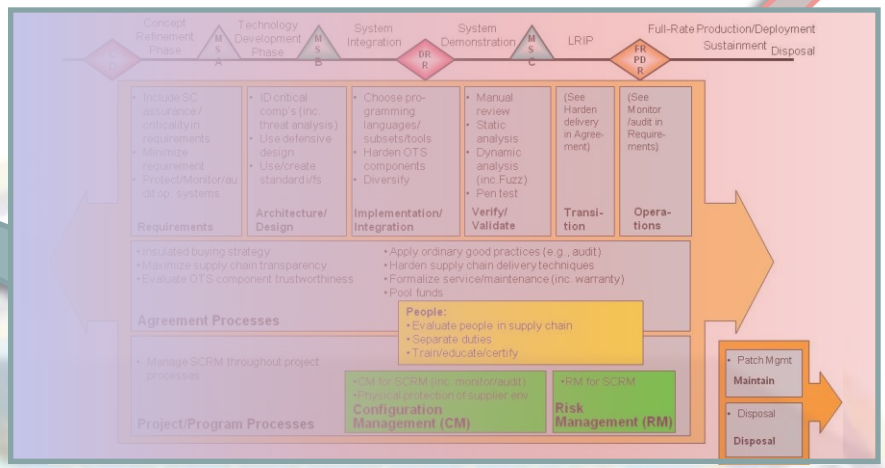
"Govt. Activities w/ SCRM & SwA Equities"

- CNCI-SCRM Section 254 Report --- Don Davidson (DoD)

  Countering Counterfeits Tiger Team (C2T2)
- Sub-IPC on CyberSecurity Standardization--- Don Davidson (DoD)
- White House Office of Science & Technology Policy (OSTP)

  call for input on S&T standardization---Ajit Jillavenkatesa (NIST)
- White House Office of Intellectual Property Enforcement Coordinator (IPEC)---Mike Powers (NASA)
- DoD Office Diminishing Manufacturing Sources and Material Shortages (DMSMS) ---Alex Melnikov (DoD)

SCRM & C2T2 in the DoD Lifecycle



"**CNCI-SCRM is** multi-pronged approach for global supply chain risk management. …Managing this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices."

