CyberSecurity,US CNCI-SCRM, Public-Private STANDARDIZATION …

Countering-COUNTERFEITS

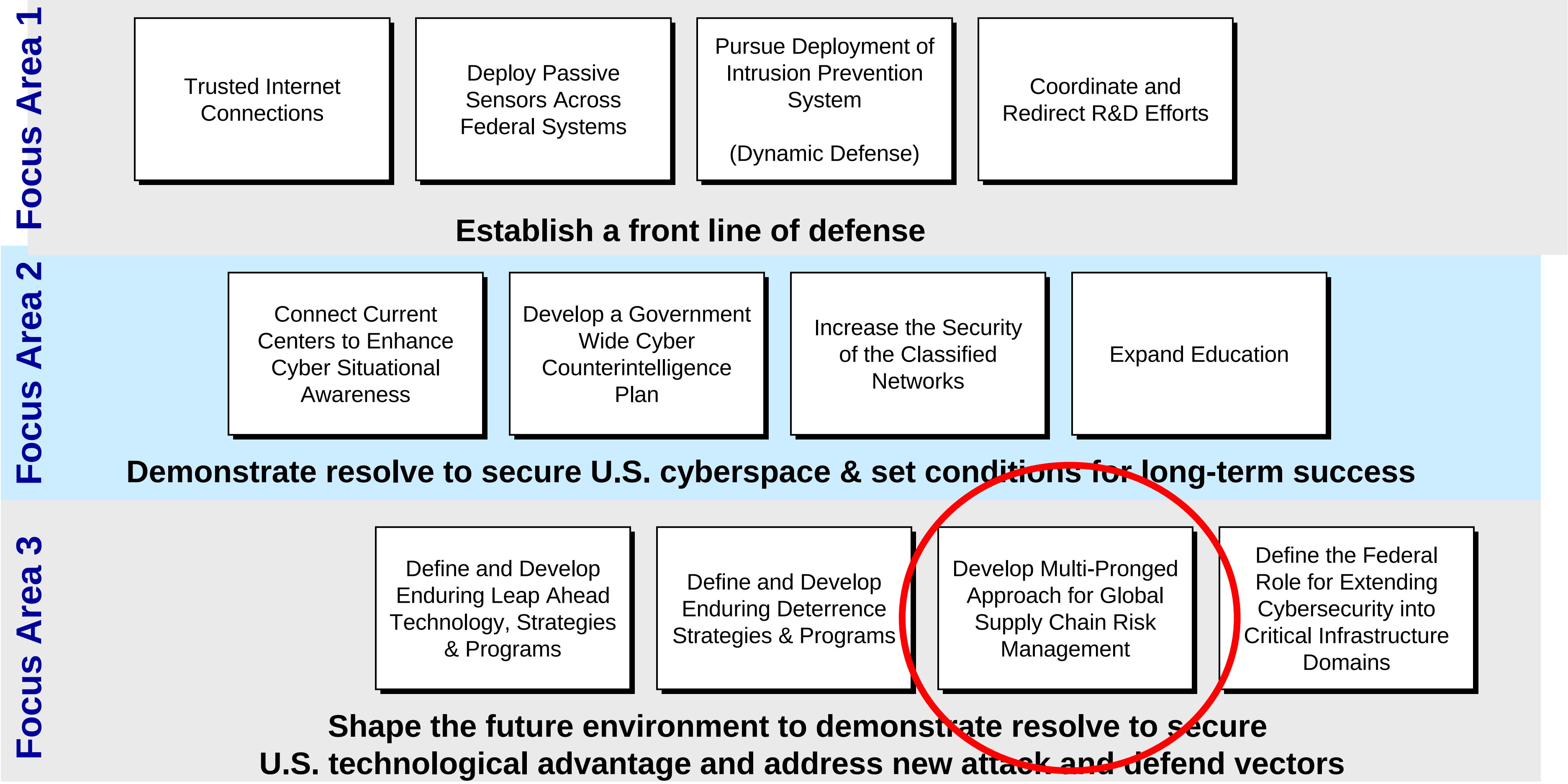
@ ANSI's – "Crossing Borders and Sectors: Exploring Robust Anti-Counterfeiting Solutions" (22 Sep 2010 in Crystal City, VA)

