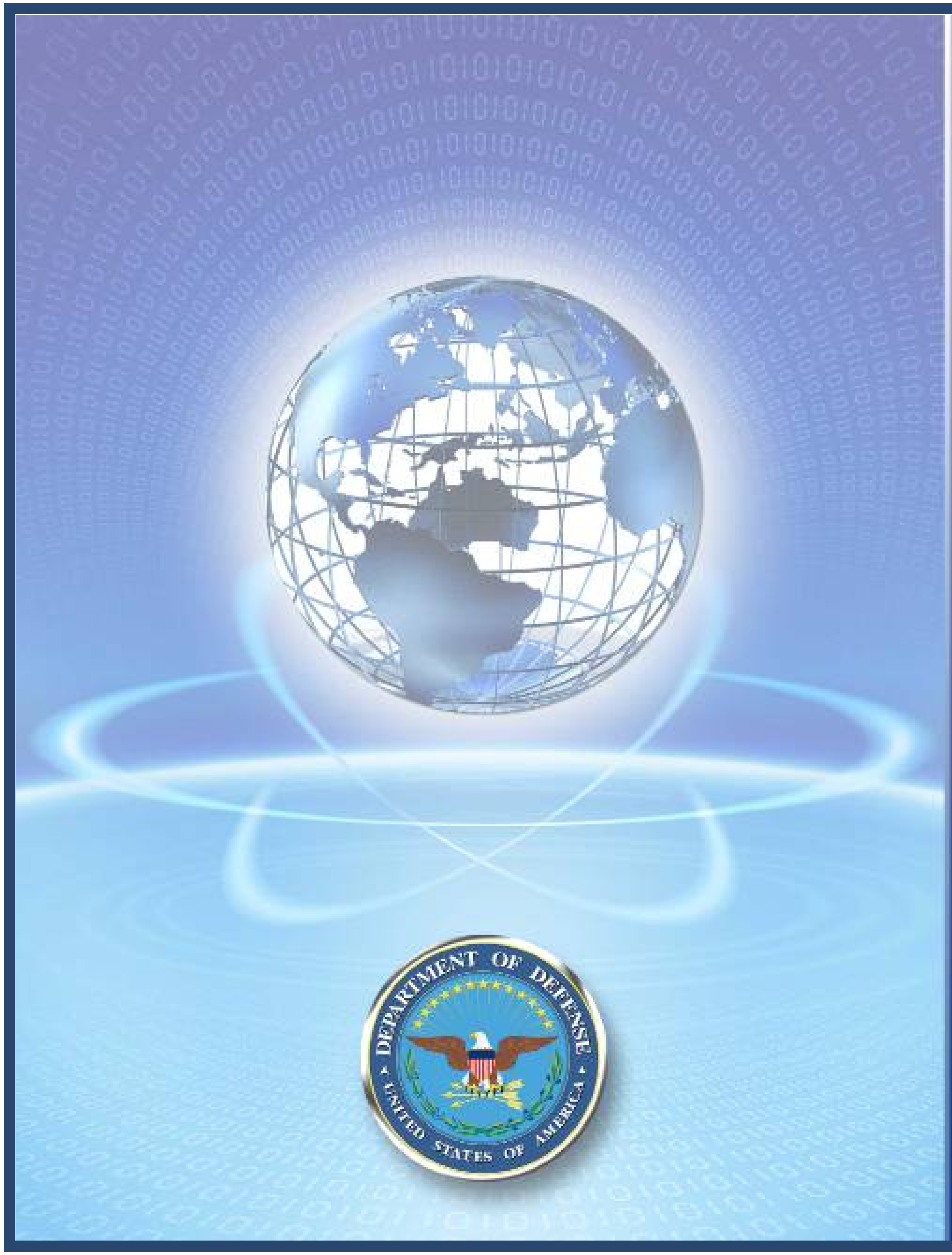


Managing Global Supply Chain Risk:

Security & Resiliency (of the Chain) and Integrity (of Product)

"How do we manage risk from Counterfeit Microelectronics & "poor" SW ?"

