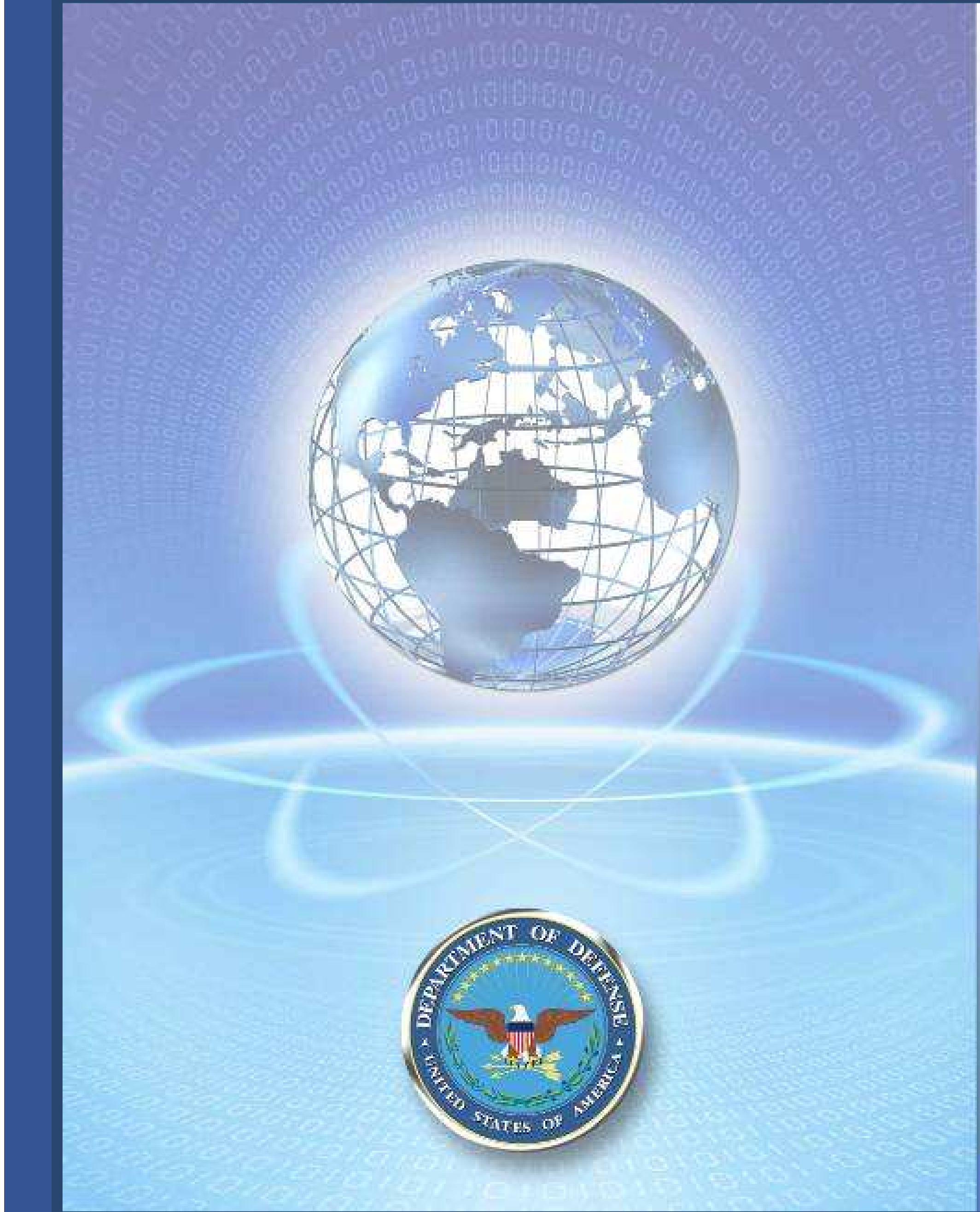


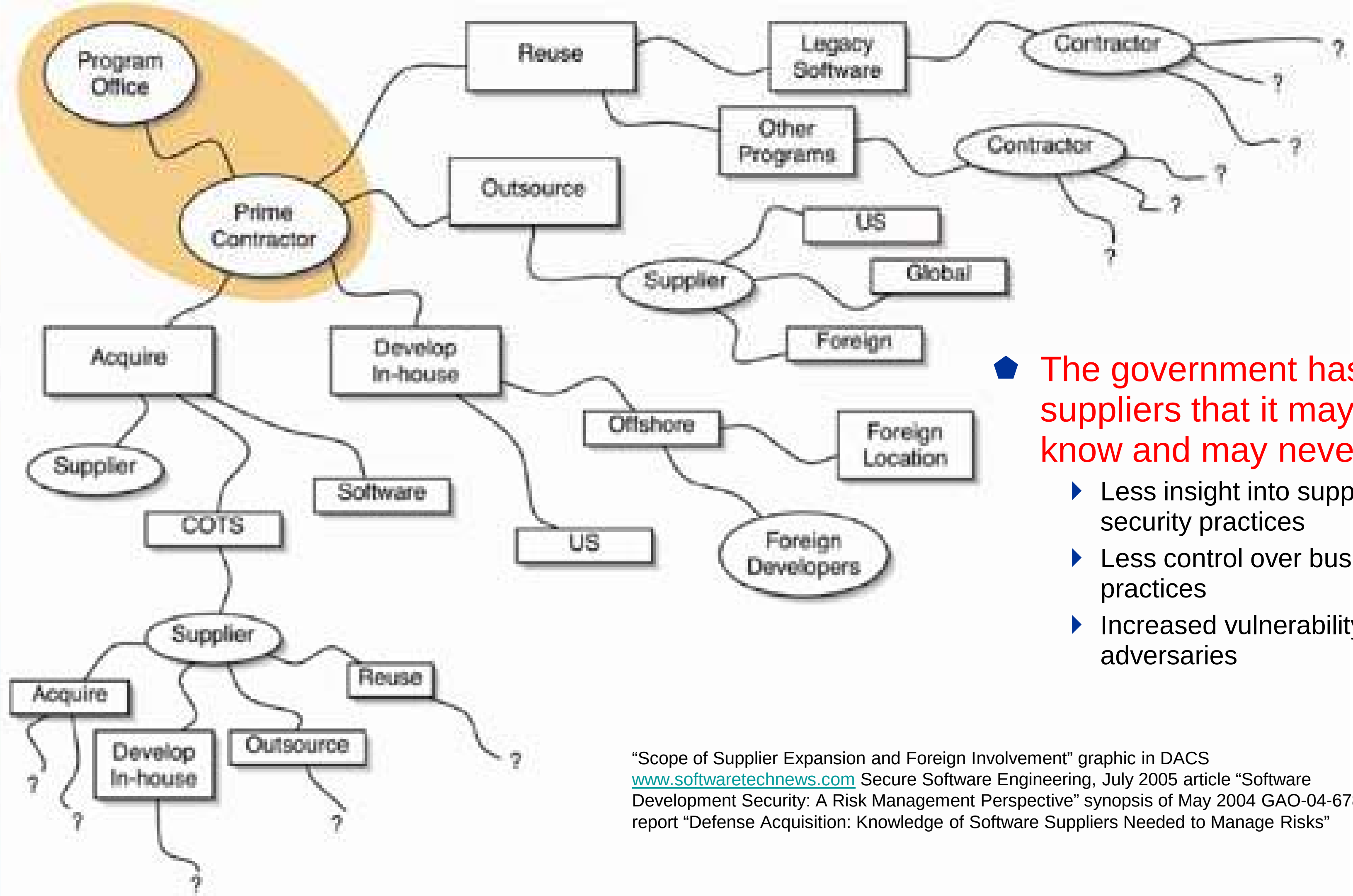
# CNCI-SCRM

## 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

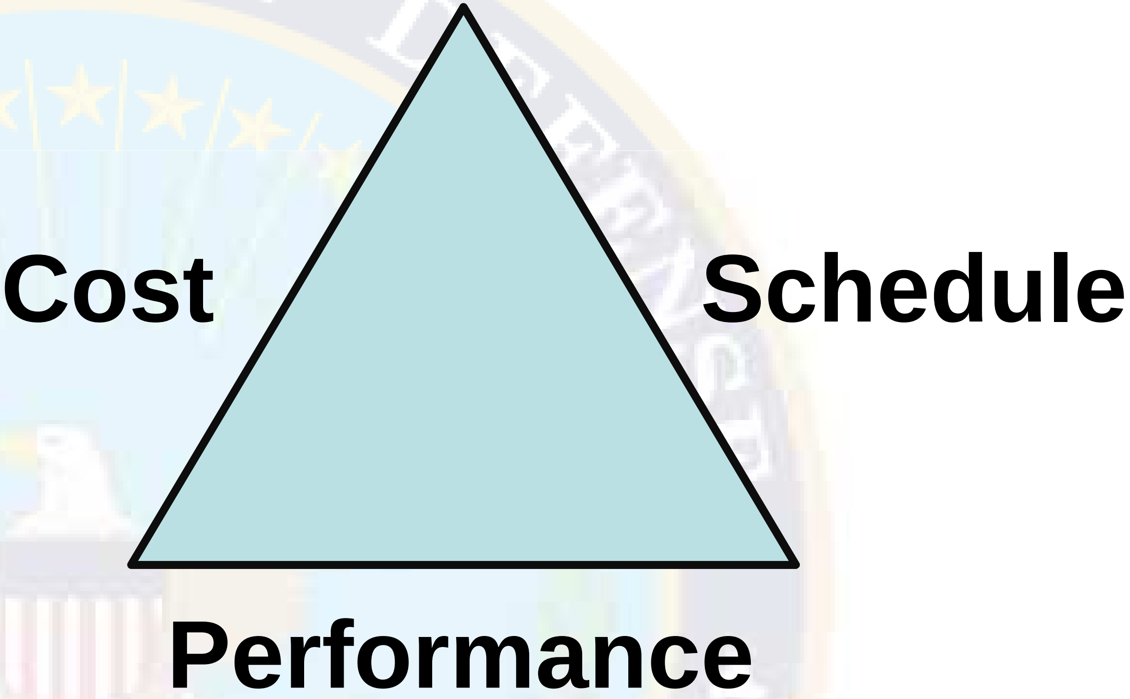
# Globalization brings challenges to DoD…



- 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”

# What’s the Impact of a Globalized Supply Chain



# Globalization brings challenges to DoD…

Program Office
Reuse
Legacy Software
Contractor
?
?
?
Other Programs
Contractor
Acqu
Supplier
Acquire
De
In-
?
?
?