Don.Davidson@osd.mil
Trusted Mission Systems & Networks
OASD-NII / DoD CIO

CYBERSECURITY

FRAUD
CARELESSNESS
causes security incidents
CYBERWARFARE
What not to post
10 Steps to a New Cyber Mission Discipline
Foreign Government
Federal Agencies
State Agencies
Local Government
Public/Private Partnerships
General Public
Building CWE & Consensus
Publicly Available: Security Taxonomies, Research, and Checklists
Fortify Brian Chess
Cigital Gary McGraw
OWASP Top Ten
Secure Software CLASP
Klockwork
Ounce Labs
Gramma Tech
Preliminary
CVE-based Preliminary List of Vulnerability Examples for Researchers (PLOVER)
Previous Vulnerability Taxonomy Research
Other Work Available in Security Taxonomies, Research, and Checklists
IBM
KDM Analytics
SPI Dynamics
Core
VERACODE
Coverity
Kestrel Technology
NSA/CTC
Stanford
SEI - CERT CC
Unisys
Parasoft
Purdue
Security University
MIT Lincoln Labs
UC Berkeley
Univ. of Maryland
North Carolina State University (NCSU)
Oracle
GMU
CWE
National Vulnerability Database (NVD)
Common Vulnerabilities and Exposures (CVE)
Object Management Group Software Assurance SIG
Open Web Application Security Project (OWASP)
Web Application Security Consortium (WASC)
DHS Software Assurance Common Body of Knowledge
NSA and CTC CAMP
You are here
http://www.

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

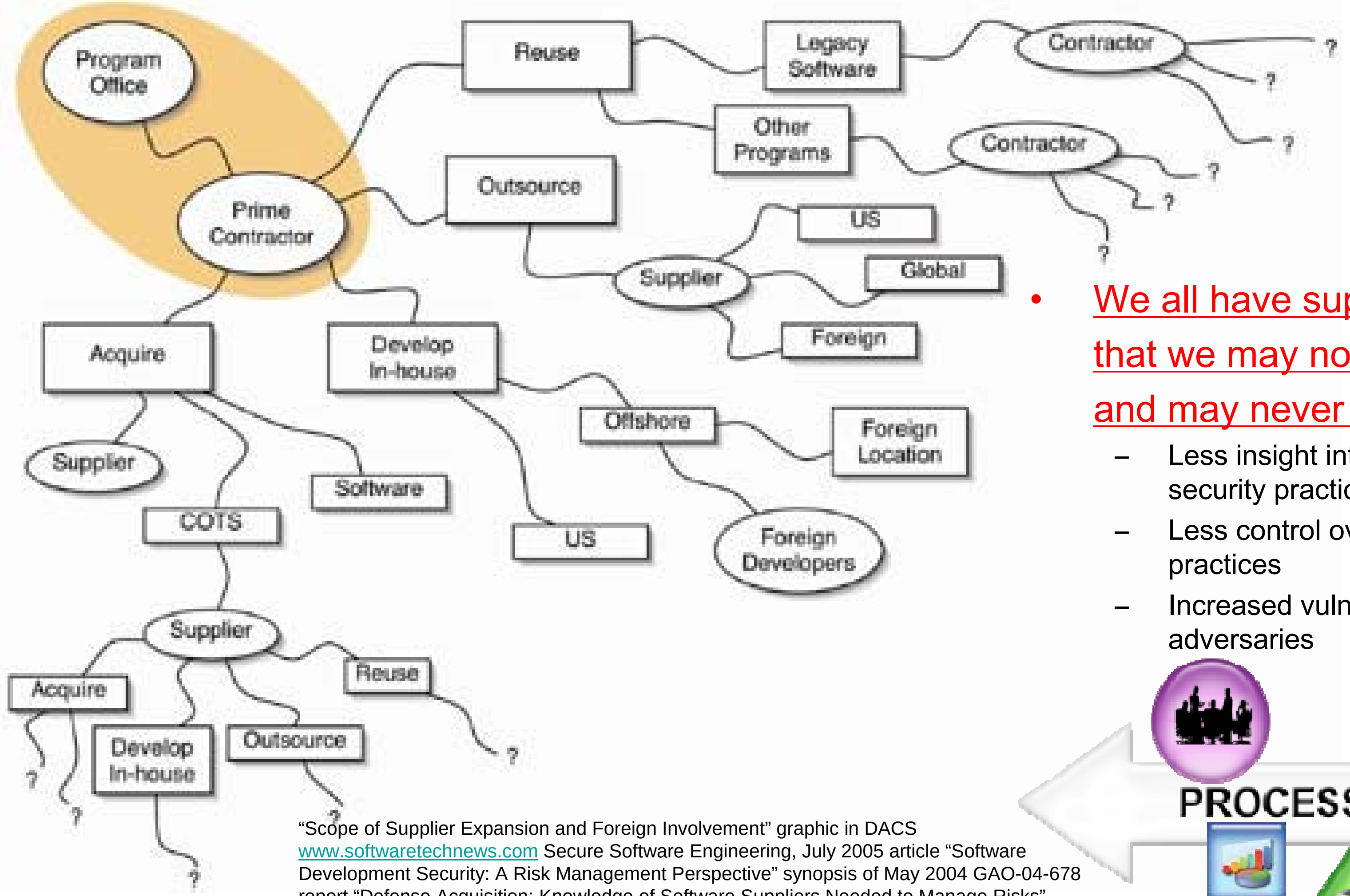
Define and Develop Enduring Deterrence Strategies & Programs