Mr. Donald Davidson,

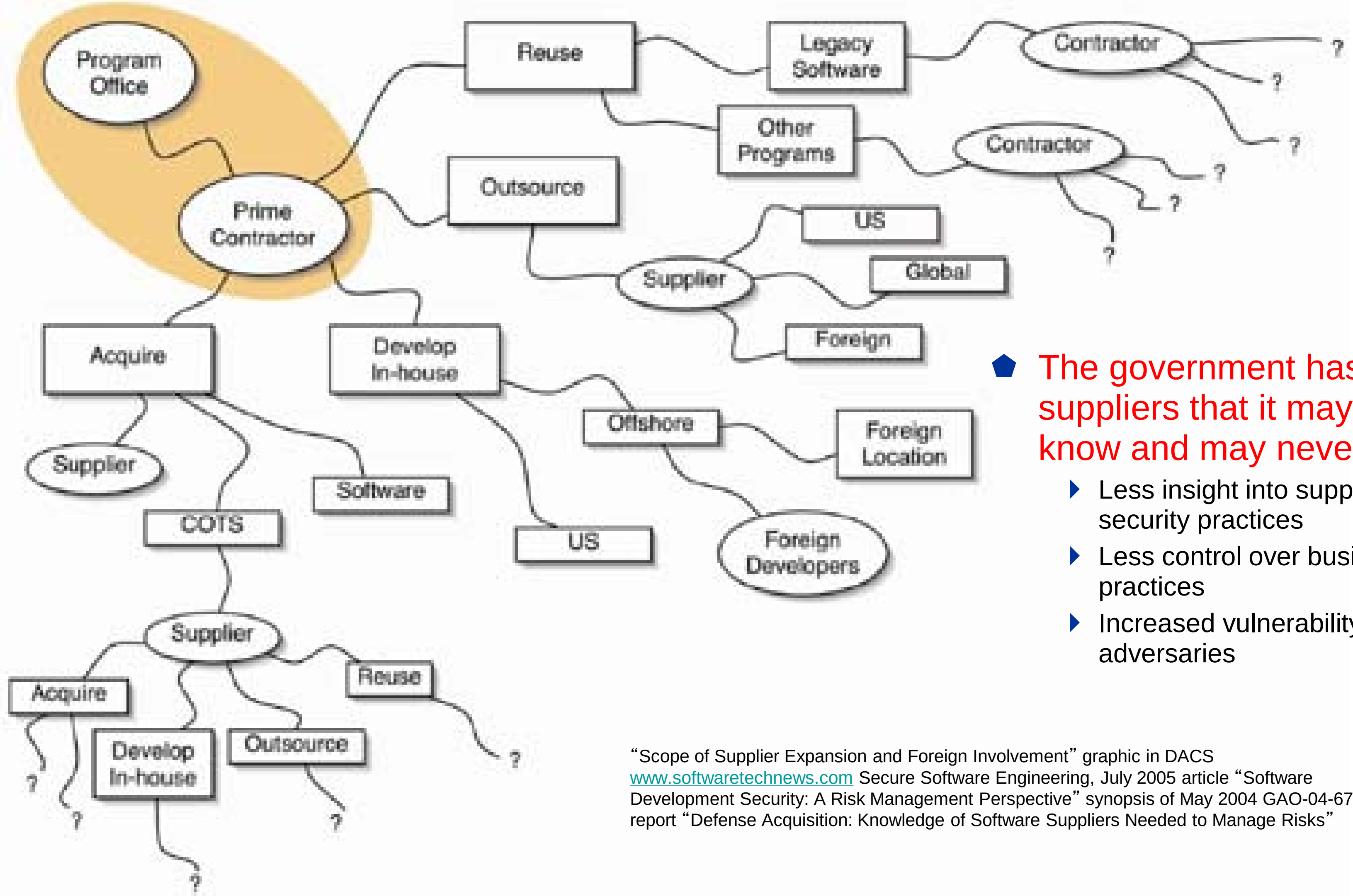
Chief, Outreach, Science & Standards

Trusted Mission Systems & Networks

Office of DoD- Deputy CIO for Cybersecurity

Don.Davidson@osd.mil

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"

Not only do we have an increasingly Global-Interdependent Supply Chain, we also have a world of capabilities that are increasingly dependent on Globally Sourced ICT

- Dependencies on technology are greater then ever

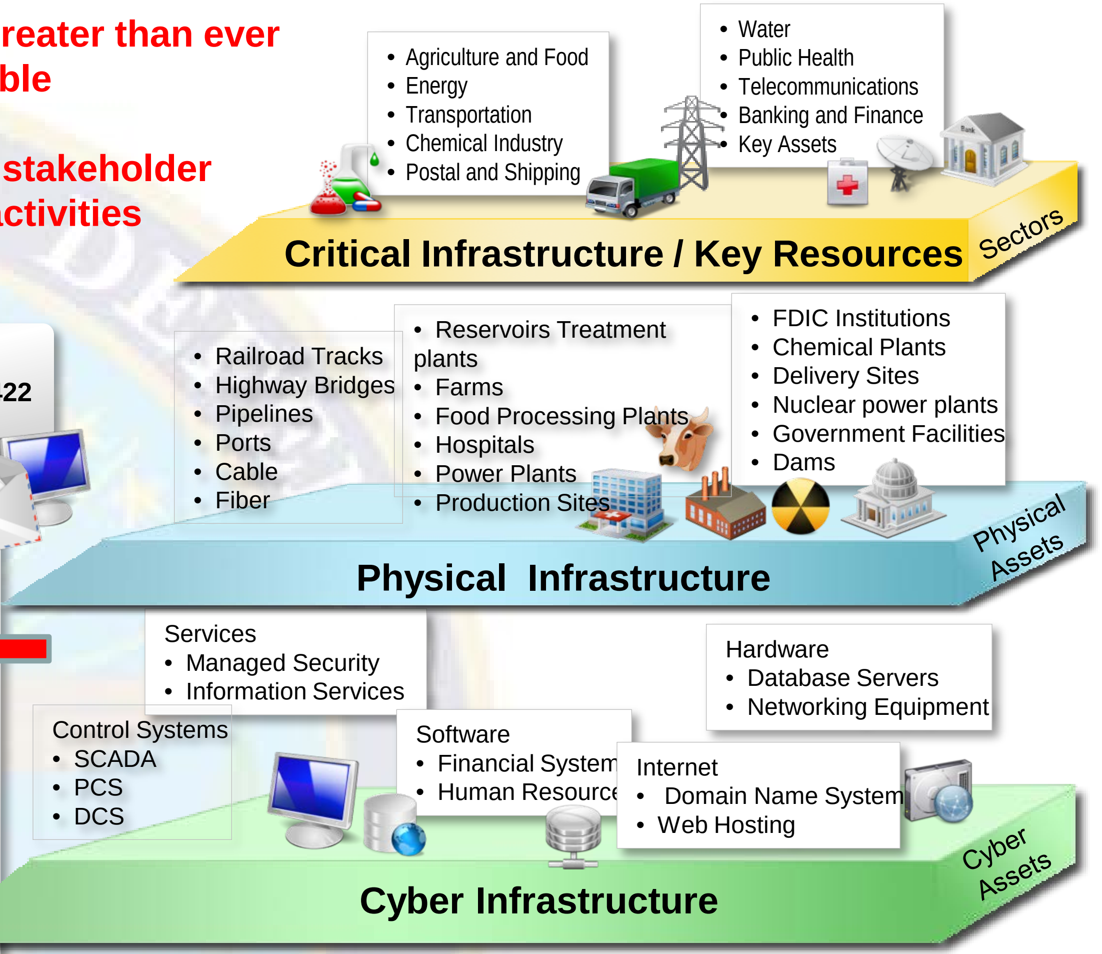
-- Possibility of disruption/sabotage is greater than ever because hardware/software is vulnerable

