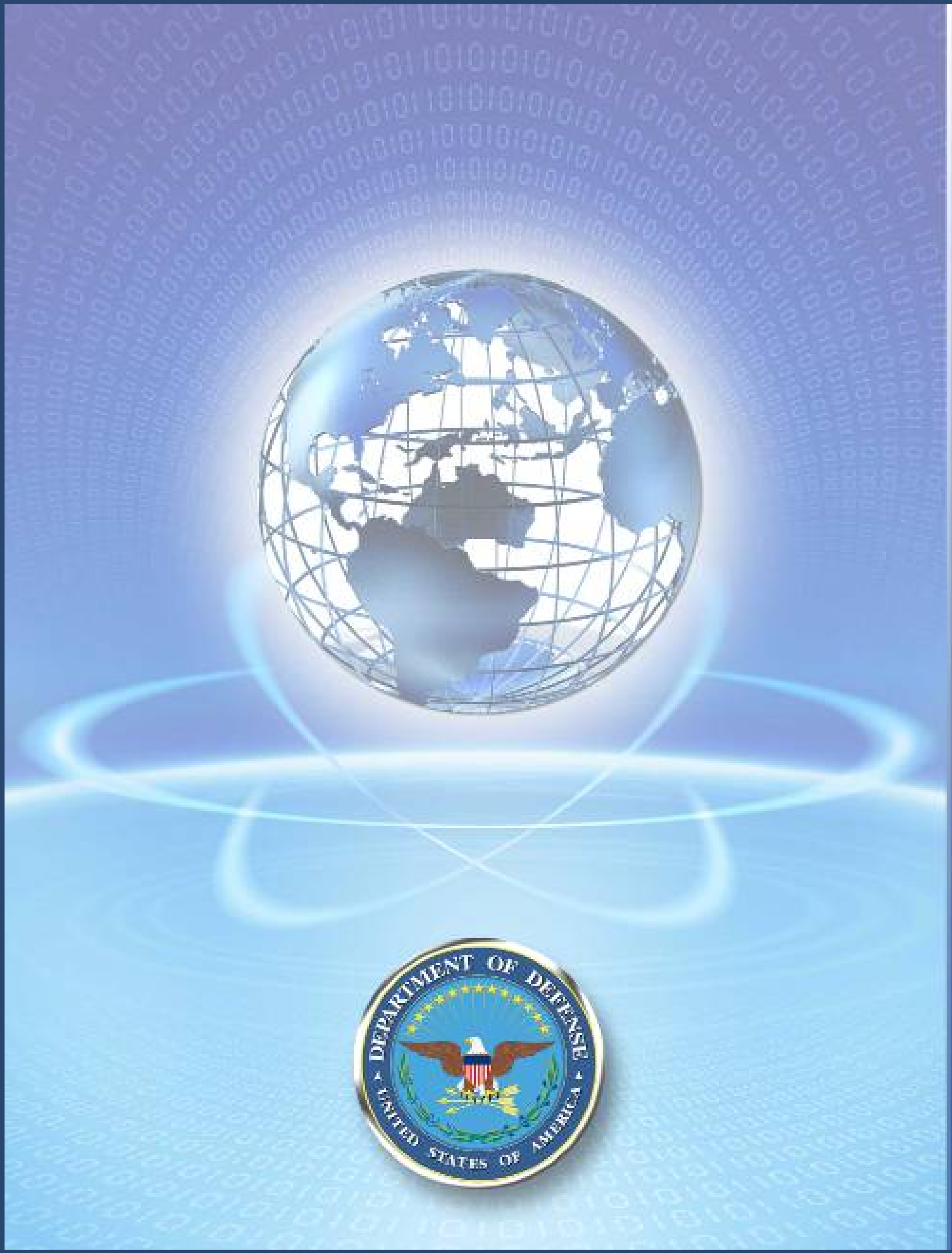


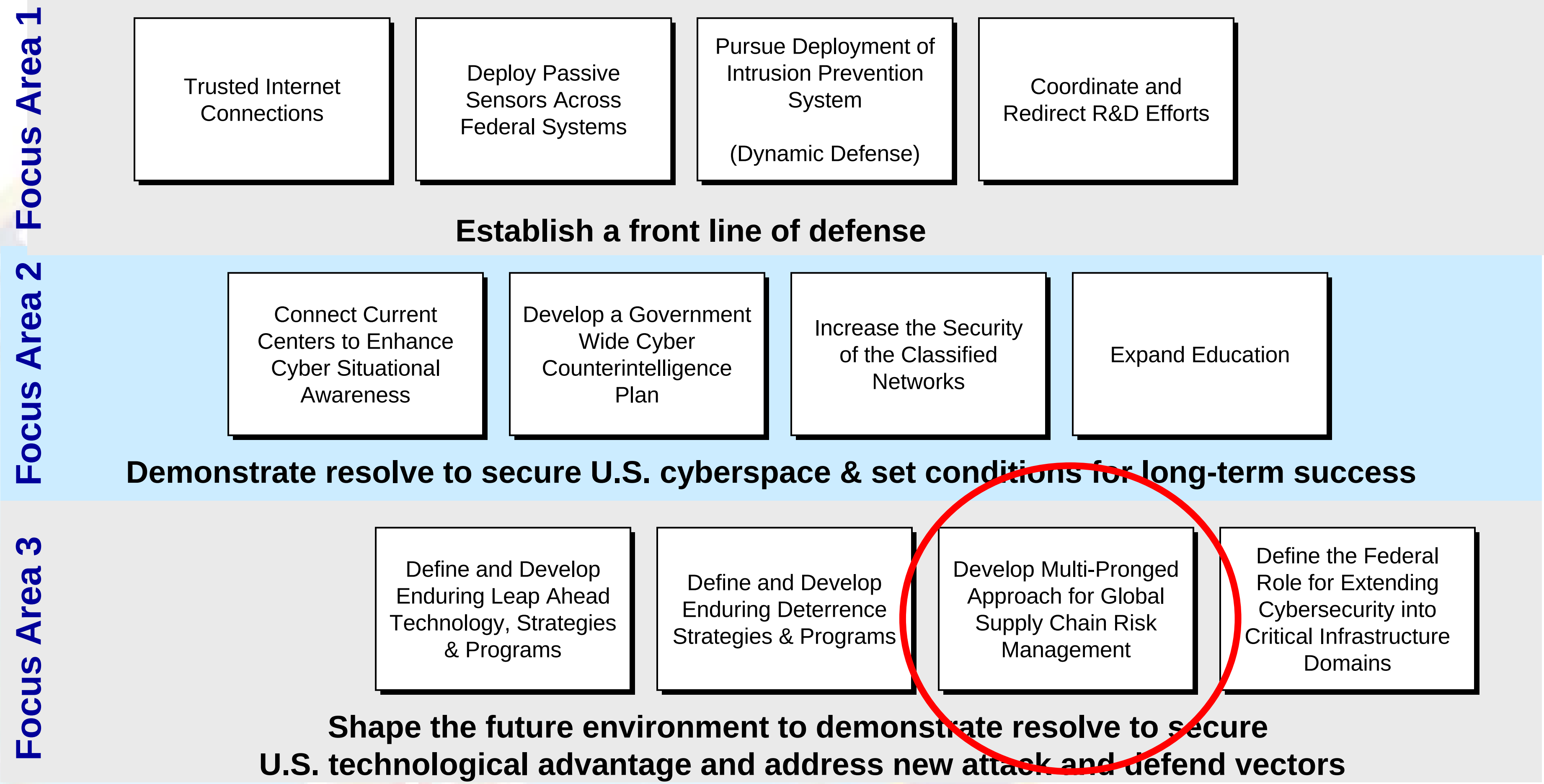
CNCI-SCRM

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

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

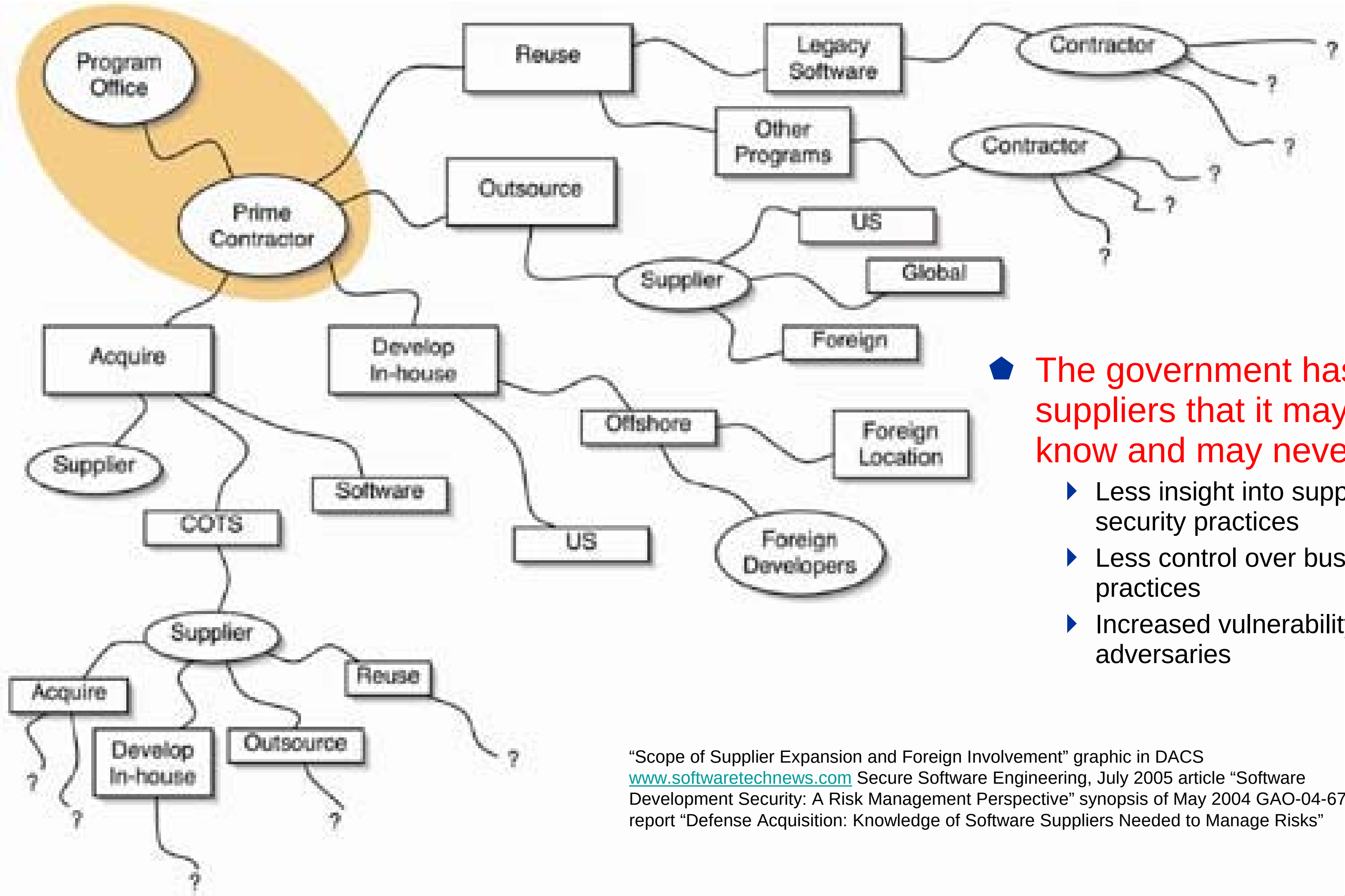
Define the Federal Role for Extending Cybersecurity into Critical Infrastructure Domains

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

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
Klocwork
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
VERACODE
Coverity
Kestrel Technology
Stanford
SEI - CERT CC
NSA/CTC
Parasoft
Purdue
Unisys
Security University
MIT Lincoln Labs
Univ of Maryland
UC Berkeley
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)
DHS Software Assurance Common Body of Knowledge
NSA and CTC CAMP
You are here
http://www.