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

Globalization brings challenges



“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”

- We all have suppliers that we may not know and may never see
  - Less insight into suppliers’ security practices
  - Less control over business practices
  - Increased vulnerability to adversaries

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

- Dependencies on technology are greater then ever

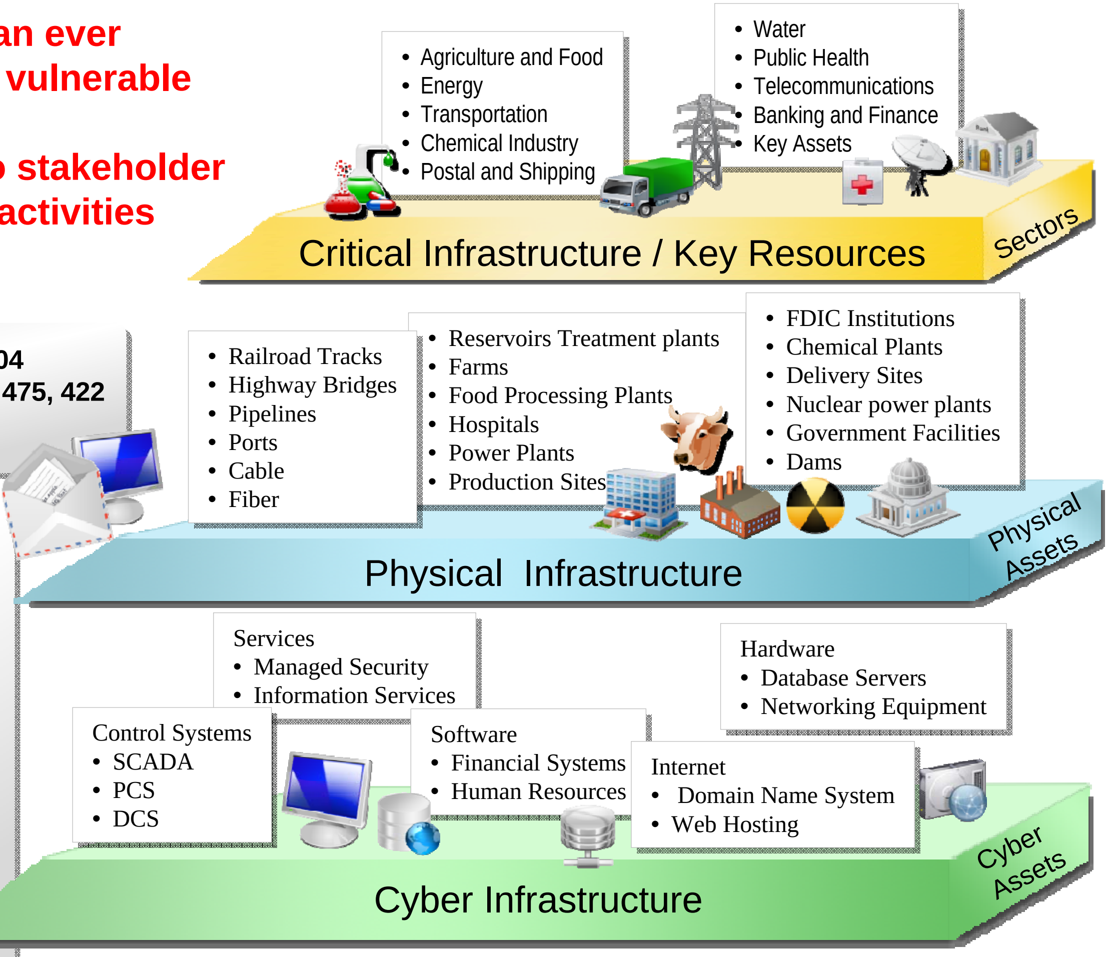
-- Possibility of disruption is greater than ever because software (and overall ICT) is vulnerable