--- 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*



Critical Infrastructure / Key Resources — Sectors

- Agriculture and Food
- Energy
- Transportation
- Chemical Industry
- Postal and Shipping

- Water
- Public Health
- Telecommunications
- Banking and Finance
- Key Assets

Physical Infrastructure — Physical Assets

- Railroad Tracks
- Highway Bridges
- Pipelines
- Ports
- Cable
- Fiber

- Reservoirs Treatment plants
- Farms
- Food Processing Plants
- Hospitals
- Power Plants
- Production Sites

- FDIC Institutions
- Chemical Plants
- Delivery Sites
- Nuclear power plants
- Government Facilities
- Dams

Cyber Infrastructure — Cyber Assets

Services
- Managed Security
- Information Services

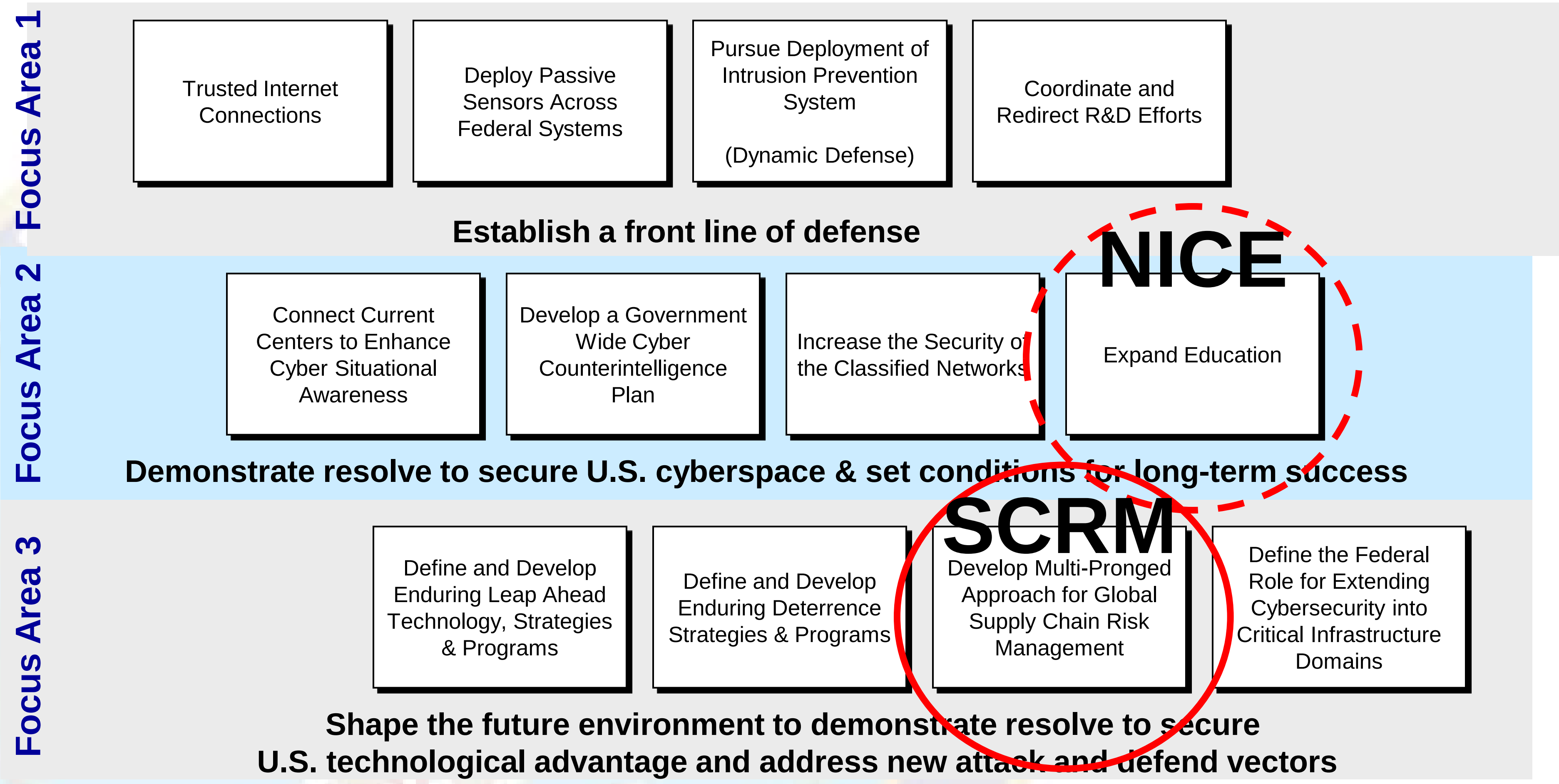
Hardware
- Database Servers
- Networking Equipment