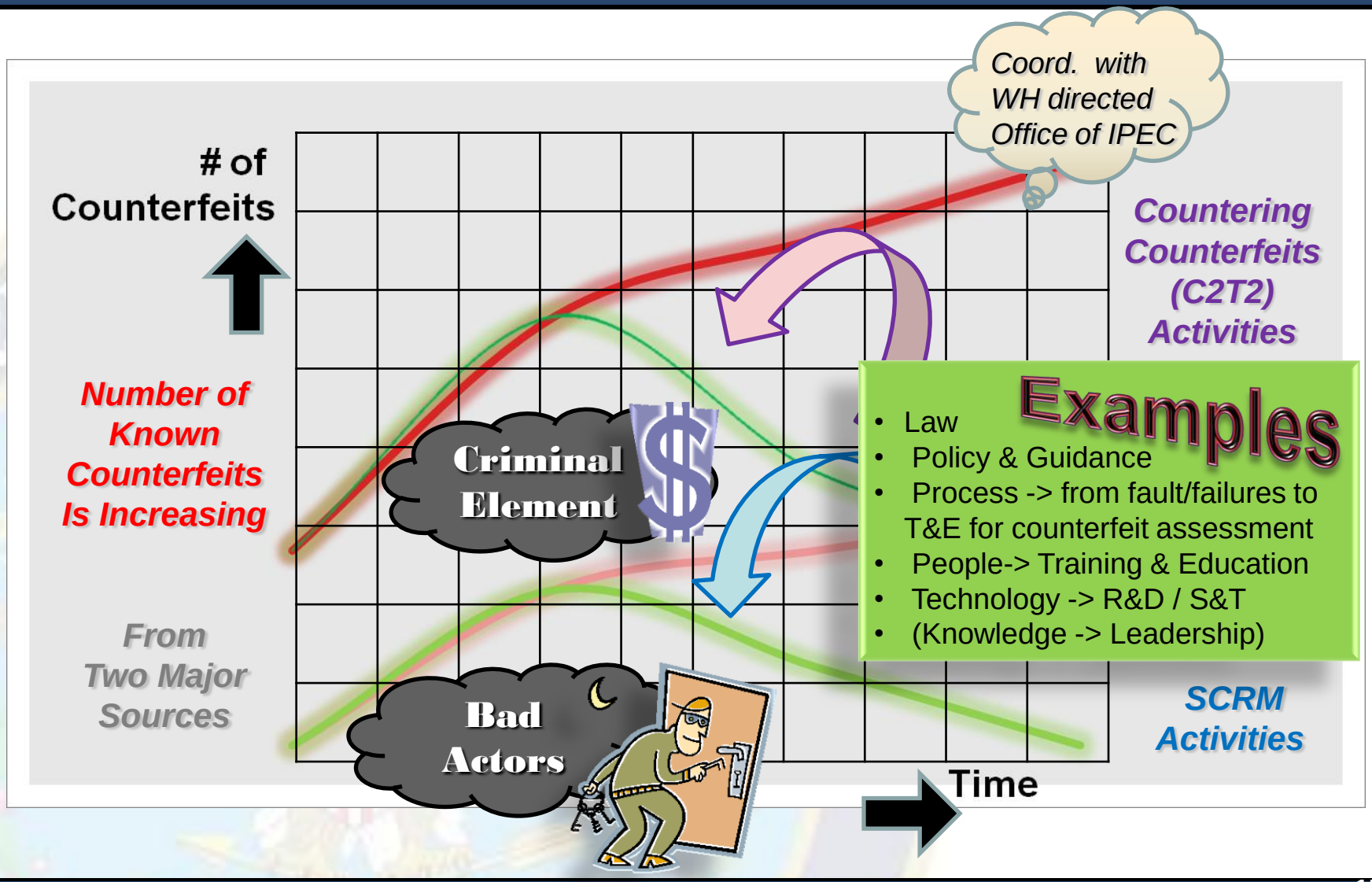
254 Report Identified a Need for a Plan-of-Action on

COUNTERING COUNTERFEITS

especially during

OPERATIONS & SUSTAINMENT

Countering Counterfeits Strategic Concept



C2T2 Process-to-Product

Work with new WH directed IPR.gov Task Force!

C2T2 Task

"…Address DoD's vulnerabilities associated with counterfeits in our supply chains and methods to mitigate risks caused by those counterfeits."

Developing a DoD "Countering Counterfeits" **holistic strategy** to reduce & manage risks from counterfeits in the supply chain

C2T2 Strategy

- ✓ Investigated Situation,
- ✓ Drafted Mission, Vision, Goals, "Definition"
- ✓ Identified "Countering Counterfeits" Activities ,
- ✓ Conducted Preliminary Gap Analysis,