--- 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*



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

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

Critical Infrastructure / Key Resources

Sectors

- 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

Physical Infrastructure

Physical Assets

Services
- Managed Security
- Information Services

Hardware
- Database Servers
- Networking Equipment

Control Systems
- SCADA
- PCS
- DCS

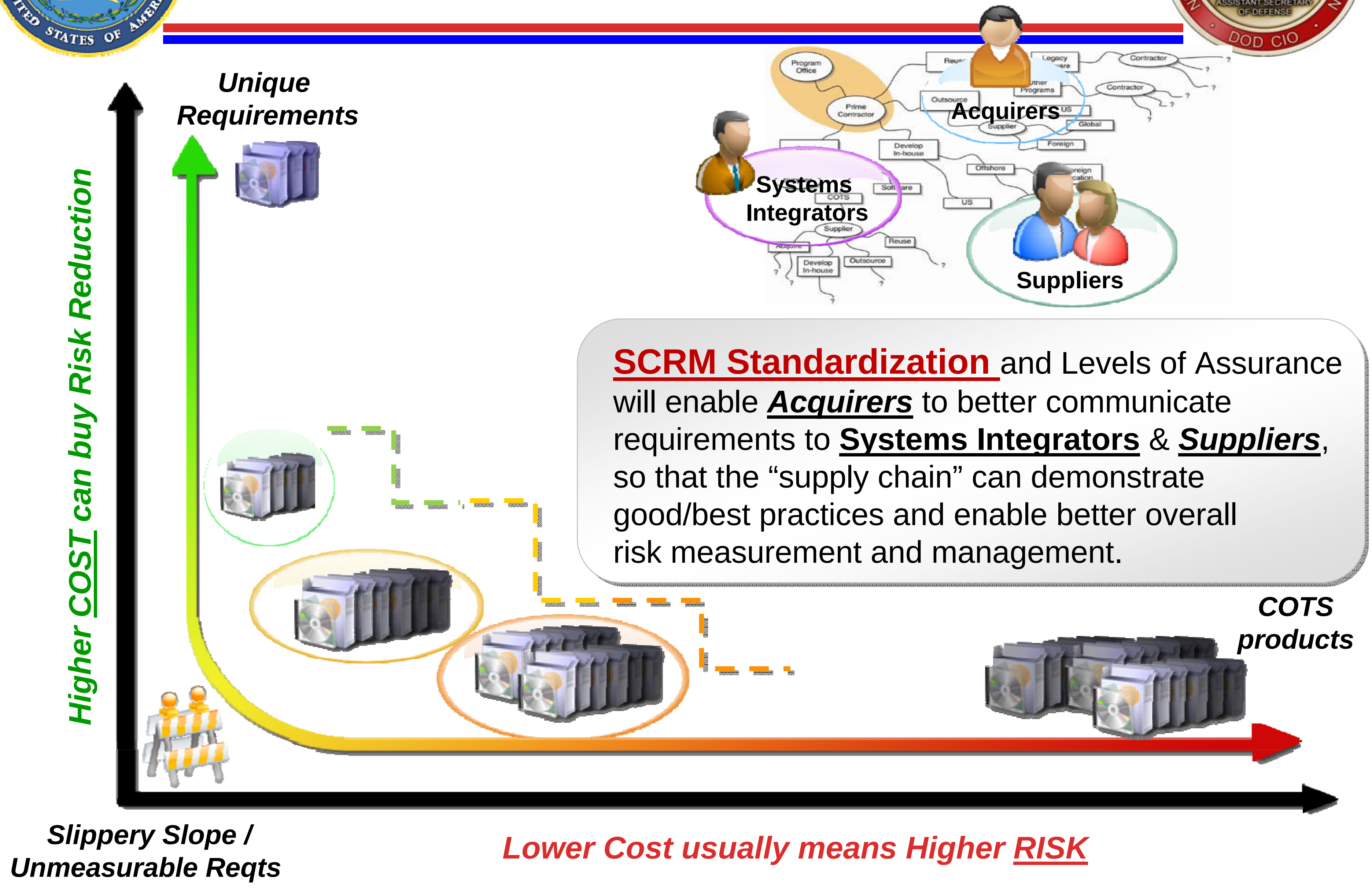
Software
- Financial Systems
- Human Resources

Internet
- Domain Name System
- Web Hosting

Cyber Infrastructure

Cyber Assets

Systems Assurance
TRADESPACE



Acquirers

Systems Integrators

Suppliers

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.