Control Systems
- SCADA
- PCS
- DCS

Software
- Financial System
- Human Resource

Internet
- Domain Name System
- Web Hosting

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

NICE

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

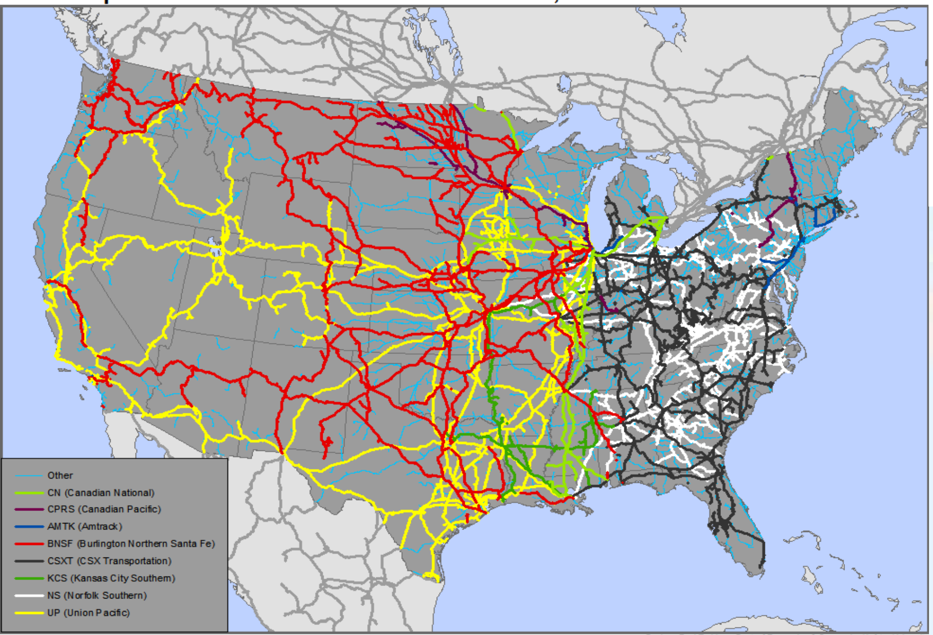
Shape the future environment to demonstrate resolve to secure U.S. technological advantage and address new attack and defend vectors

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: US 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

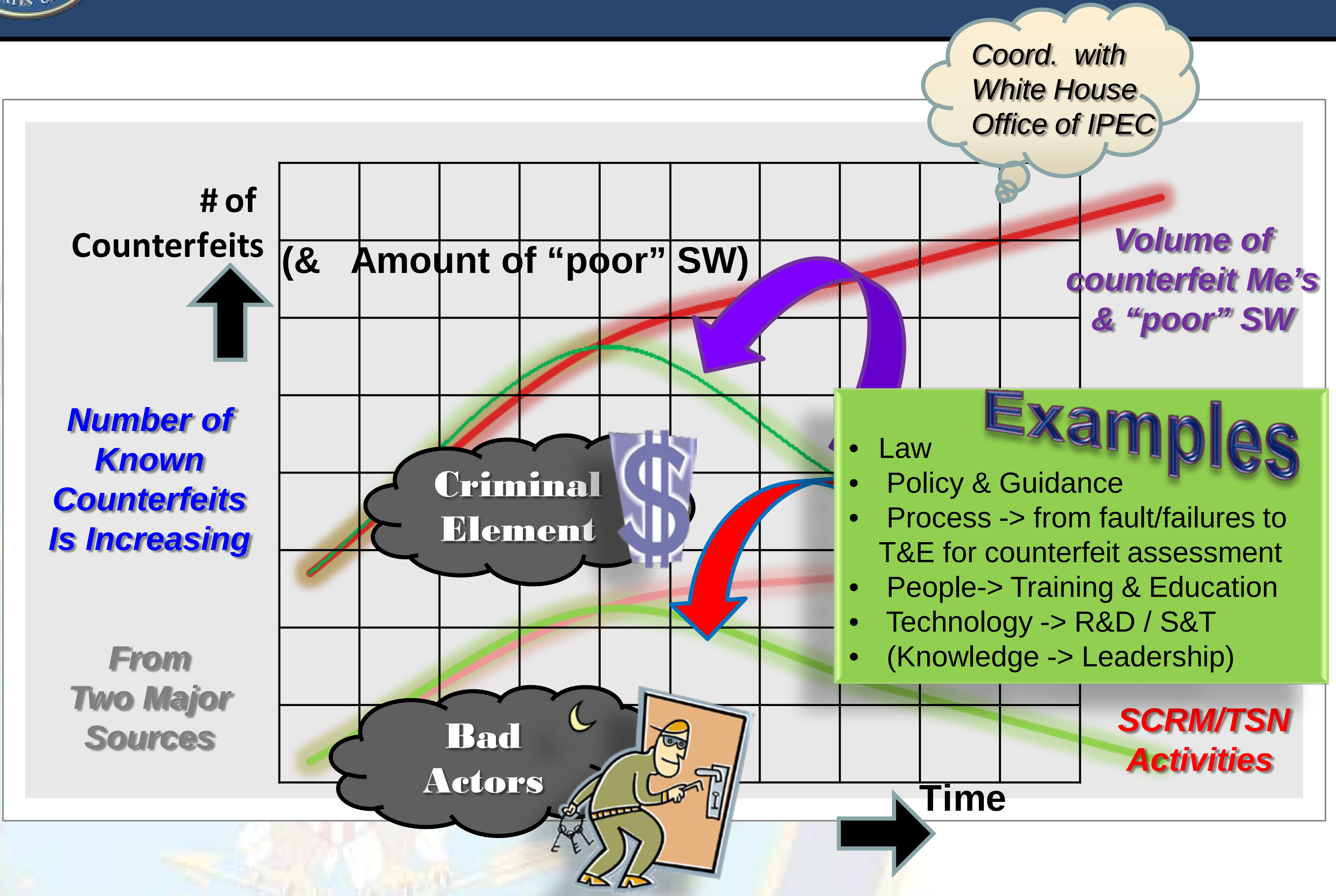
- fix-on-the-fly (while doing , w/ no pause) … to continue to move product

Supply Chain: PERSPECTIVES

Product INTEGRITY

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

Countering effects of Microelectronics Counterfeits & “poor “ SW in the Global Supply Chain