Acquirers

Systems Integrators

Suppliers

PROCESS

## Hardware. Software & Services

# 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
- 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**

# 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."

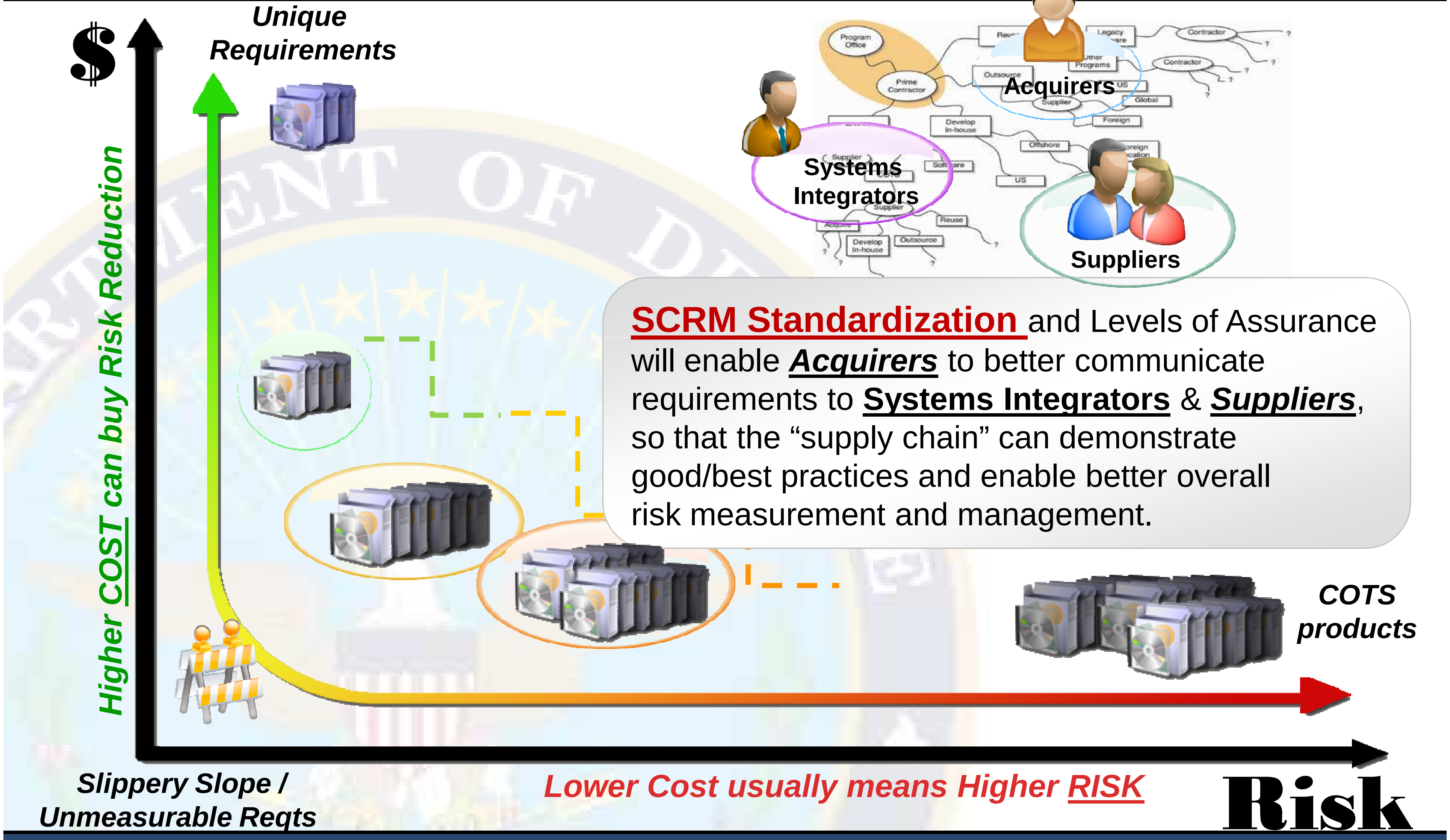
**<u>254 Report</u>**
**Identified a Need for a Plan-of-Action on**