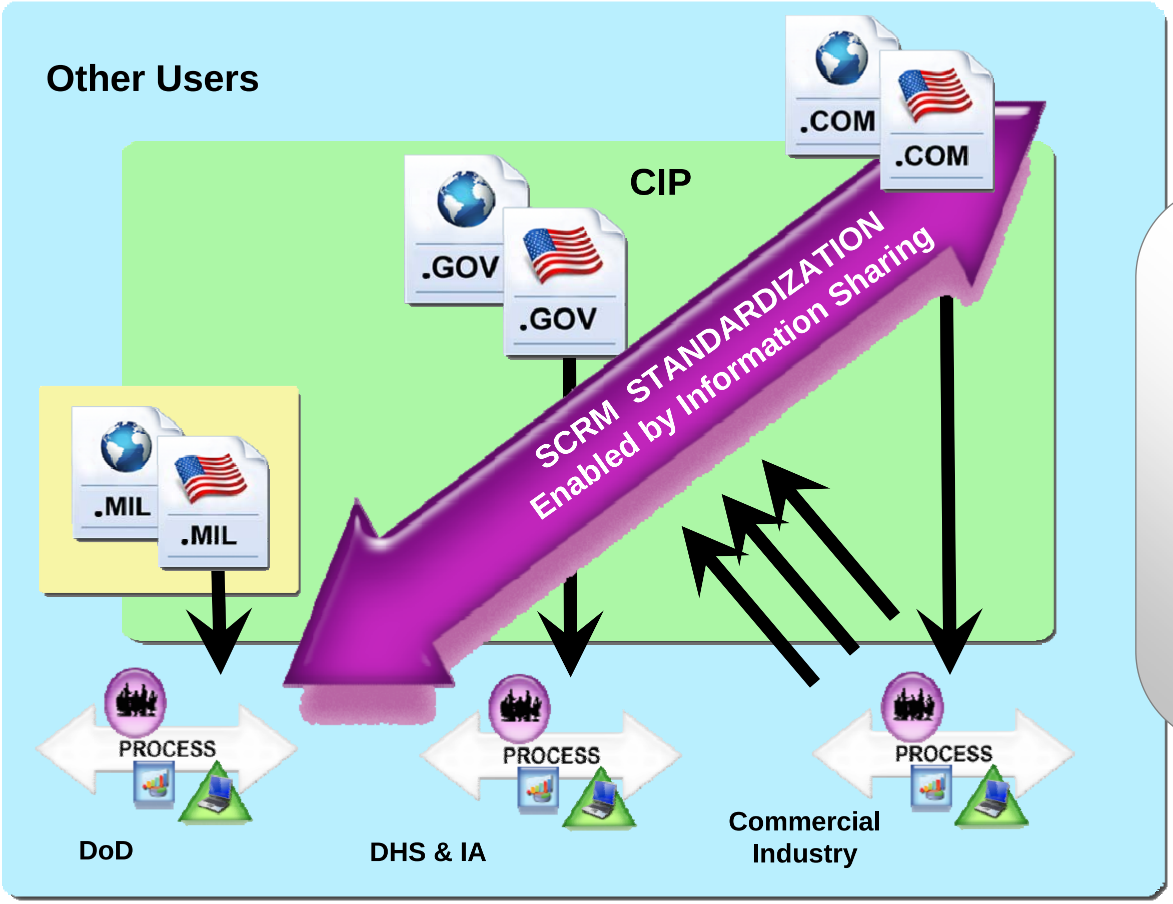
COTS products

Slippery Slope / Unmeasurable Reqts

Lower Cost usually means Higher RISK

SCRM Stakeholders

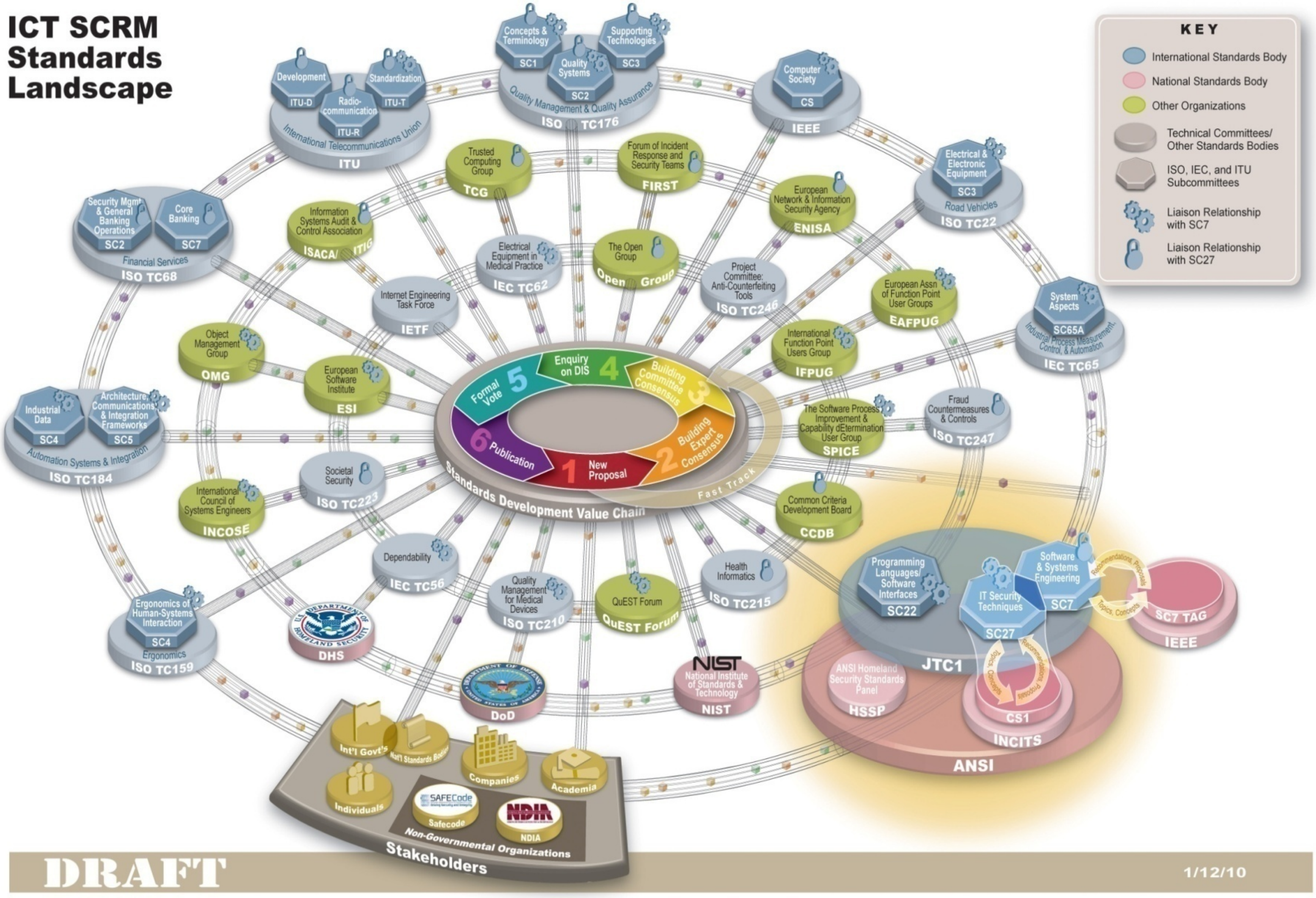
US (CNCI) has vital interest in the global supply chain.