Coord. with White House Office of IPEC

# of Counterfeits (& Amount of “poor” SW)

Volume of counterfeit Me’s & “poor” SW

Number of Known Counterfeits Is Increasing

From Two Major Sources

Criminal Element

Bad Actors

Examples

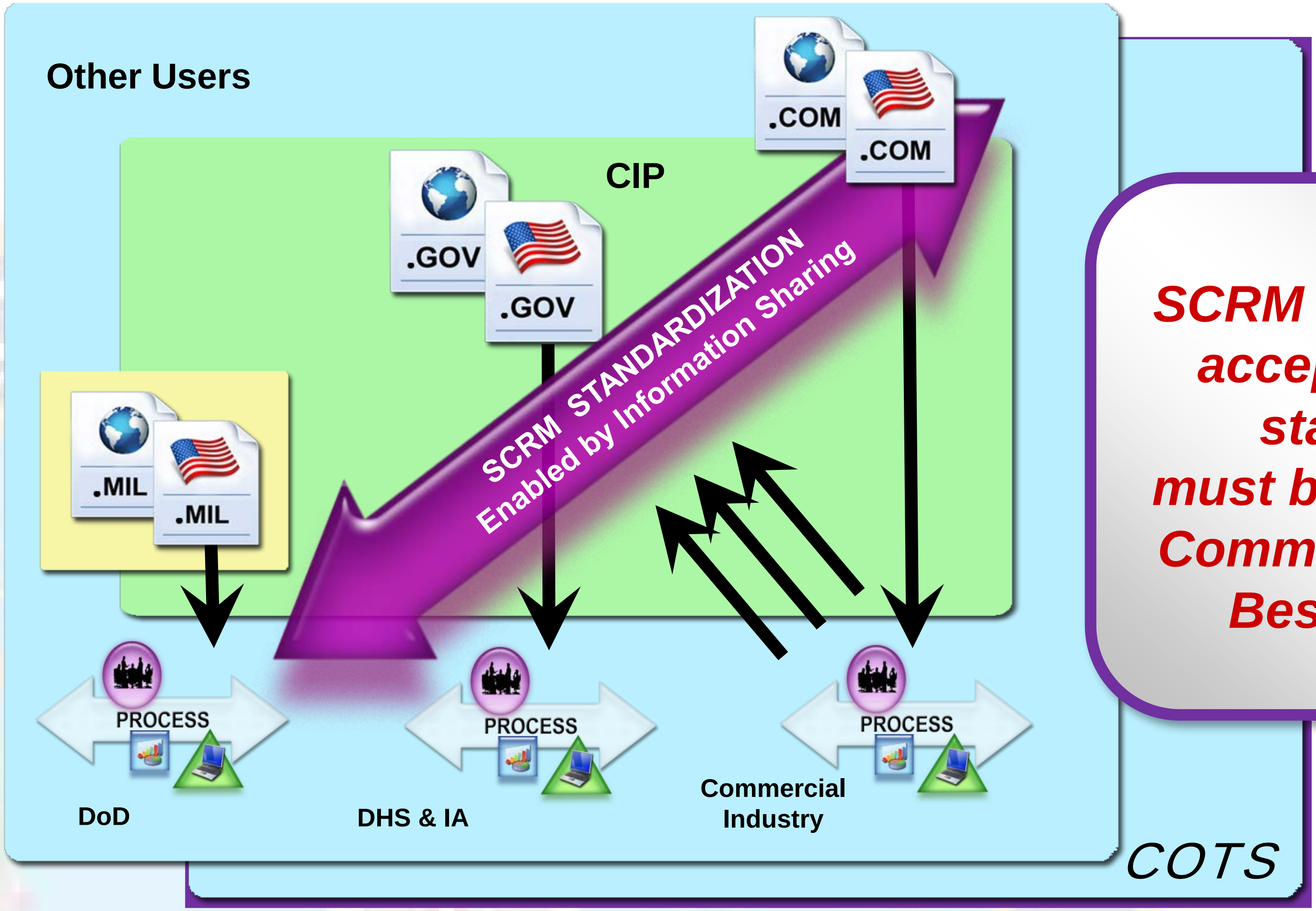
- Law
- Policy & Guidance
- Process -> from fault/failures to T&E for counterfeit assessment
- People-> Training & Education
- Technology -> R&D / S&T
- (Knowledge -> Leadership)

SCRM/TSN Activities

Time

SCRM Stakeholders

US has vital interest in the global supply chain.