**<u>COUNTERING COUNTERFEITS</u>**

**especially during**

**<u>OPERATIONS & SUSTAINMENT</u>**

# Product Assurance *TRADESPACE*

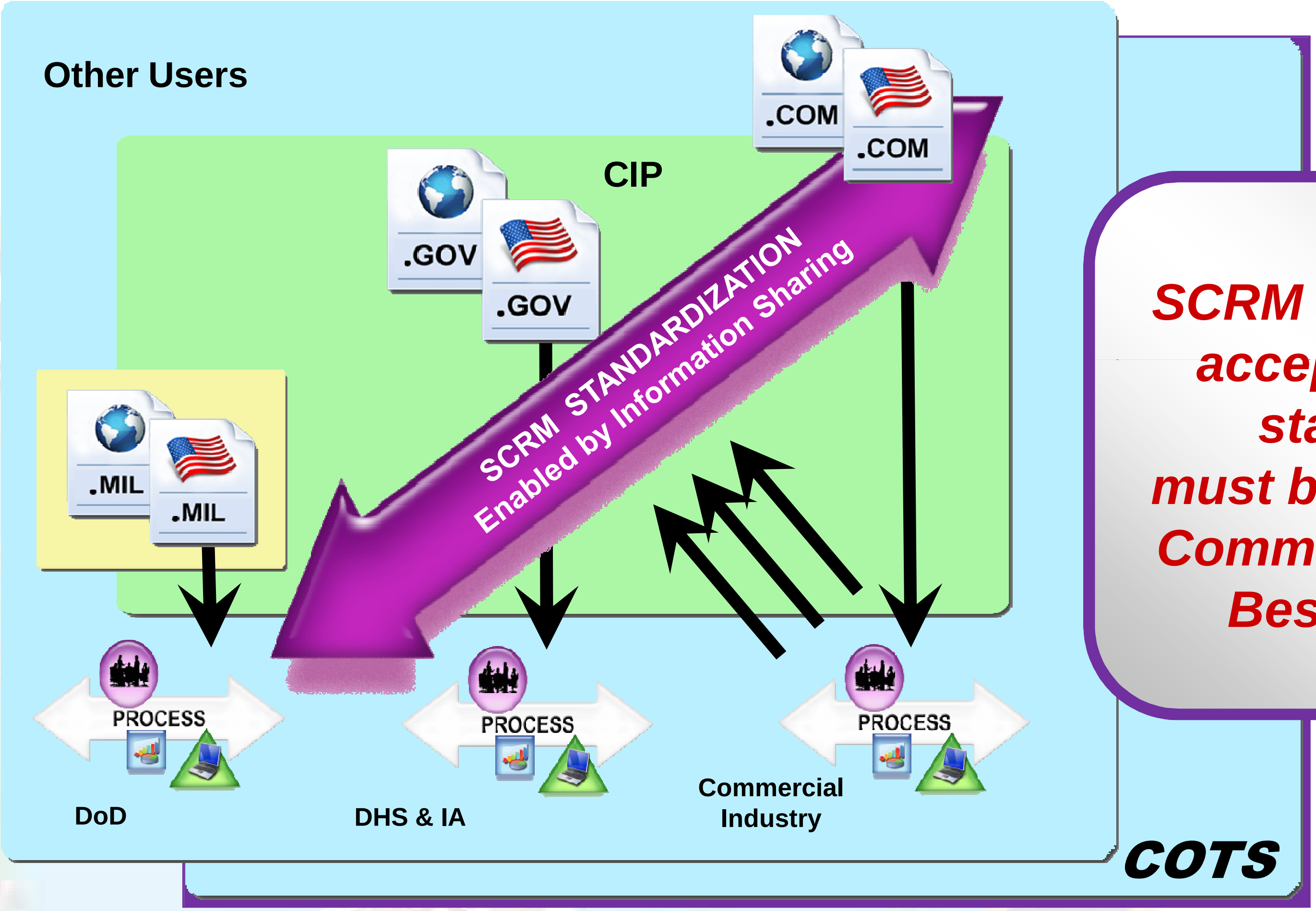


**SCRM Standardization** and Levels of Assurance will enable ***Acquirers*** to better communicate requirements to **Systems Integrators** & ***Suppliers***, so that the "supply chain" can demonstrate good/best practices and enable better overall risk measurement and management.

*Lower Cost usually means Higher RISK*

# SCRM Stakeholders

*US has vital interest in the global supply chain.*

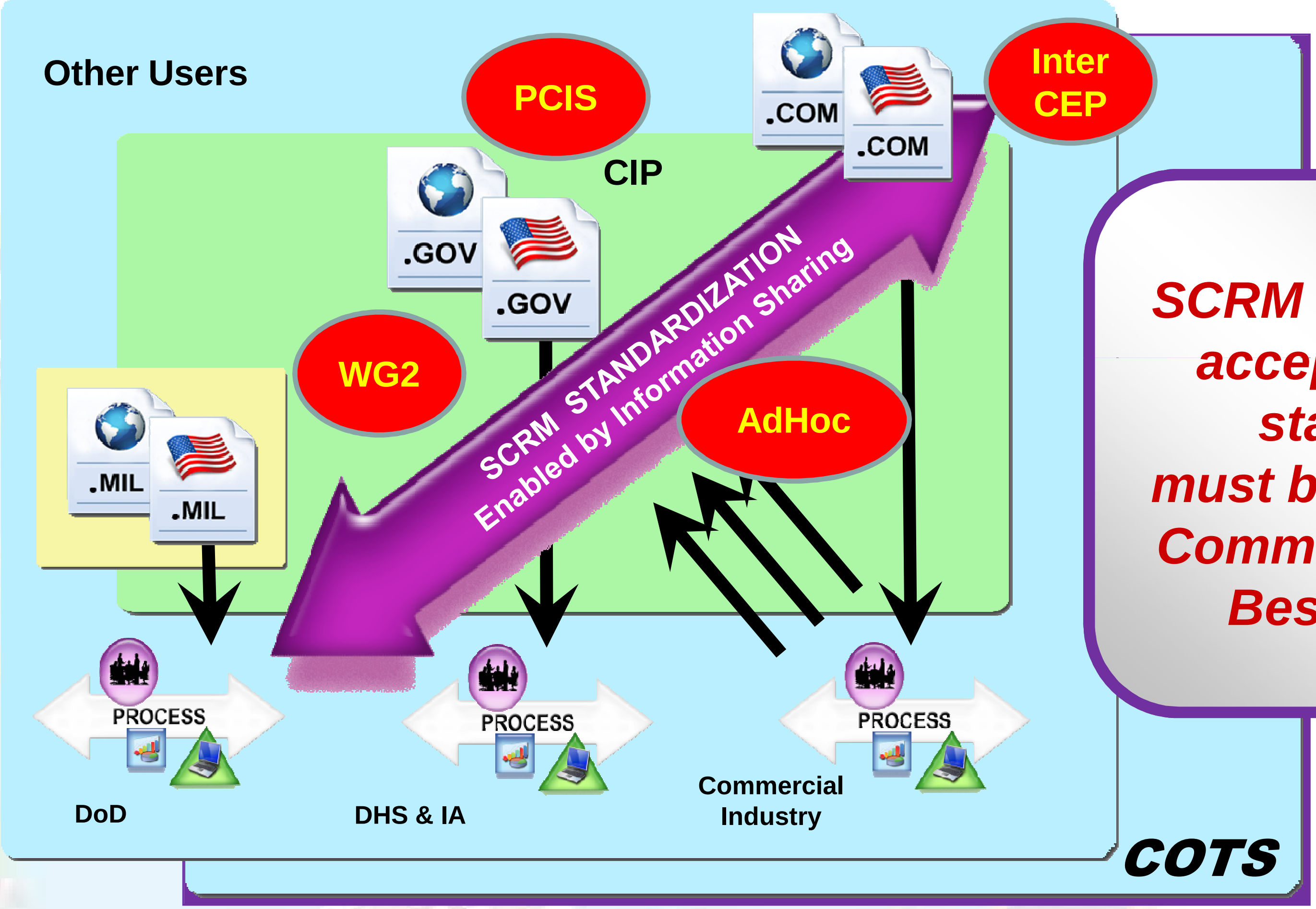


*SCRM "commercially acceptable global standard(s)" must be derived from Commercial Industry Best Practices.*