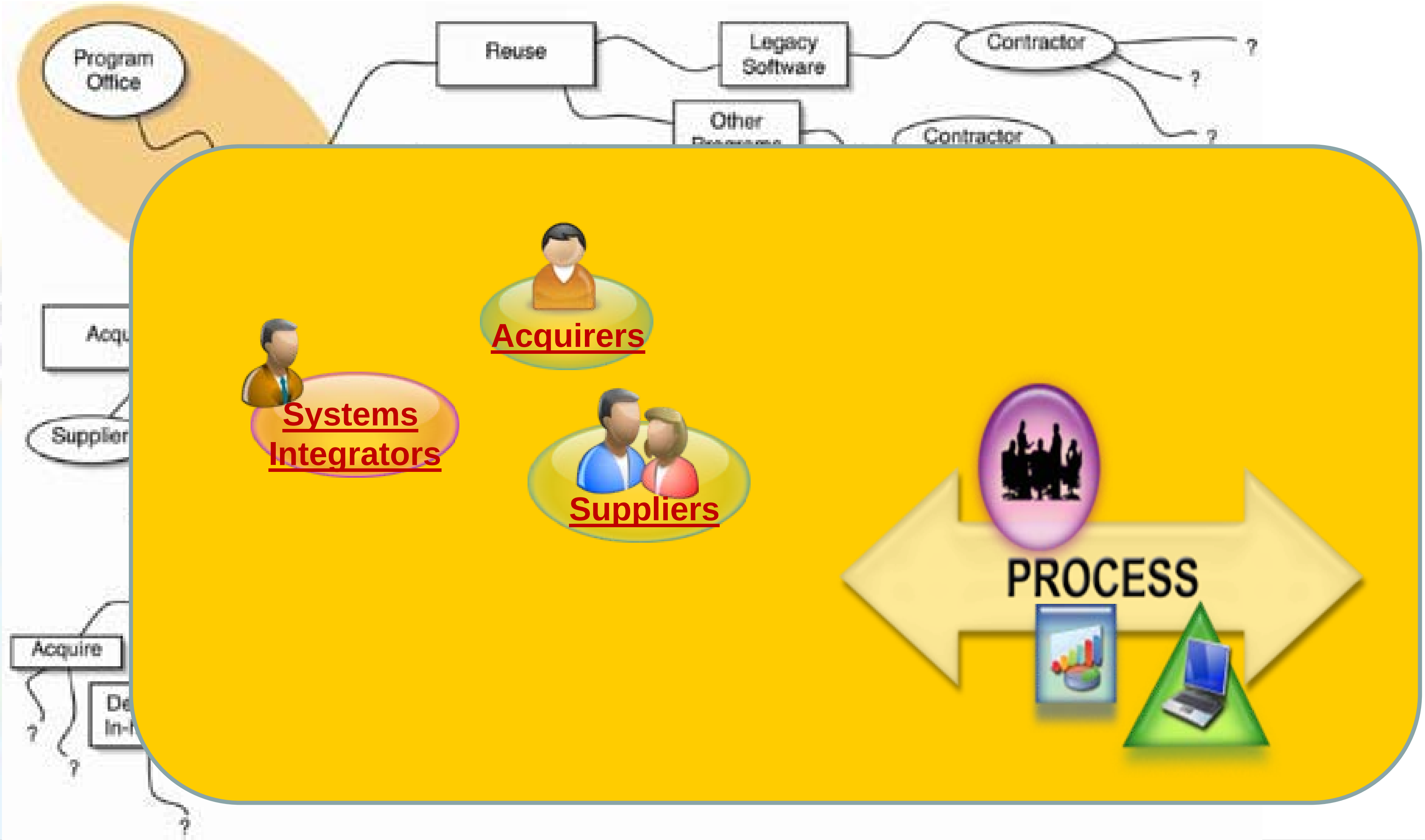
Globalization brings challenges to DoD…



- 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…



Acquirers

Systems Integrators

Suppliers

PROCESS

… and to Industry

- Many things are more challenging in a global environment where ICT supply chain gets less clear with each layer
  - Intellectual property protection
  - Assurance that you are buying authentic products
  - Quality control in a global environment
  - Gaining a desired level of assurance about sound business and system development/integration practices
  - Etc…