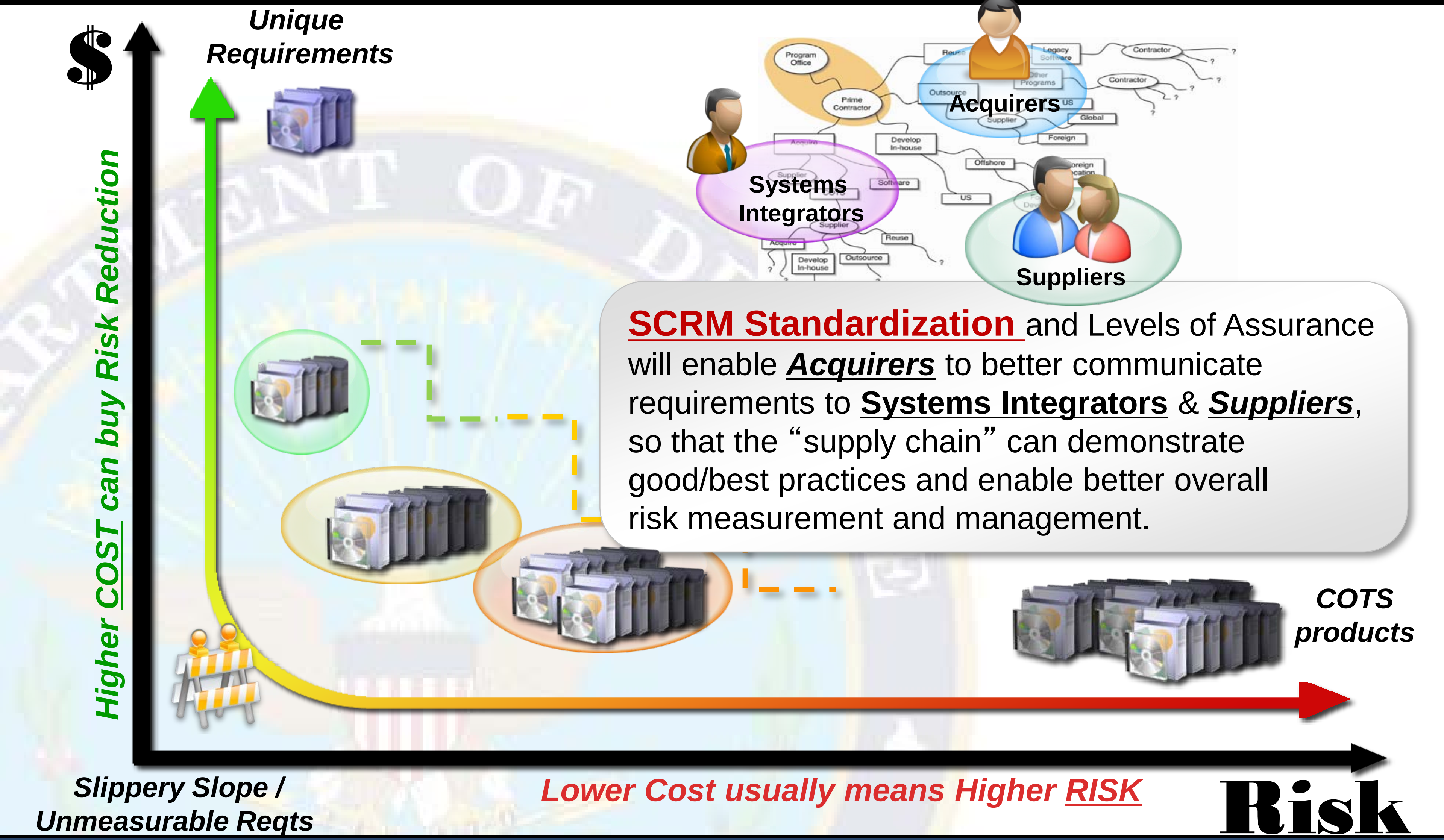


SCRM "commercially acceptable global standard(s)" must be derived from Commercial Industry Best Practices.

SCRM Standardization Requires Public-Private Collaborative Effort

Product Assurance *TRADESPACE*

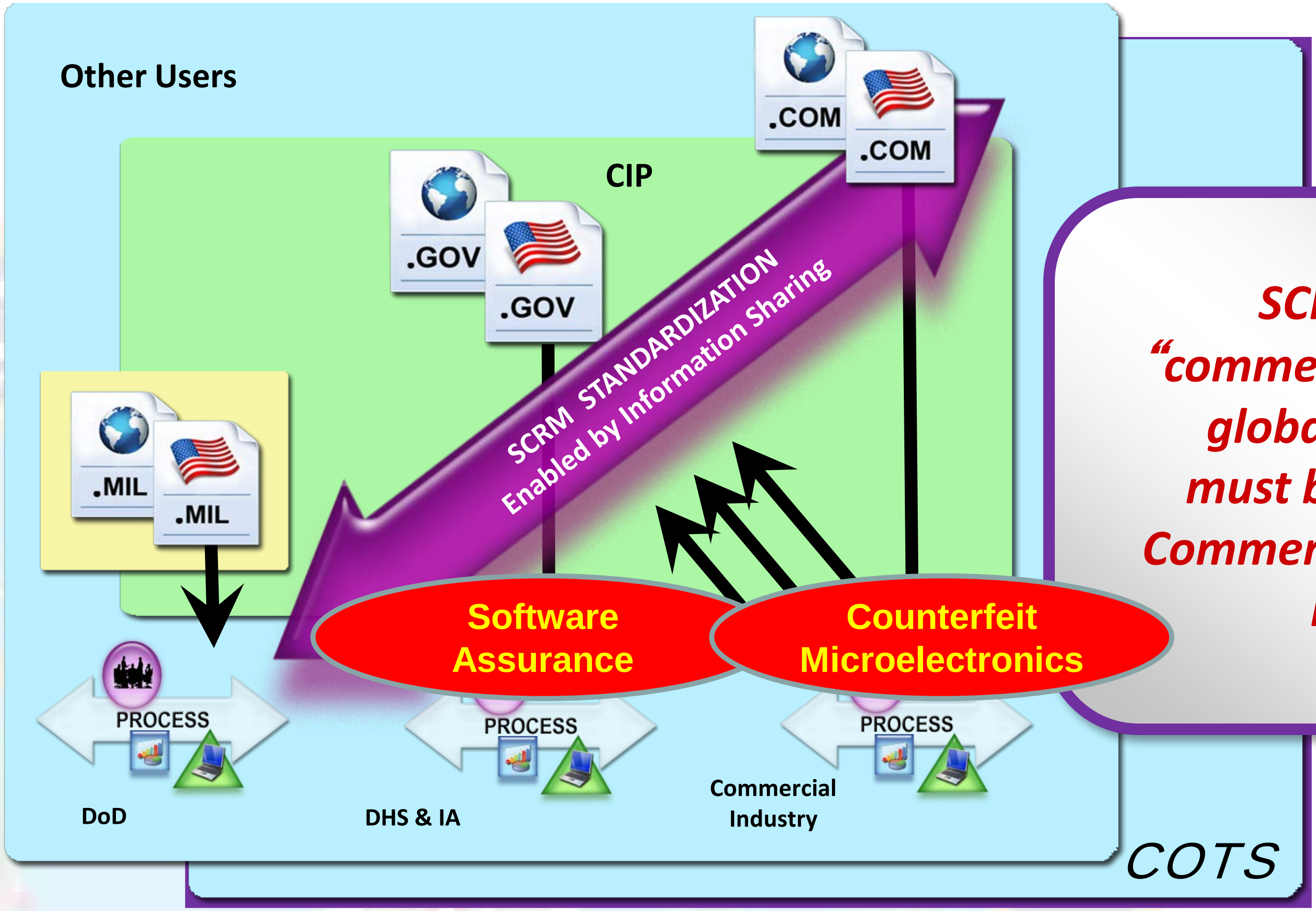
Custom
1982-----------2012
COTS



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.