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

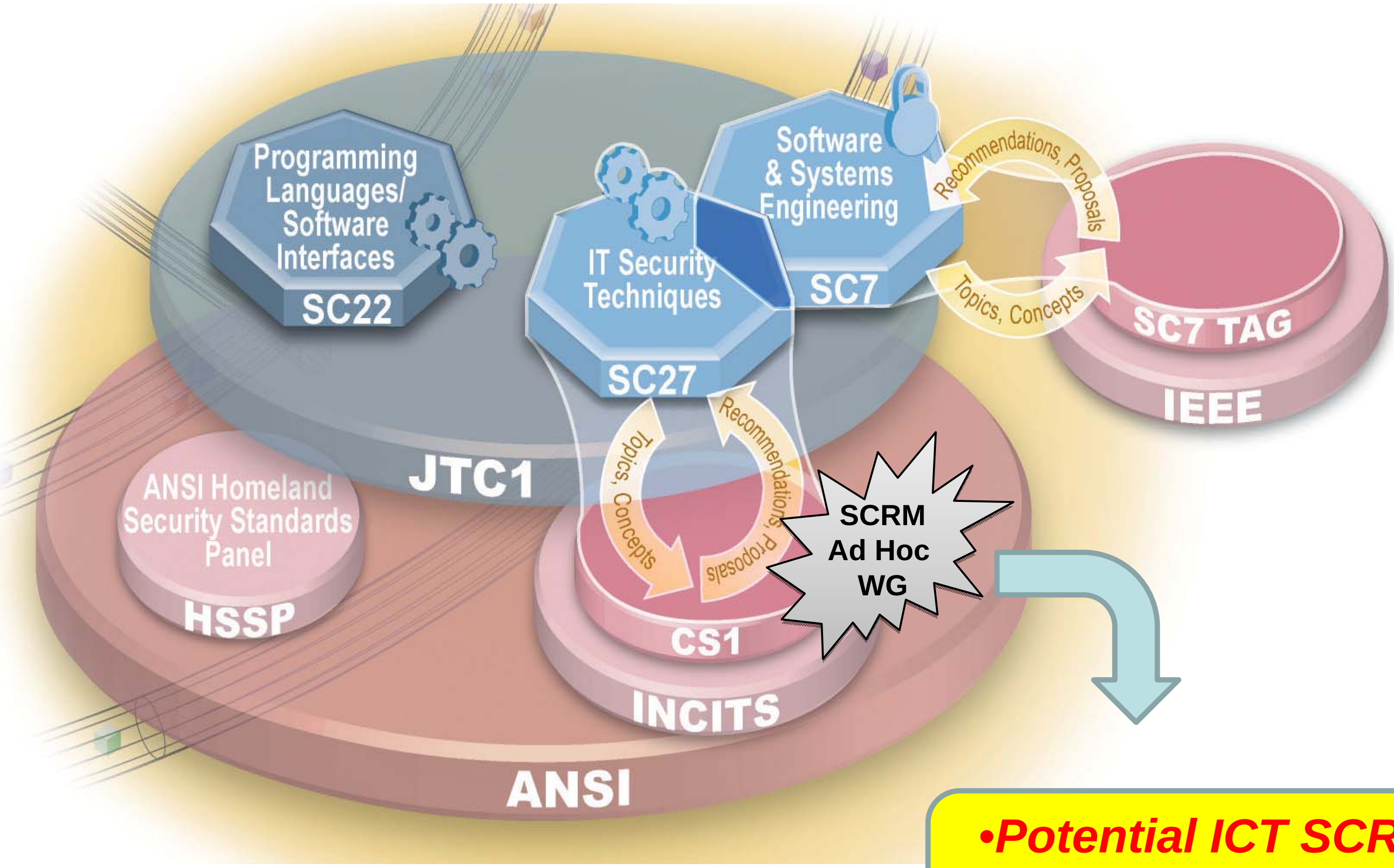
SCRM Standardization Requires Public-Private Collaborative Effort