to better enable DoD to prevent, detect, and respond to counterfeits

- ✓ Drafted DTM & POAM

C2T2 Way Ahead

Appoint OPR

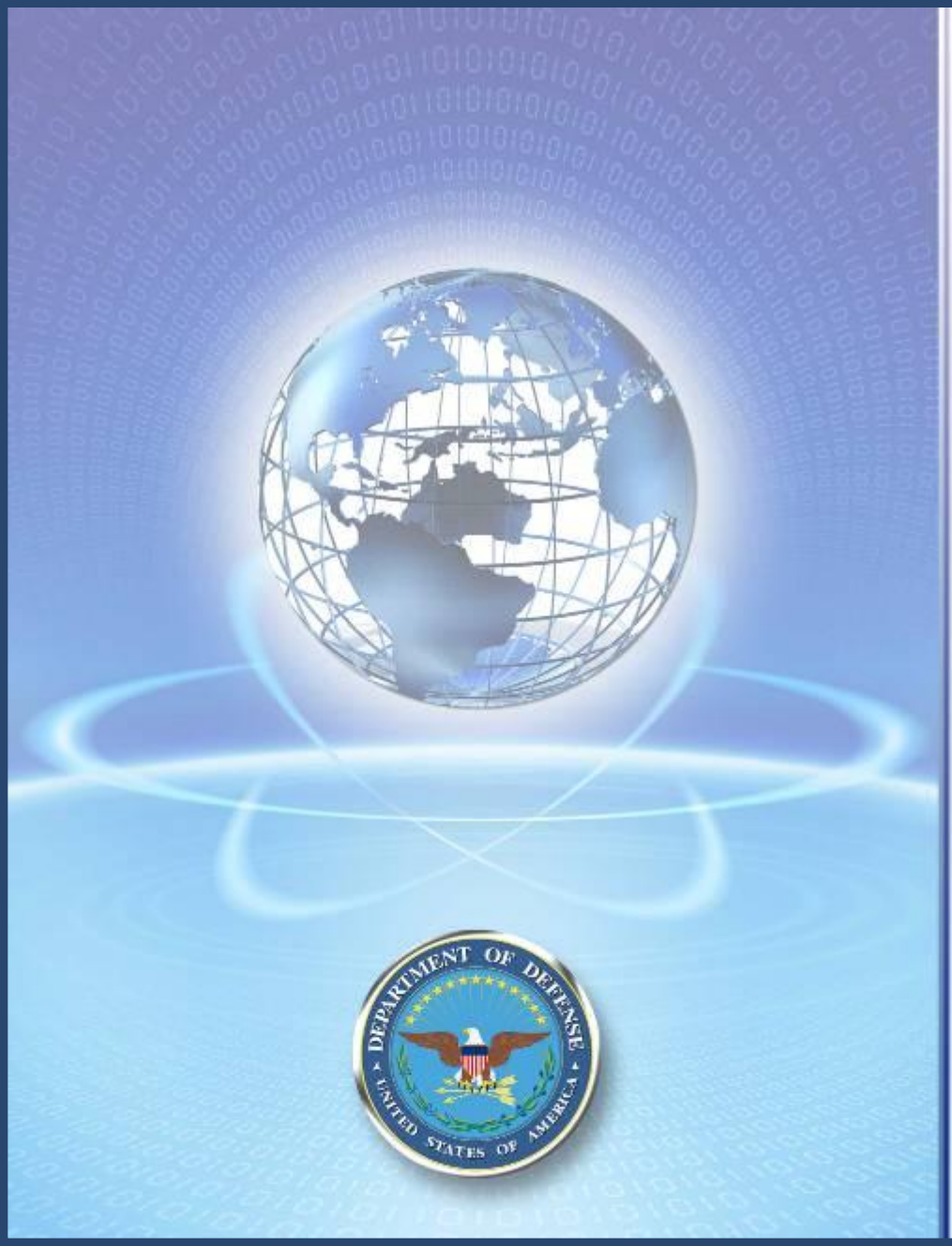
Finalize DTM & POAM

- Policy
- Processes (with Metrics)
- Resources

… to implement Strategy

Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec
22 Dec'09 C2T2 Memorandum		Data Collection & Meetings		Tri-Chair Updates		Site Visits / Analysis & Meetings		AT&L / NII Strategy UPDATE	Way Ahead C2T2 → OPR			Dec'10 OPR, DTM & POAM

Some Key ICT Applications / Core Areas of Cyber Security Standardization	Cloud Computing	First Responders	Industrial Control Systems	Health IT	Smart Grid	Telecommuting	Voting
Cryptographic Techniques							
Cyber Incident Management							
ICT System Security Evaluation							
Identity Management							
Information Security Management Systems							
Network Security							
Privacy							
Software Assurance							
Supply Chain	New Standards Needed	New Standards Needed	New Standards Needed	New Standards Needed	New Standards Needed	New Standards Needed	New Standards Needed
System Security Engineering							



CNCI-SCRM

US Comprehensive National Cybersecurity Initiative – Supply Chain Risk Management

Mr. Donald Davidson,
Chief, Outreach & Standardization
Trusted Mission Systems & Networks
(formerly Globalization Task Force, GTF)
OASD (NII) / DoD CIO

Don.Davidson@osd.mil