SCRM has a Landscape of activities must address Counterfeits & Software

US has vital interest in the global supply chain.

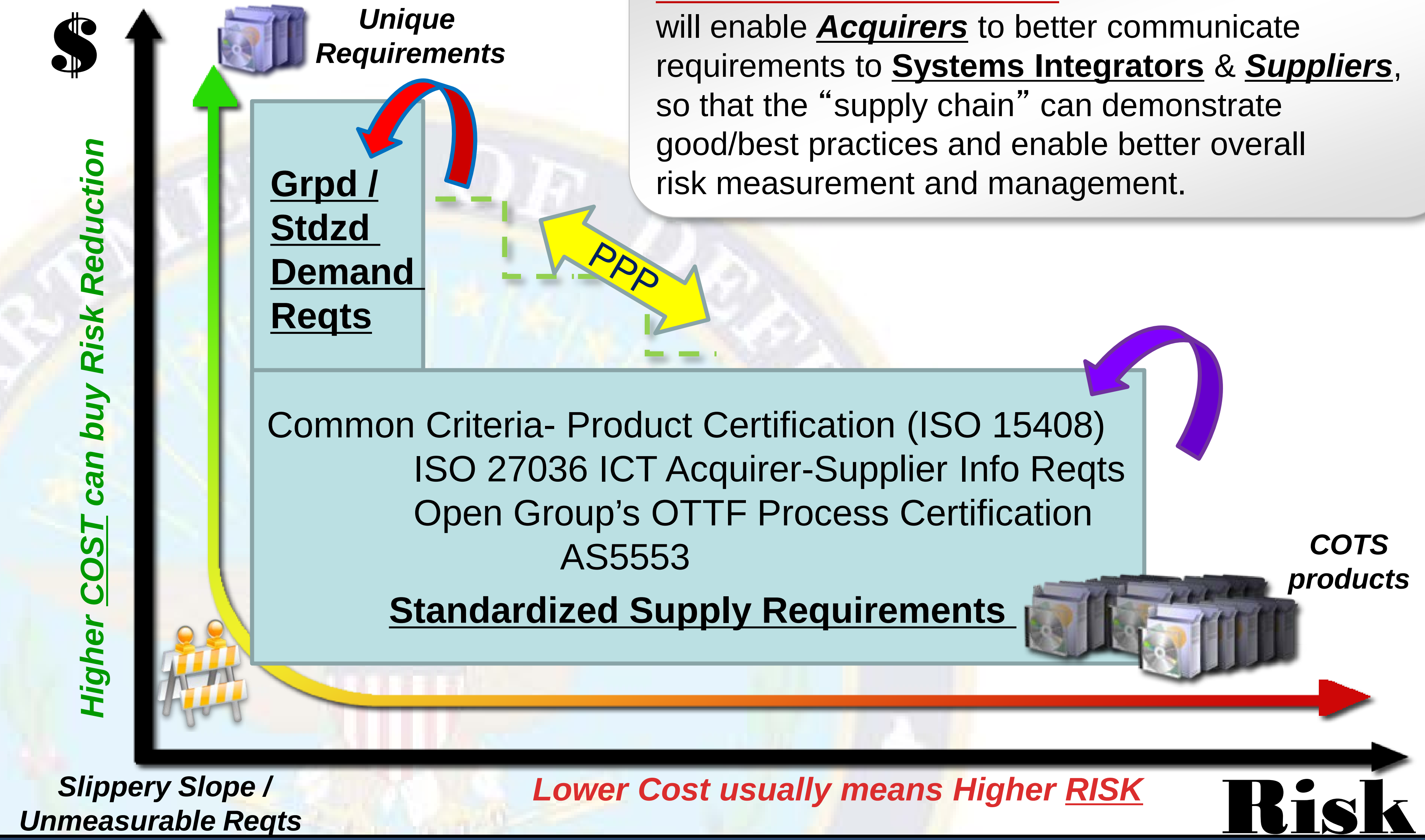


SCRM believes "commercially acceptable global standard(s)" must be derived from Commercial Industry Best Practices.

SCRM Standardization Requires Public-Private Collaborative Effort

Building Assurance *Levels* *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.



Unique Requirements

Grpd / Stdzd Demand Reqts

Common Criteria- Product Certification (ISO 15408)
ISO 27036 ICT Acquirer-Supplier Info Reqts
Open Group’s OTTF Process Certification
AS5553

Standardized Supply Requirements

COTS products

Higher COST can buy Risk Reduction

Slippery Slope / Unmeasurable Reqts

Lower Cost usually means Higher RISK

Risk

Recent Evolution of Strategy & Policy

Counterfeit Microelectronics---

Who is working this (DoD, US,gov, public-private, standards)
& NDAA'12 Section 818…upcoming NDAA'13 ?