USG refers to this challenge as global sourcing and

supply chain risk management

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

- Dependencies on technology are greater then ever

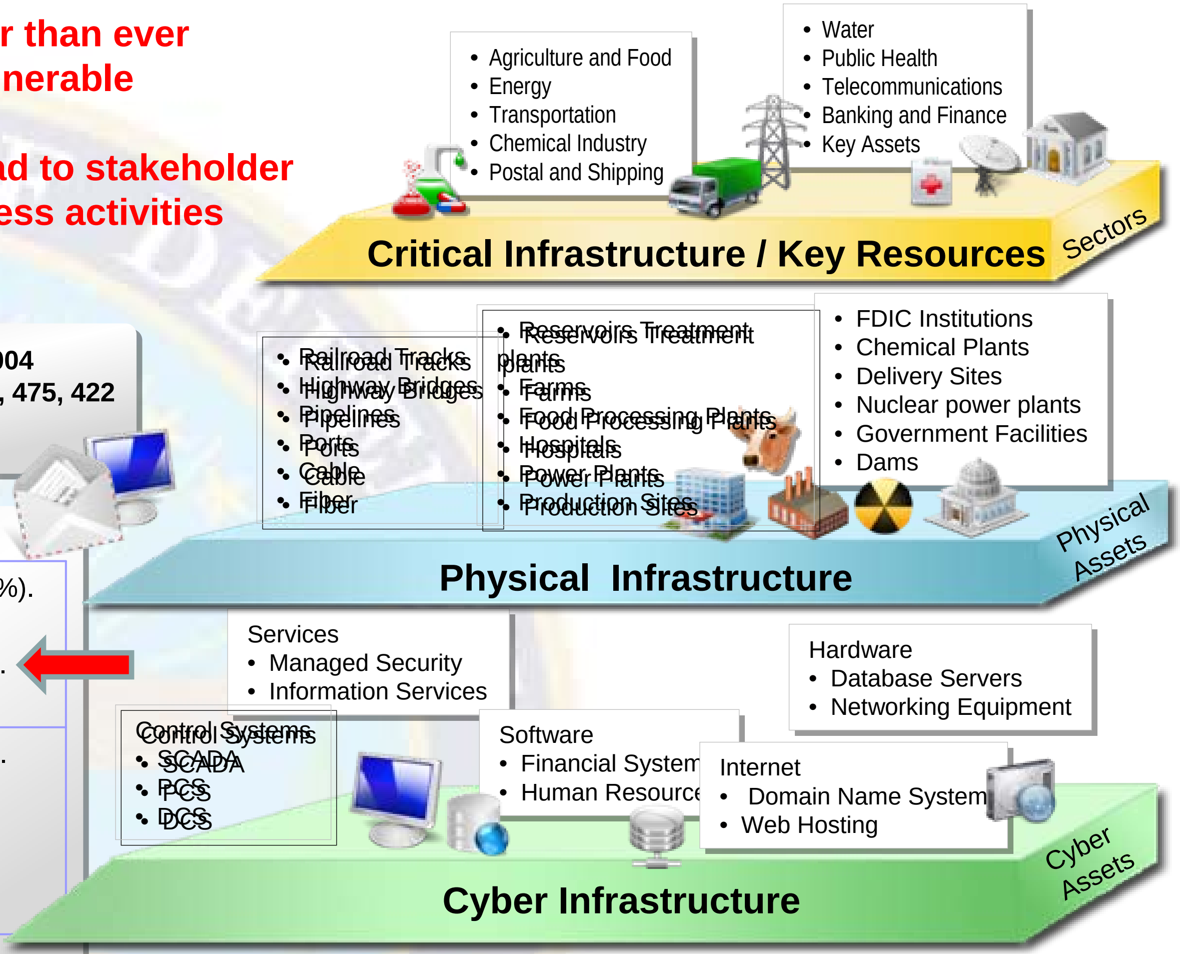
-- Possibility of disruption is greater than ever because hardware/software is vulnerable

--- 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*



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

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

Critical Infrastructure / Key Resources

- 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

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

Cyber Infrastructure

Things that can go wrong

- Technologies are integrated without regard to the criticality and risk levels of the parent system or network
  - *Vulnerabilities*: All ICT (incl. systems, networks, applications)
    - Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
    - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
    - Counterfeit components/products prematurely degrade / otherwise disrupt operations
- Adversary has increased access and opportunity to infiltrate otherwise closed-off technologies and services
- *Consequences*: Stolen critical data & technology; corruption, denial of critical functionality

SCRM Guiding Principles

- Defense-in-breadth: Mitigate risk across the entire lifecycle

- Understand risk management problem from a systems perspective
  - Response should be commensurate with risk and system/network criticality
  - Need to understand levels of vulnerability and threat relative to each system

- Investigate higher assurance characteristics of commercial products where we have leverage

- Continued access to global ICT is critical to DoD mission

To meet tomorrow's threat we must develop protection measures across product lifecycle and reinforce these measures through USG acquisition processes and effective implementation of agency security practices.

DoD Defense-in-Breadth Technical Toolbox: Systems Assurance

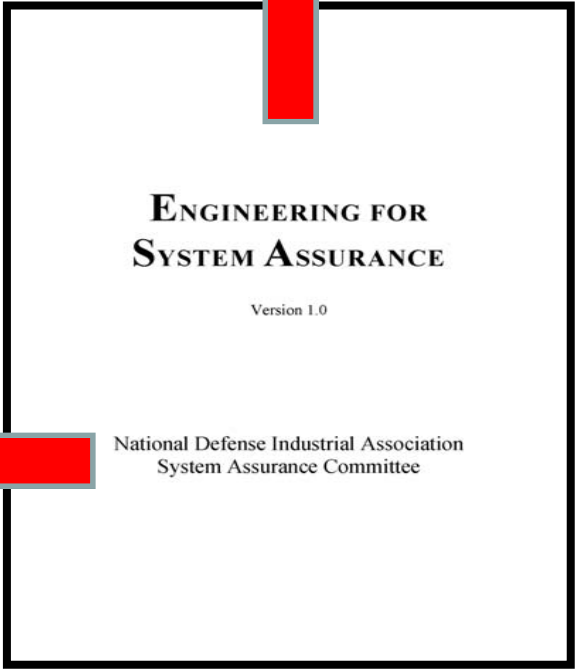
- Systems Engineering Guidance for Systems Assurance
  - Maps ISSE, Anti-tamper/software protection, program protection planning to DoD acquisition/systems engineering lifecycle
  - Identifies critical components for enhanced protection
- SCRM Key Practices Guide
  - Implements Defense-in-breadth approach by identifying supply chain risk mitigation measures across entire lifecycle
- Trusted Access Program Office/Trusted Foundry
  - Provides leading-edge DoD application specific integrated circuits (ASIC) from cleared foundries
- Software Assurance
  - Software static analysis methodology and metrics
  - Enhanced vulnerability detection R&D
- **NDAA Section 254 - Report to Congress**

Engineering for Systems Assurance

- Developed by AT&L and NII through NDIA Systems Assurance Committee
- Intent of the Guidebook: Provide practical guidance augmenting systems engineering with systems assurance practices
  - Provide knowledge for applying technical assurance measures within ISO 15288 systems engineering technical process
  - Encompass overall program and project management
  - Integrate systems assurance into the acquisition lifecycle
- Guidance developed using DOD Lifecycle Framework
  - Guidance for each technical review within the lifecycle
  - “Proto-checklist” level of detail
  - Built IA, program protection, Anti-tamper into lifecycle, as they pertain to and enforce system assurance
- Scope
  - Management of risk
  - Assurance of security
  - All within the context of system and software lifecycles

“SYSTEM ASSURANCE IN NATO PROGRAMMES” (AEP-67)

“NIST-IR 7622”