*SCRM Standardization Requires Public-Private Collaborative Effort*

# SCRM Stakeholders

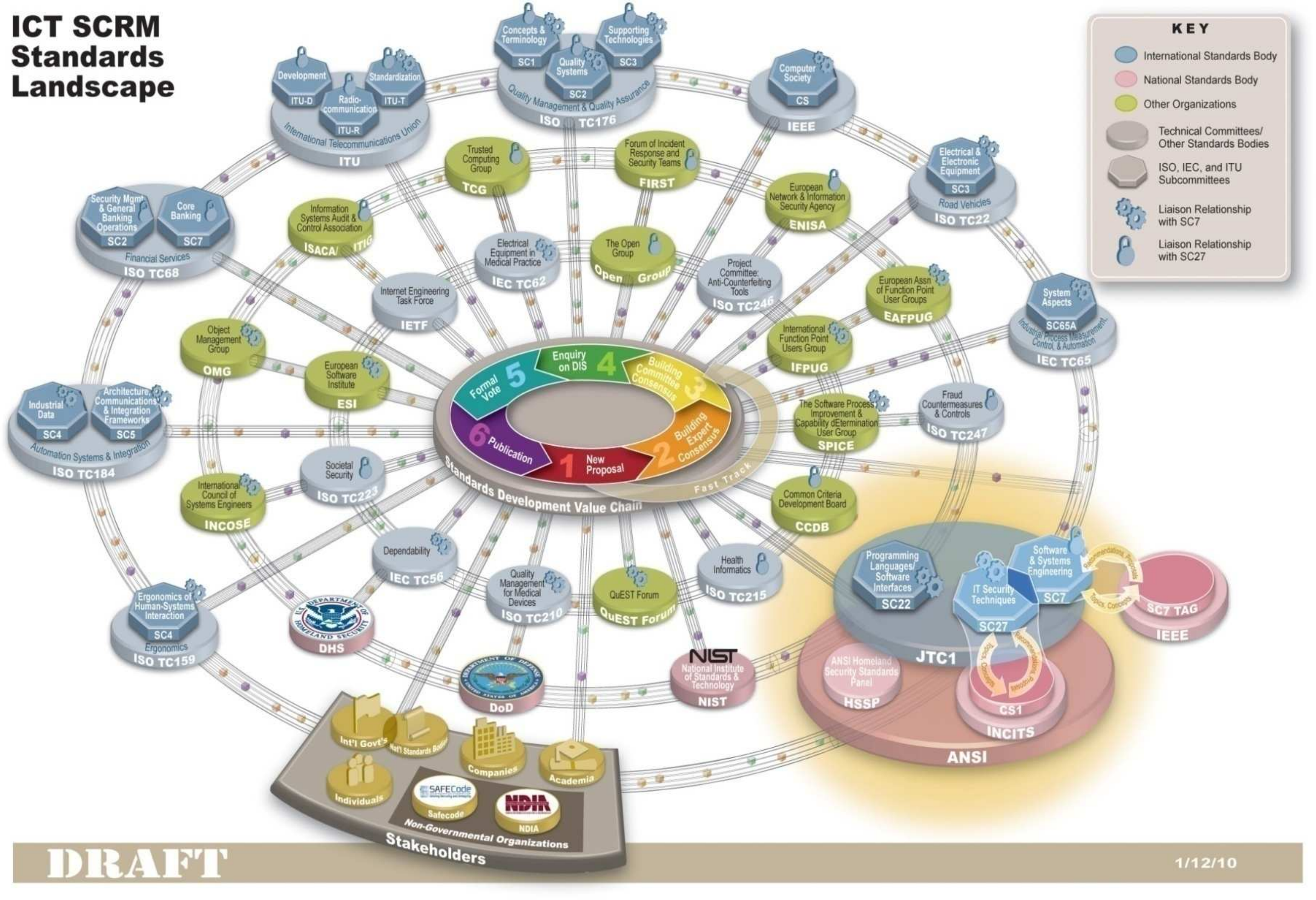
*US has vital interest in the global supply chain.*