Standards Development Organizations SDOs Landscape: an 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
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
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
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

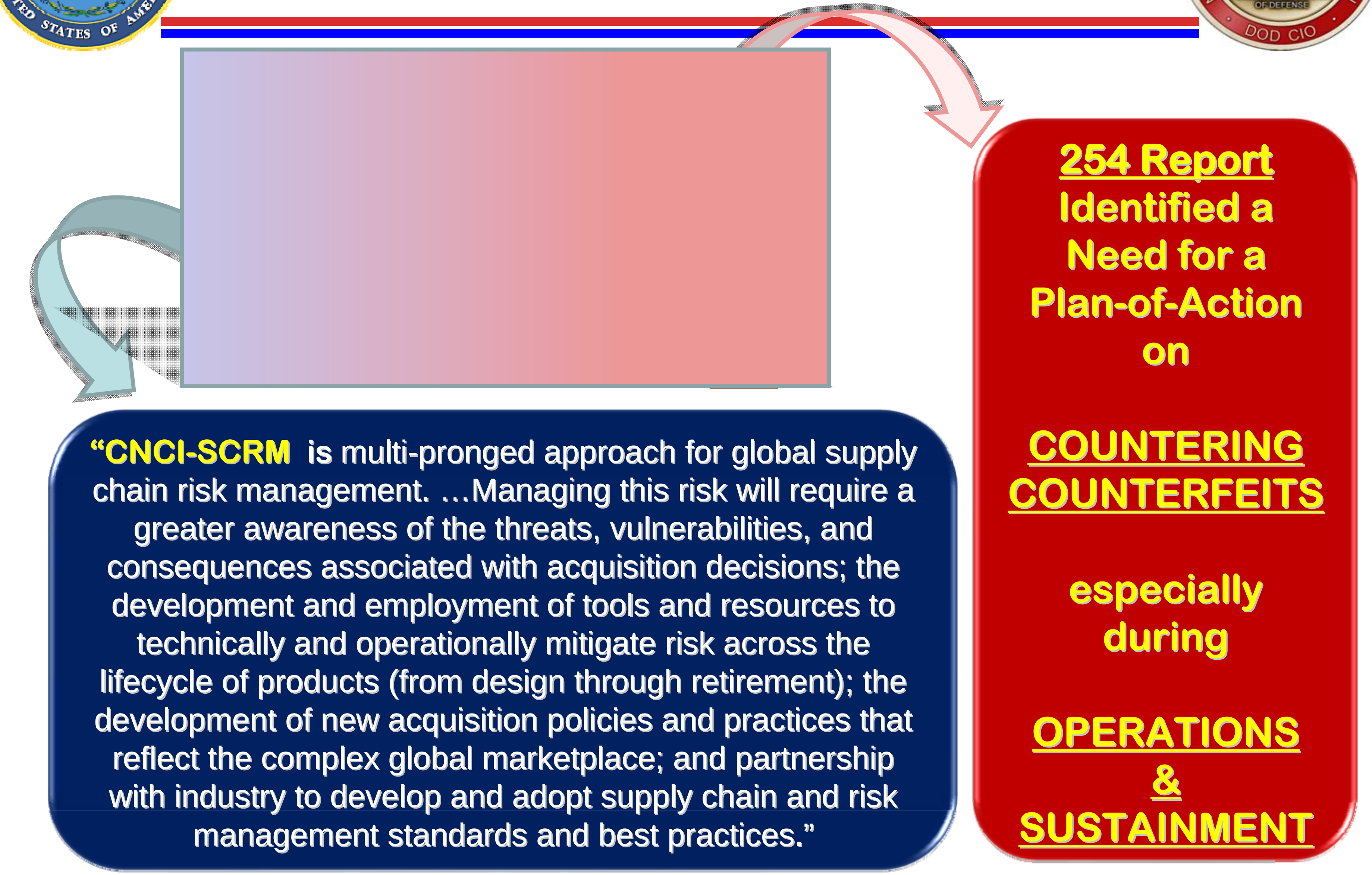
SCRM Study Periods:

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
ANSI Homeland Security Standards Panel
HSSP
Topics, Concepts
Recommendations, Proposals
CS1
INCITS
ANSI
SCRM Ad Hoc WG

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

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.”