ENGINEERING FOR SYSTEM ASSURANCE

Version 1.0

National Defense Industrial Association
System Assurance Committee

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</u>
<u>COUNTERFEITS</u>

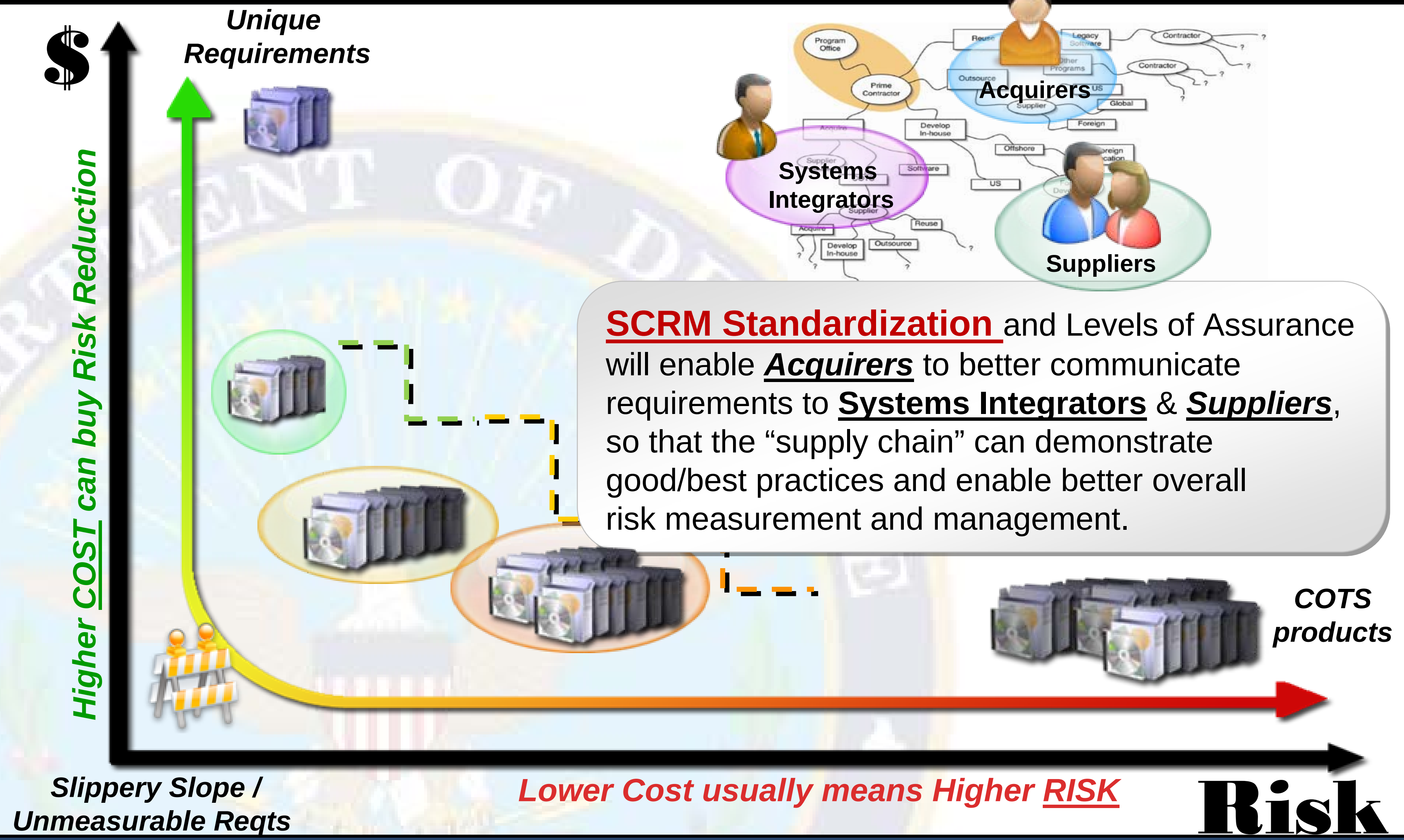
especially
during

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

Collaborating with Industry

- Understand industry perspective for managing supply chain risk
  - Both minimums and best practices
  - Technical solutions under development
  - Areas where government policy must be improved
- Develop commercially-acceptable standards that advance the state of the art for managing a global ICT supply chain
  - Types of standards: Process, Product/System, Management
  - Key themes: Prioritization, Transparency/Awareness
  - Reference standards in sourcing
- CS1 portfolio includes key standards that can help
  - ISO/IEC 27001 and 27002 revisions
  - Guidelines for Security of Outsourcing
  - Guidelines for Secure System Design Principles
  - Application Security
  - Supply Chain Trust/Security: National & International Study Periods
  - **ISO 27036: Information technology – Security techniques –Information Security for Supplier Relationships**