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

*SCRM Standardization Requires Public-Private Collaborative Effort*

# Standards Development Organizations
# SDOs Landscape: SCRM Perspective



ICT SCRM Standards Landscape

KEY

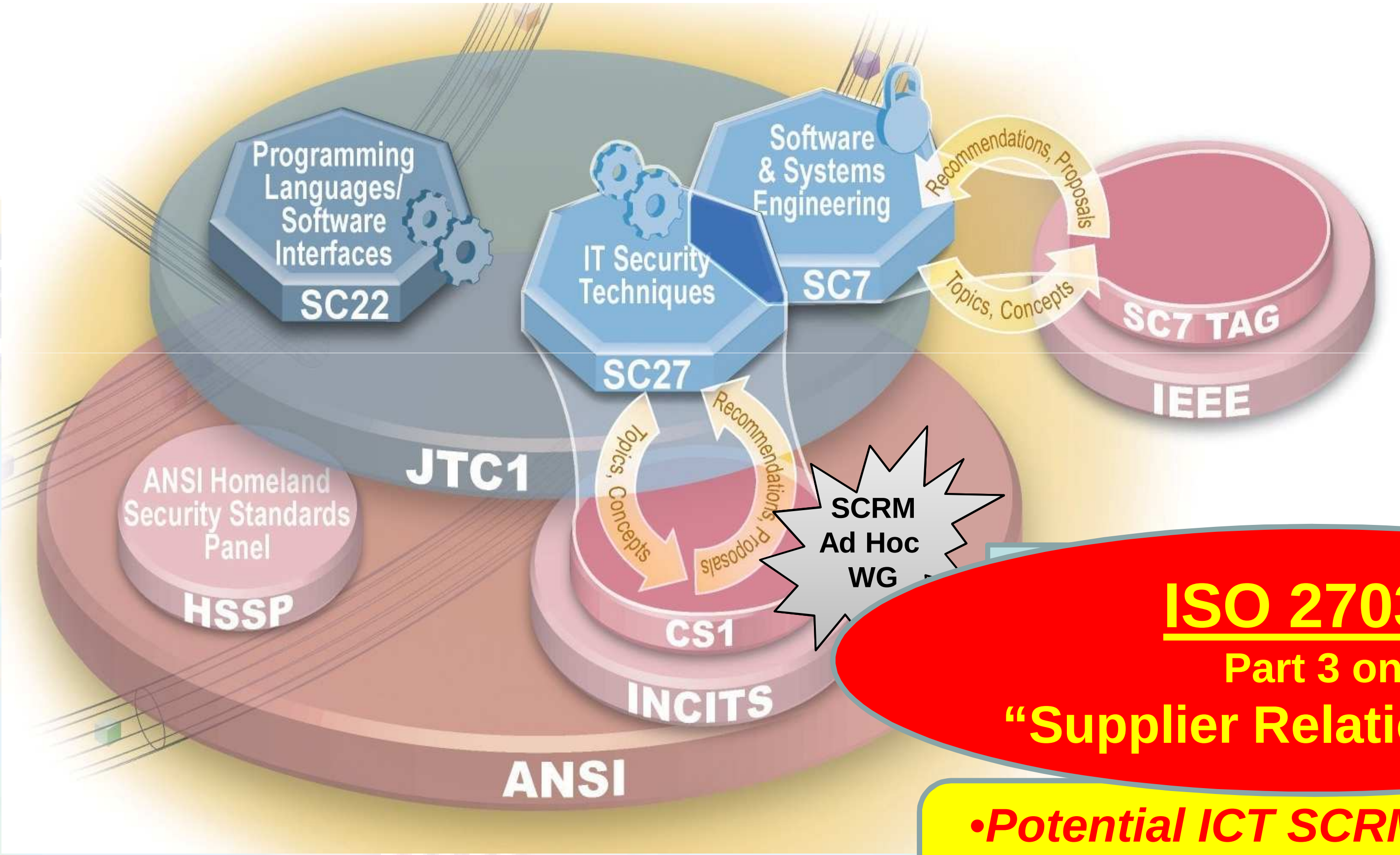
- 🔵 International Standards Body
- 🔴 National Standards Body
- 🟢 Other Organizations
- Technical Committees/ Other Standards Bodies
- ISO, IEC, and ITU Subcommittees
- ⚙ Liaison Relationship with SC7
- 🔒 Liaison Relationship with SC27

Development
ITU-D
Radio-communication
ITU-R
Standardization
ITU-T
International Telecommunications Union
ITU
Concepts & Terminology
SC1
Quality Systems
SC2
Supporting Technologies
SC3
Quality Management & Quality Assurance
ISO TC176
Computer Society
CS
IEEE
Electrical & Electronic Equipment
SC3
Road Vehicles
ISO TC22
System Aspects
SC65A
Industrial Process Measurement, Control, & Automation
IEC TC65
Security Mgmt & General Banking Operations
SC2
Core Banking
SC7
Financial Services
ISO TC68
Trusted Computing Group
TCG
Forum of Incident Response and Security Teams
FIRST
European Network & Information Security Agency
ENISA
Information Systems Audit & Control Association
ISACA/ ITIG
Electrical Equipment in Medical Practice
IEC TC62
The Open Group
Open Group
Project Committee: Anti-Counterfeiting Tools
ISO TC246
European Assn of Function Point User Groups
EAFPUG
Internet Engineering Task Force
IETF
Object Management Group
OMG
European Software Institute
ESI
International Function Point Users Group
IFPUG
Industrial Data
SC4
Architecture, Communications & Integration Frameworks
SC5
Automation Systems & Integration
ISO TC184
Enquiry on DIS
4
Building Committee Consensus
3
Building Expert Consensus
2
New Proposal
1
Publication
6
Formal Vote
5
Fast Track
Standards Development Value Chain
The Software Process Improvement & Capability dEtermination User Group
SPICE
Fraud Countermeasures & Controls
ISO TC247
Societal Security
ISO TC223
International Council of Systems Engineers
INCOSE
Common Criteria Development Board
CCDB
Dependability
IEC TC56
Health Informatics
ISO TC215
Quality Management for Medical Devices
ISO TC210
QuEST Forum
QuEST Forum
Ergonomics of Human-Systems Interaction
SC4
Ergonomics
ISO TC159
DHS
DoD
NIST
National Institute of Standards & Technology
NIST
Programming Languages/ Software Interfaces
SC22
IT Security Techniques
SC27
Software & Systems Engineering
SC7
Recommendations, Proposals
Topics, Concepts
SC7 TAG
IEEE
JTC1
ANSI Homeland Security Standards Panel
HSSP
Topics, Concepts
Recommendations, Proposals
CS1
INCITS
ANSI
Int'l Govt's
Nat'l Standards Bodies
Companies
Academia
Individuals
SAFECode
Safecode
NDIA
NDIA
Non-Governmental Organizations
Stakeholders

DRAFT

1/12/10

# SCRM Study Periods: Nov'09 – Apr'10 / May-Oct'10


Programming Languages/ Software Interfaces
SC22
IT Security Techniques
SC27
Software & Systems Engineering
SC7
Recommendations, Proposals
Topics, Concepts
SC7 TAG
IEEE
JTC1
Topics, Concepts
Recommendations, Proposals
ANSI Homeland Security Standards Panel
HSSP
CS1
INCITS
ANSI