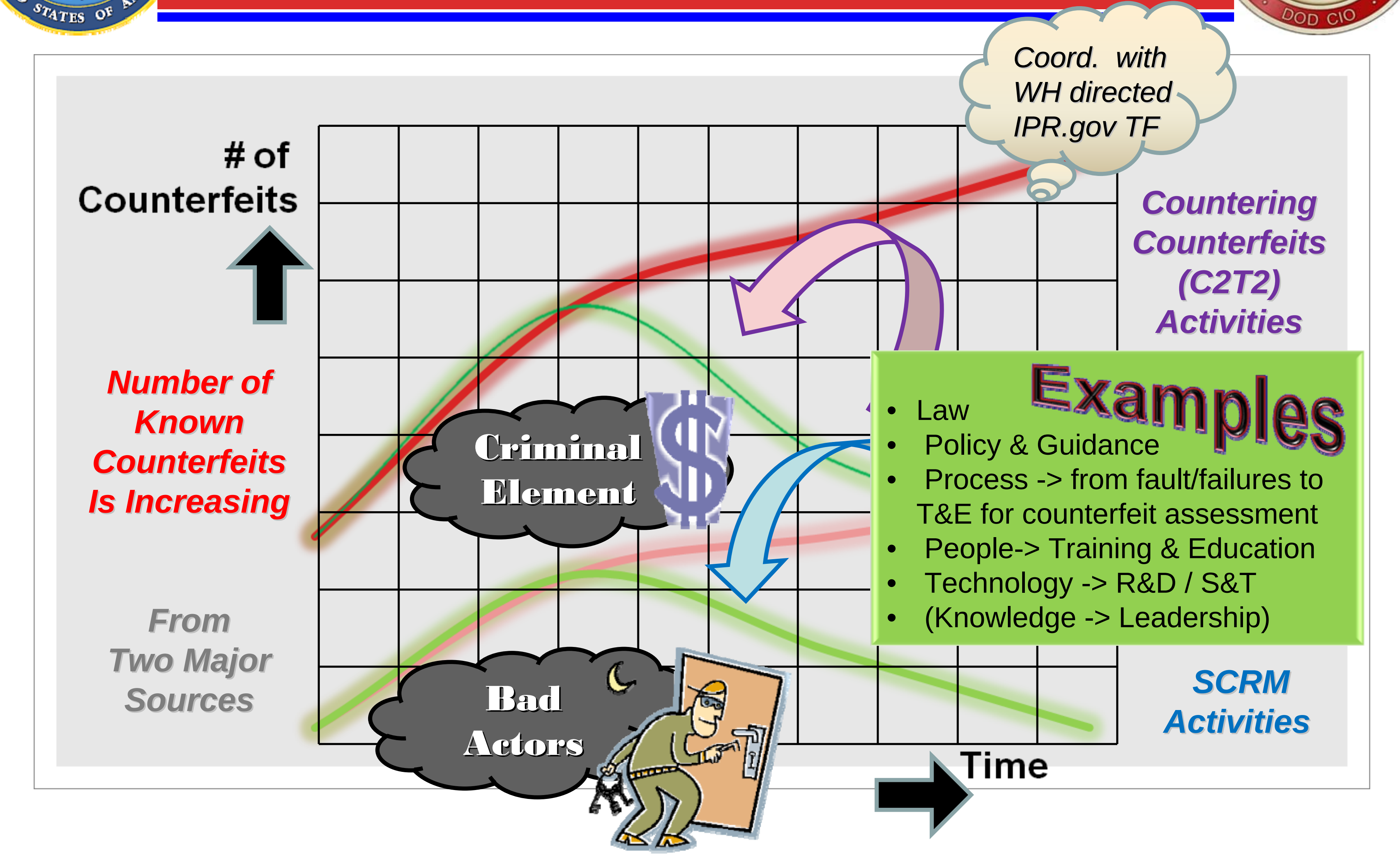
254 Report **Identified a Need for a Plan-of-Action on**

COUNTERING COUNTERFEITS

especially during

OPERATIONS & SUSTAINMENT

Countering Counterfeits Strategic Concept



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)

CyberSecurity,US CNCI-SCRM,
Public-Private STANDARDIZATION …

Countering-COUNTERFEITS

Don.Davidson@osd.mil
Trusted Mission Systems & Networks
OASD-NII / DoD CIO