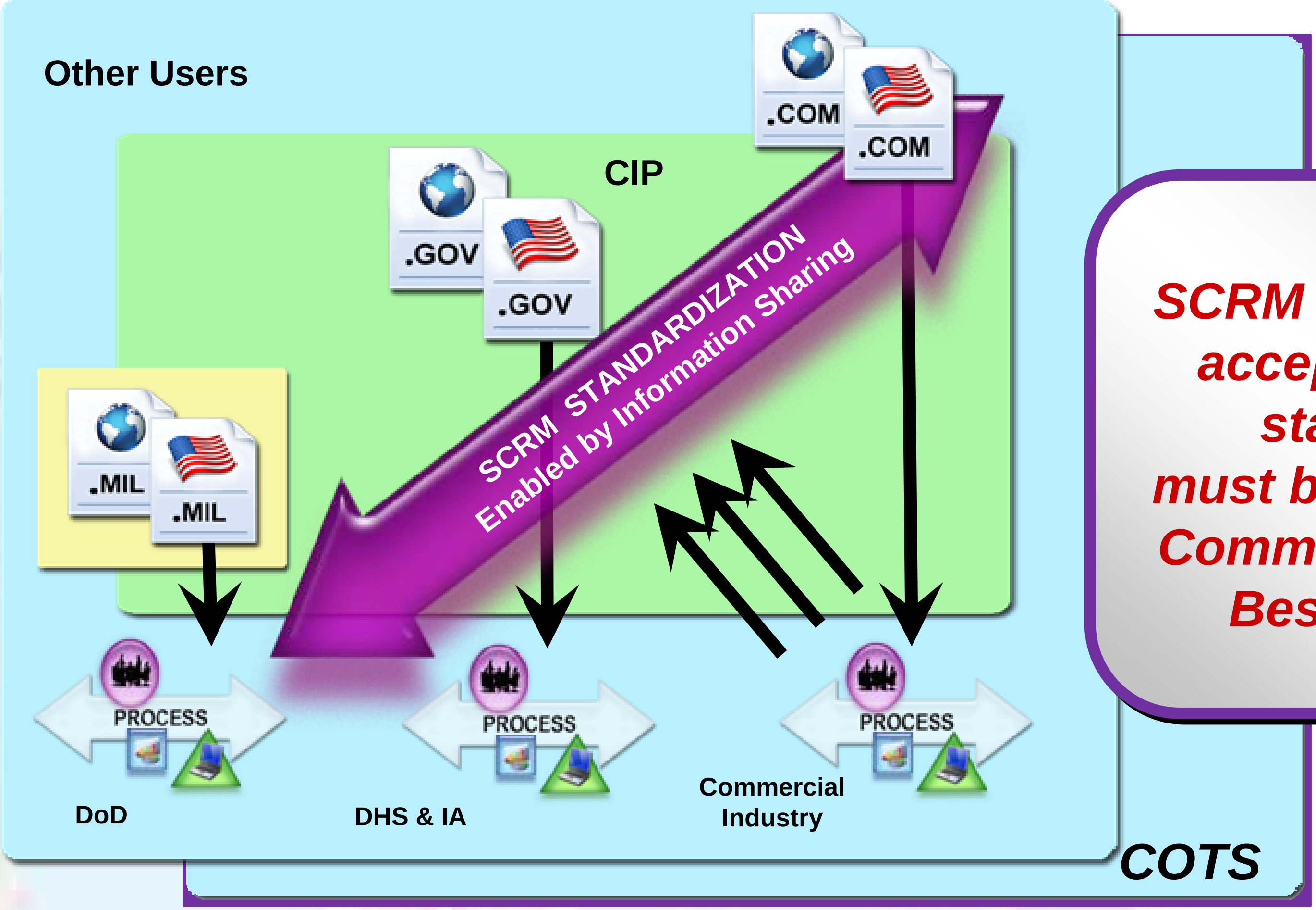
Product Assurance *TRADESPACE*



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.

SCRM Stakeholders

US has vital interest in the global supply chain.

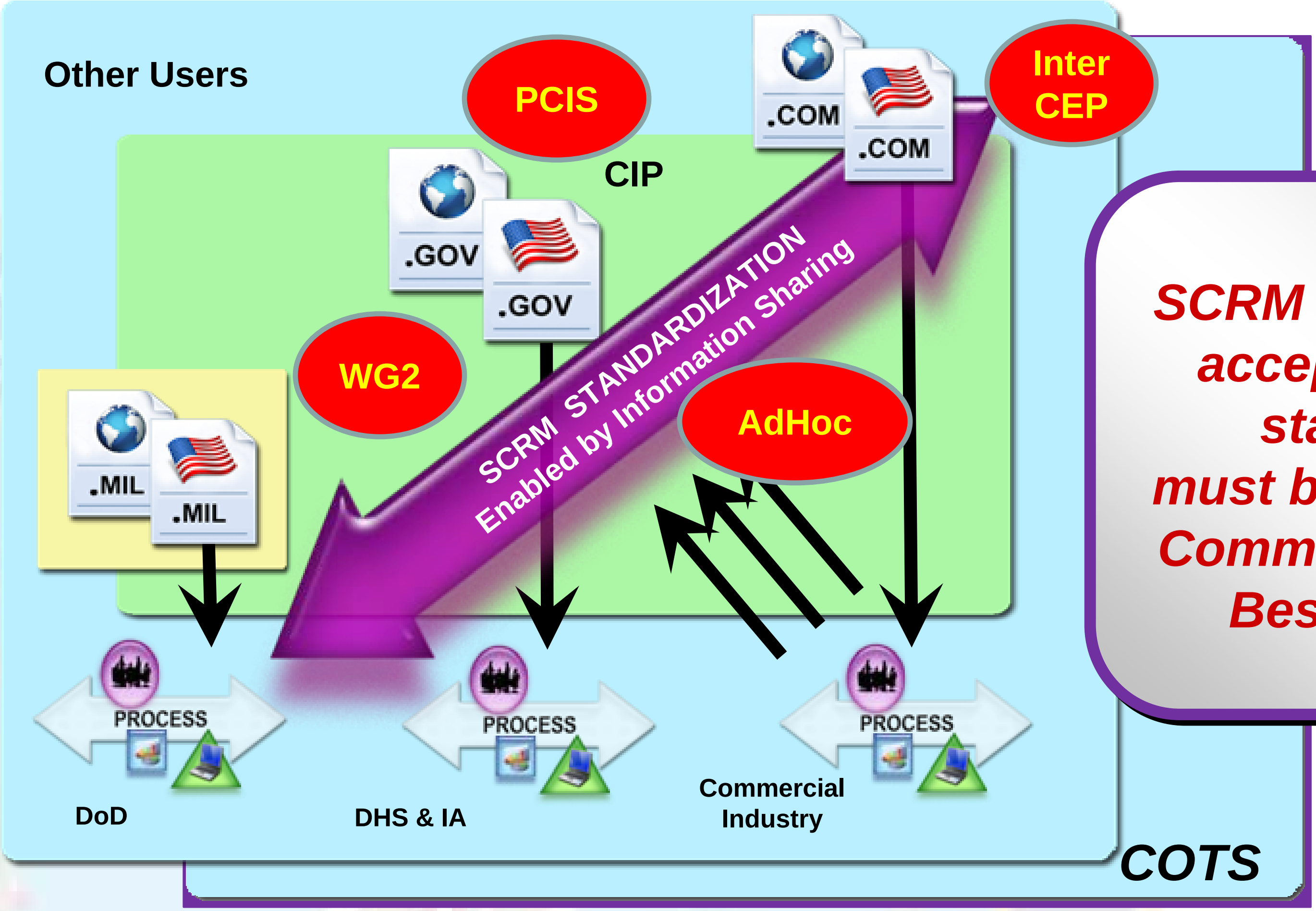


SCRM "commercially acceptable global standard(s)" must be derived from Commercial Industry Best Practices.