SCRM Ad Hoc WG

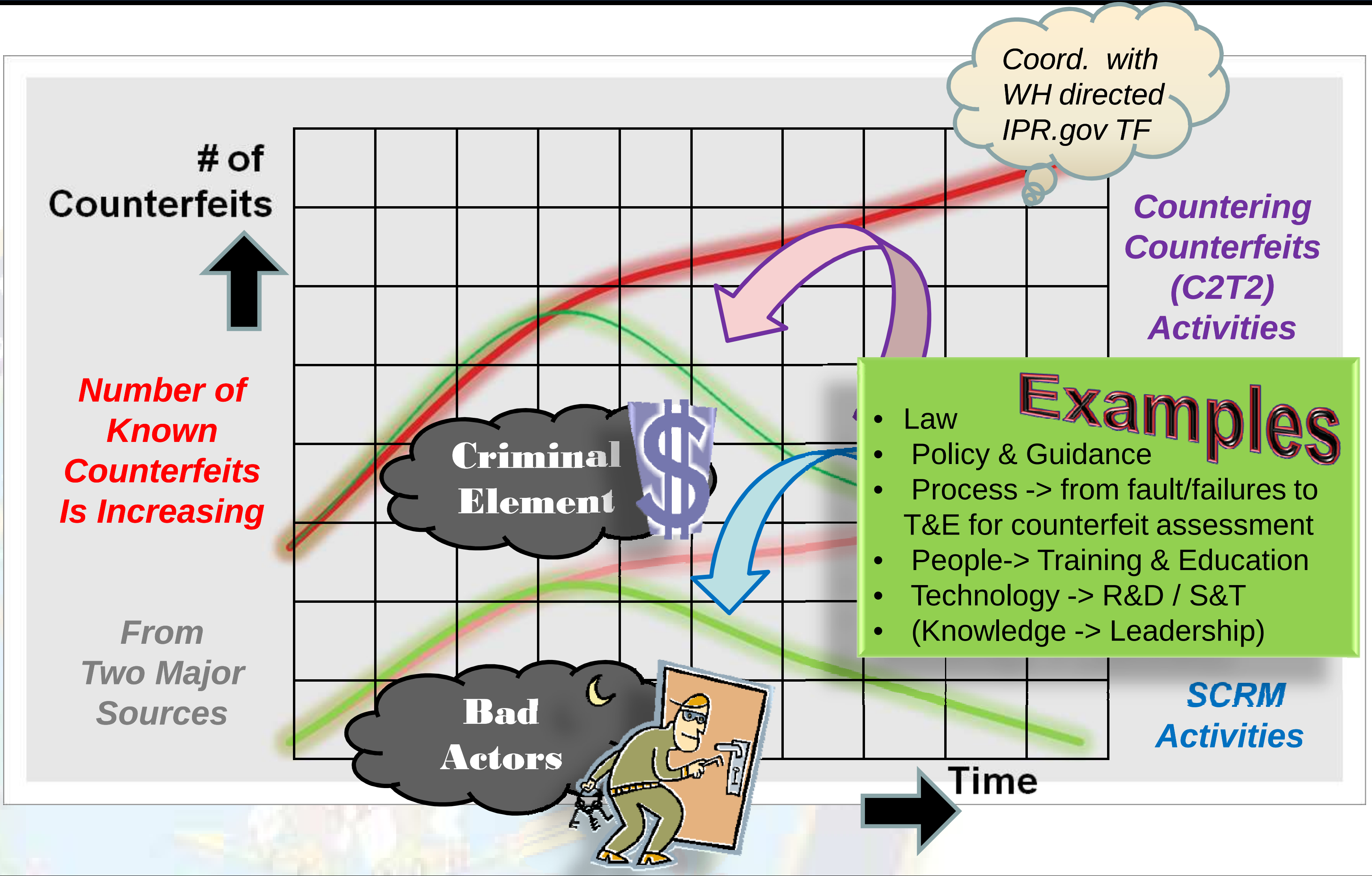
**<u>ISO 27036</u>**

**Part 3 on**

**"Supplier Relationships"**

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

# Countering Counterfeits Strategic Concept



Coord. with WH directed IPR.gov TF

*Countering Counterfeits (C2T2) Activities*

*Number of Known Counterfeits Is Increasing*

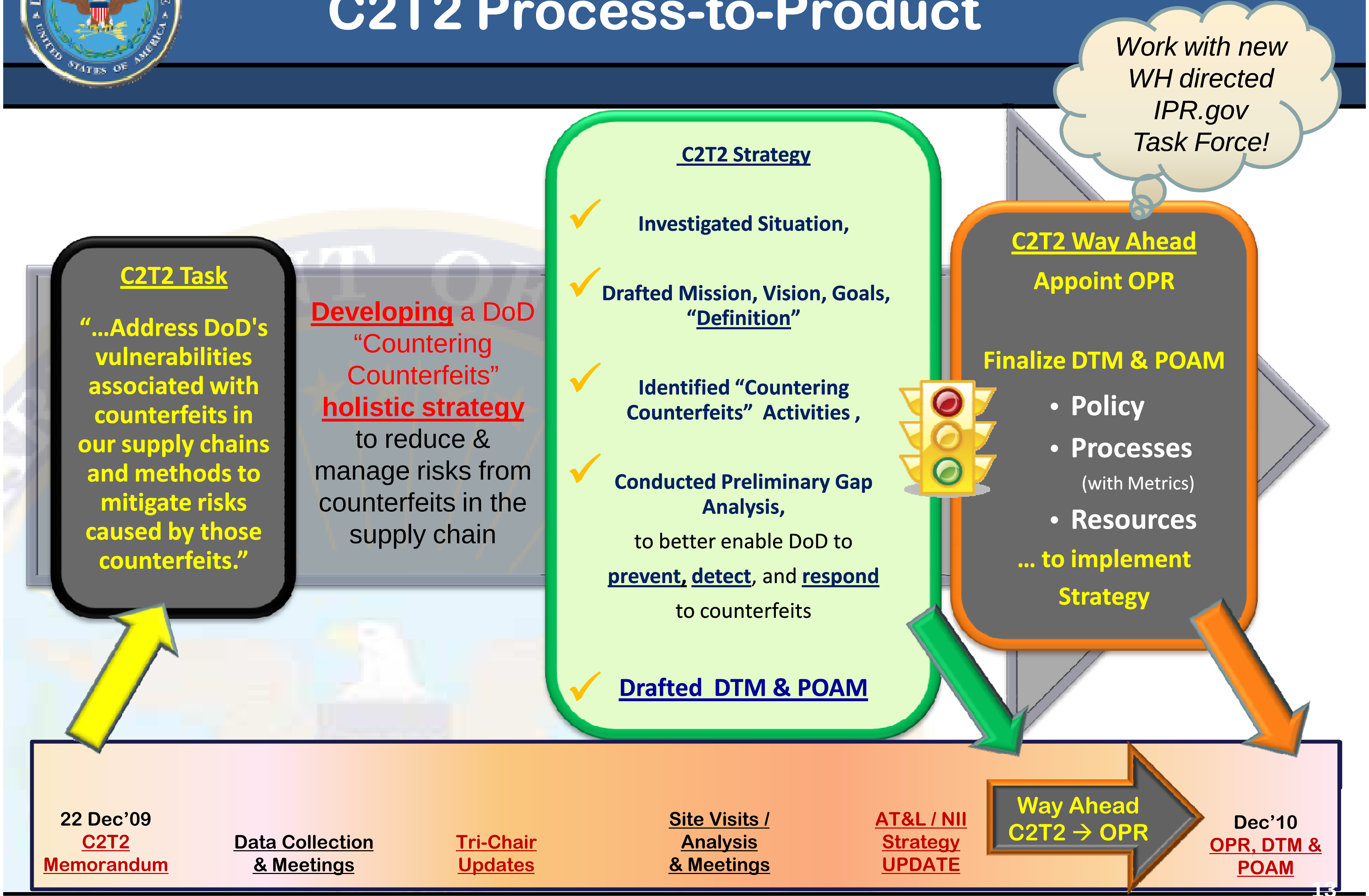
*From Two Major Sources*

*SCRM Activities*

**Examples**

- Law
- Policy & Guidance