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

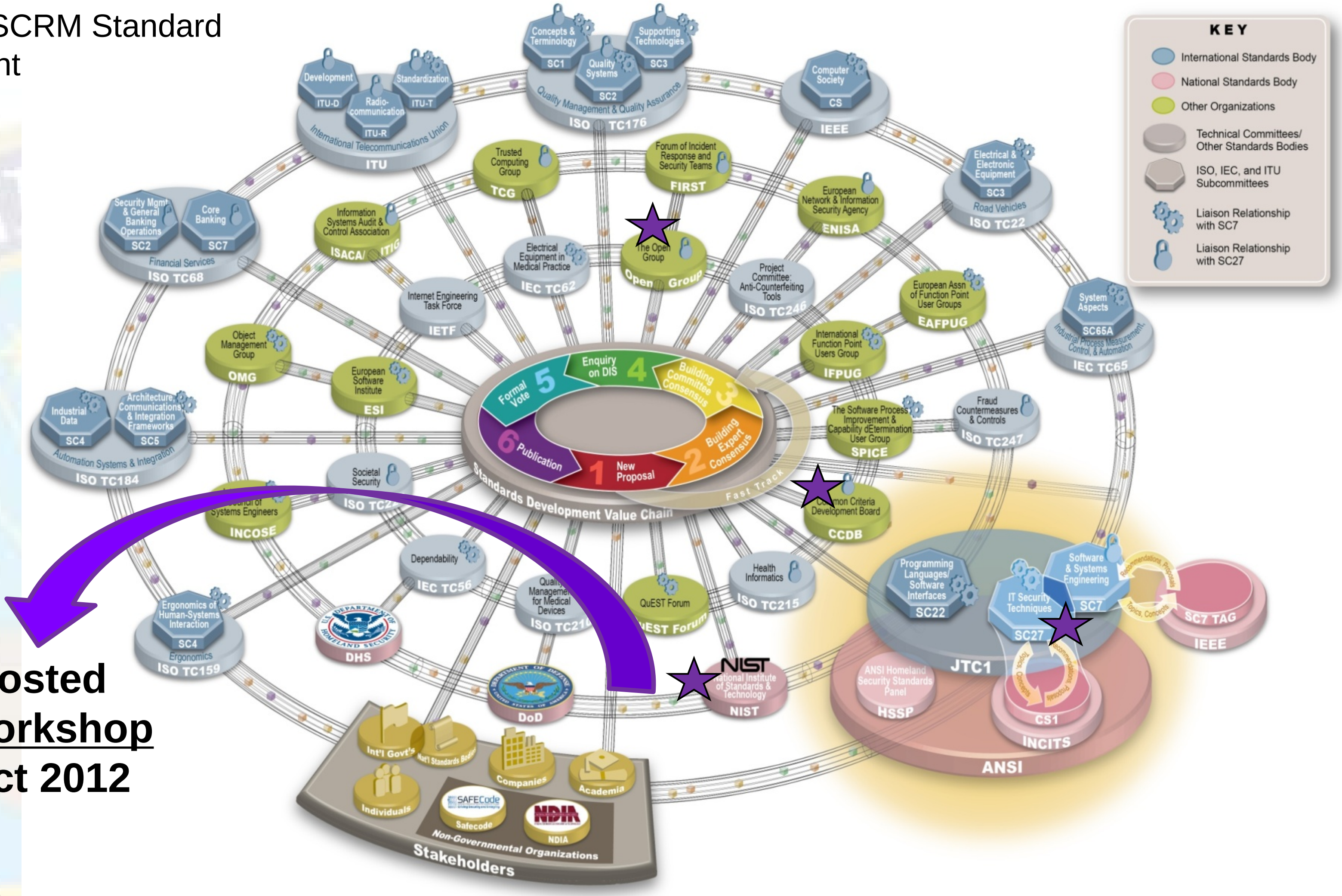
Software Assurance---

Who is working this (DoD, US,gov, public-private, standards)
& NDAA'11 Section 932… upcoming NDAA'13 ?

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

The ICT SCRM Standard Development Organization Landscape

★ Active ICT SCRM Standard Development


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
Trusted Computing Group
TCG
Forum of Incident Response and Security Teams
FIRST
European Network & Information Security Agency
ENISA
Electrical & Electronic Equipment
SC3
Road Vehicles
ISO TC22
Security Mgmt & General Banking Operations
SC2
Core Banking
SC7
Financial Services
ISO TC68
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
System Aspects
SC65A
Industrial Process Measurement, Control, & Automation
IEC TC65
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 TC22
Systems Engineers
INCOSE
Common Criteria Development Board
CCDB
Dependability
IEC TC56
Quality Management for Medical Devices
ISO TC210
QuEST Forum
QuEST Forum
Health Informatics
ISO TC215
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
JTC1
Recommendations, Proposals
Topics, Concepts
SC7 TAG
IEEE
ANSI Homeland Security Standards Panel
HSSP
CS1
INCITS
ANSI
Int'l Govt's
Nat'l Standards Bodies
Companies
Academia
Individuals
SAFECode
Safecode
NDIA
NDIA
Non-Governmental Organizations
Stakeholders

NIST-hosted
<u>SCRM Workshop</u>
15-16 Oct 2012

SCRM Developments & Standards

- New CNSS DIRECTIVE 505 on SCRM from Committee on National Security Systems (FOUO)
- New NIST-IR 7622 & NIST 800-53 rev4 out for public-comment (US.gov participates in SCRM WG2)

  http://csrc.nist.gov/news_events/index.html
- New "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
- SNAPSHOT of Best Practices from TheOpenGroup's Trusted Technology Forum (OTTF) (Trusted Technology Provider Framework & Snapshot)

  https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12341

  https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12561

  (login reqd)
- Supply Chain Technical Working Group (CCTWG) “approved” by Common Criteria Development Board (CCDB) in Japan in Mar’12 to advise CCDB & development of new CC "Protection Profiles" that will replace EALs

  http://www.commoncriteriaportal.org/

  https://cc-supplychain.teamlab.com/products/files/#408084 (login reqd)
- ISO 27036 on ICT Acquirer-Supplier Relationships (Parts 1-2-3) migrating from “initial draft” to “committee draft” in 2012… (TMSN leads US participation in ANSI CS1 SCRM adHoc WG)

Technology Supply Chain Threat Matrix

	Tainted			Counterfeit		
	Upstream	Provider	Downstream	Upstream	Provider	Downstream
Malware	☑	☑	☑			
Unauthorized “Parts”	☑	☑	☑	☑		
Unauthorized Configuration			☑			
Scrap/ Substandard Parts				☑		
Unauthorized Production				☑		☑