SCRM Standardization Requires Public-Private Collaborative Effort

SCRM Stakeholders

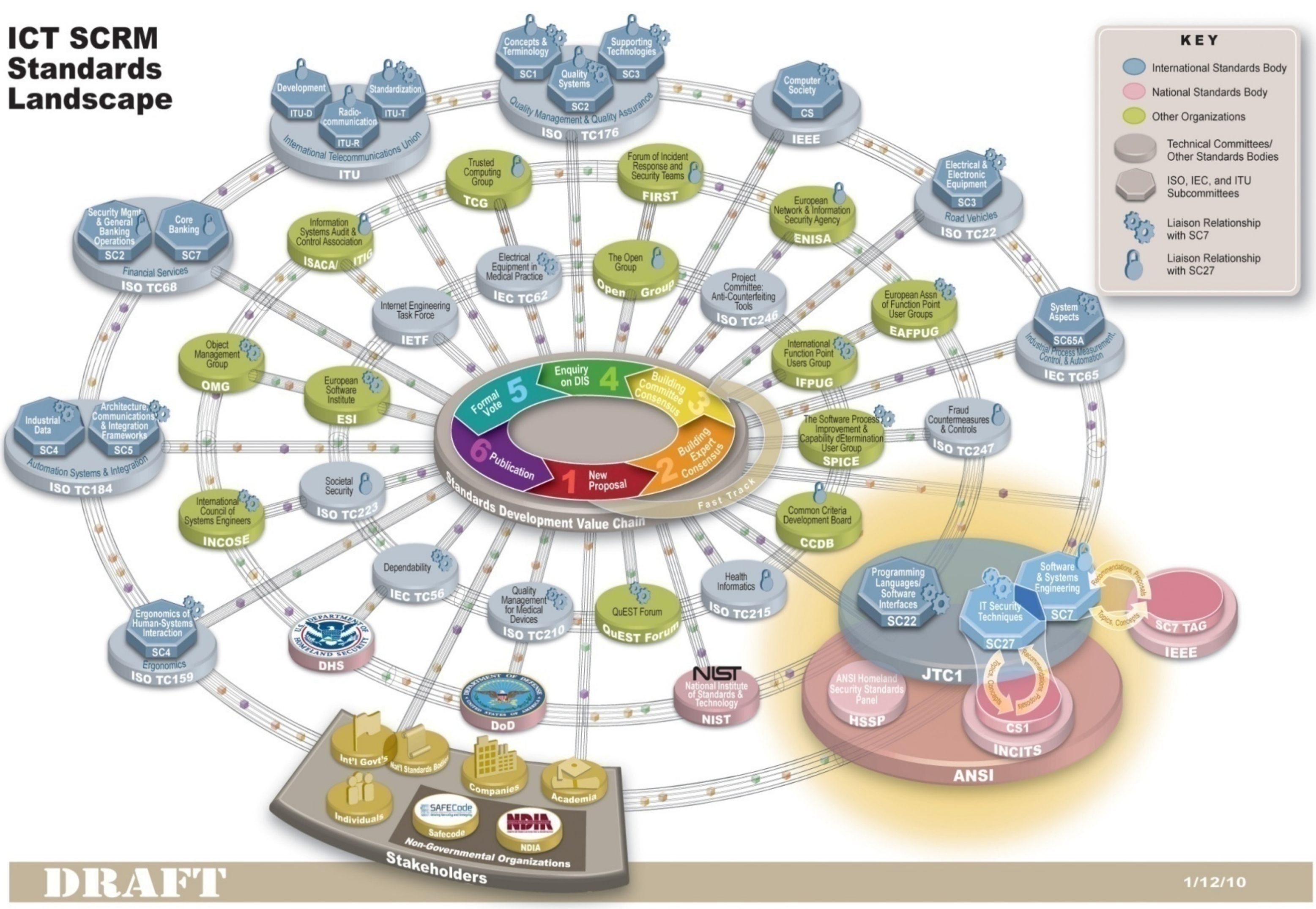
US has vital interest in the global supply chain.



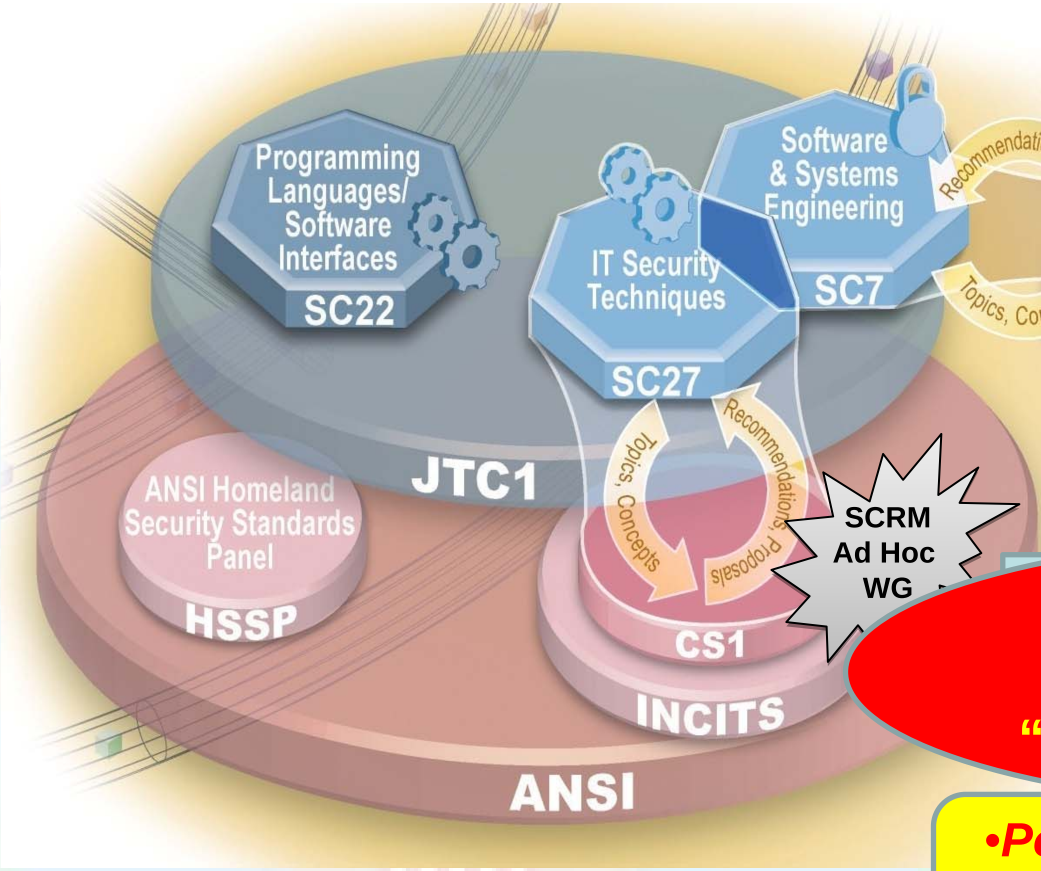
SCRM "commercially acceptable global standard(s)" must be derived from Commercial Industry Best Practices.