- Process -> from fault/failures to T&E for counterfeit assessment
- People-> Training & Education
- Technology -> R&D / S&T
- (Knowledge -> Leadership)

# 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**

22 Dec'09 C2T2 Memorandum

Data Collection & Meetings

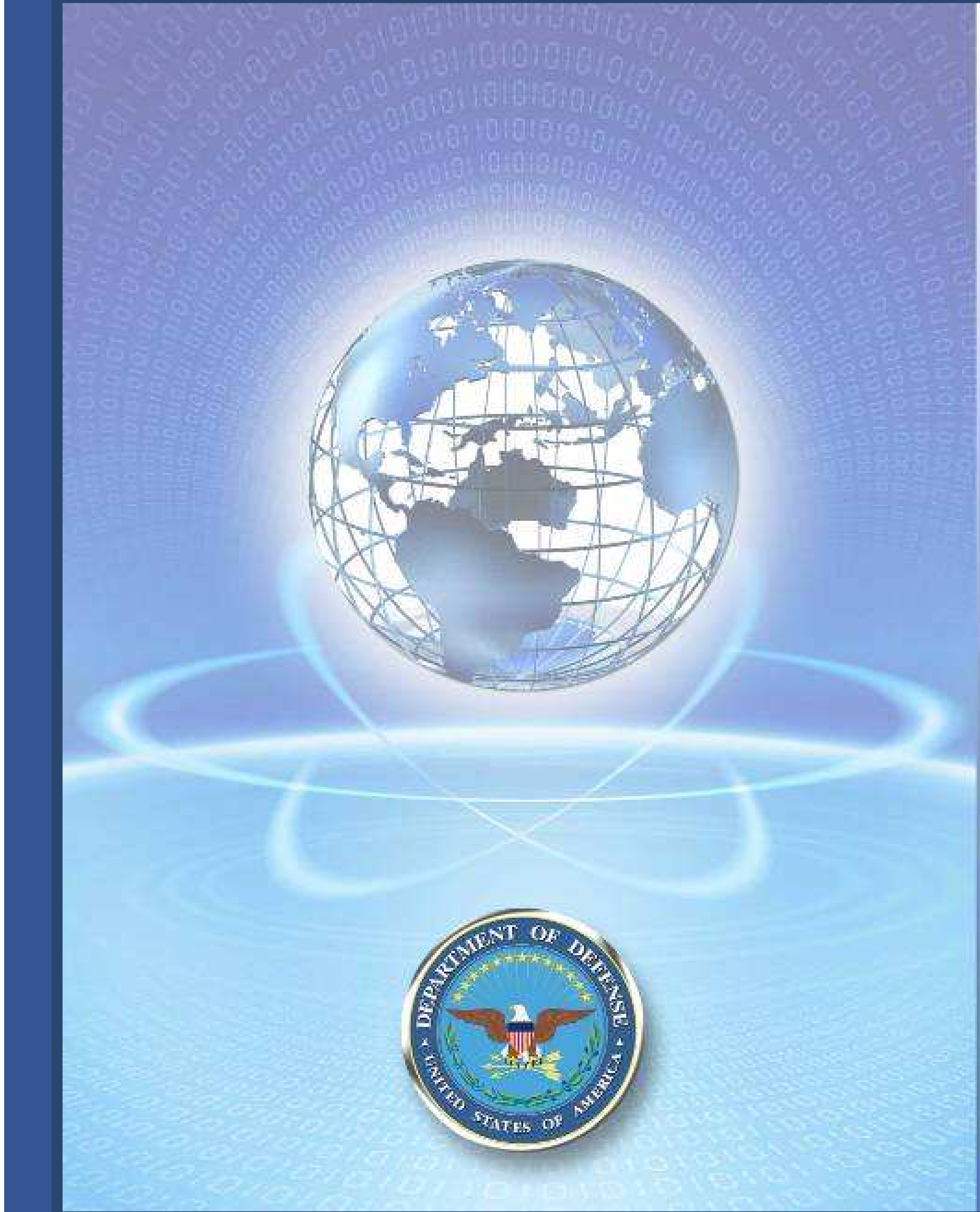
Tri-Chair Updates

Site Visits / Analysis & Meetings

AT&L / NII Strategy UPDATE

Way Ahead C2T2 → OPR

Dec'10 OPR, DTM & POAM



# 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