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
International Function Point Users Group
IFPUG
Object Management Group
OMG
European Software Institute
ESI
Industrial Data
SC4
Architecture, Communications, & Integration Frameworks
SC5
Automation Systems & Integration
ISO TC184
Formal Vote
5
Enquiry on DIS
4
Building Committee Consensus
3
Building Expert Consensus
2
New Proposal
1
Publication
6
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
Programming Languages/ Software Interfaces
SC22
IT Security Techniques
SC27
Software & Systems Engineering
SC7
Recommendations, Proposals
Topics, Concepts
SC7 TAG
IEEE
JTC1
Ergonomics of Human-Systems Interaction
SC4
Ergonomics
ISO TC159
DHS
DoD
NIST
National Institute of Standards & Technology
NIST
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
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

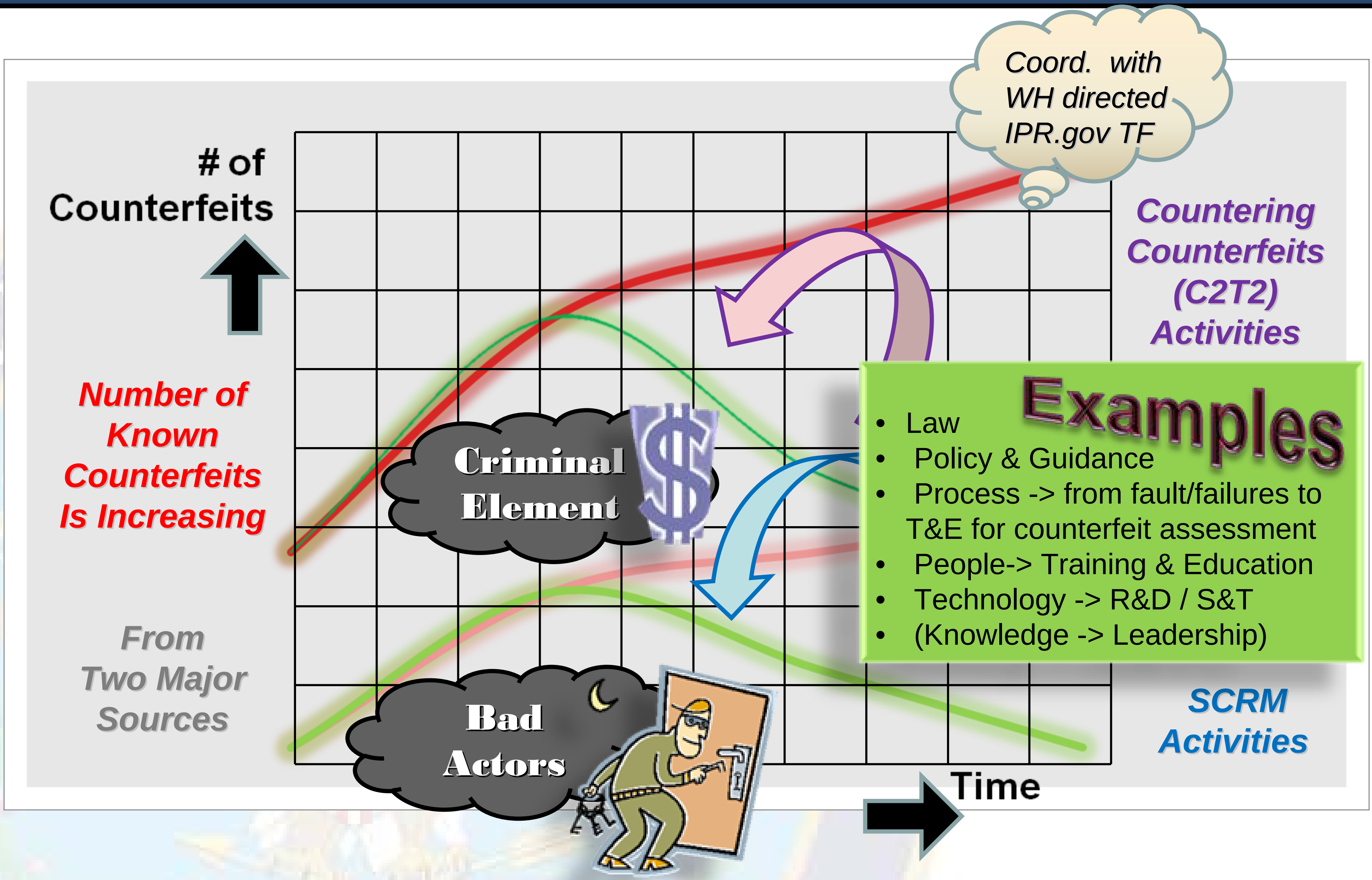
ISO 27036

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

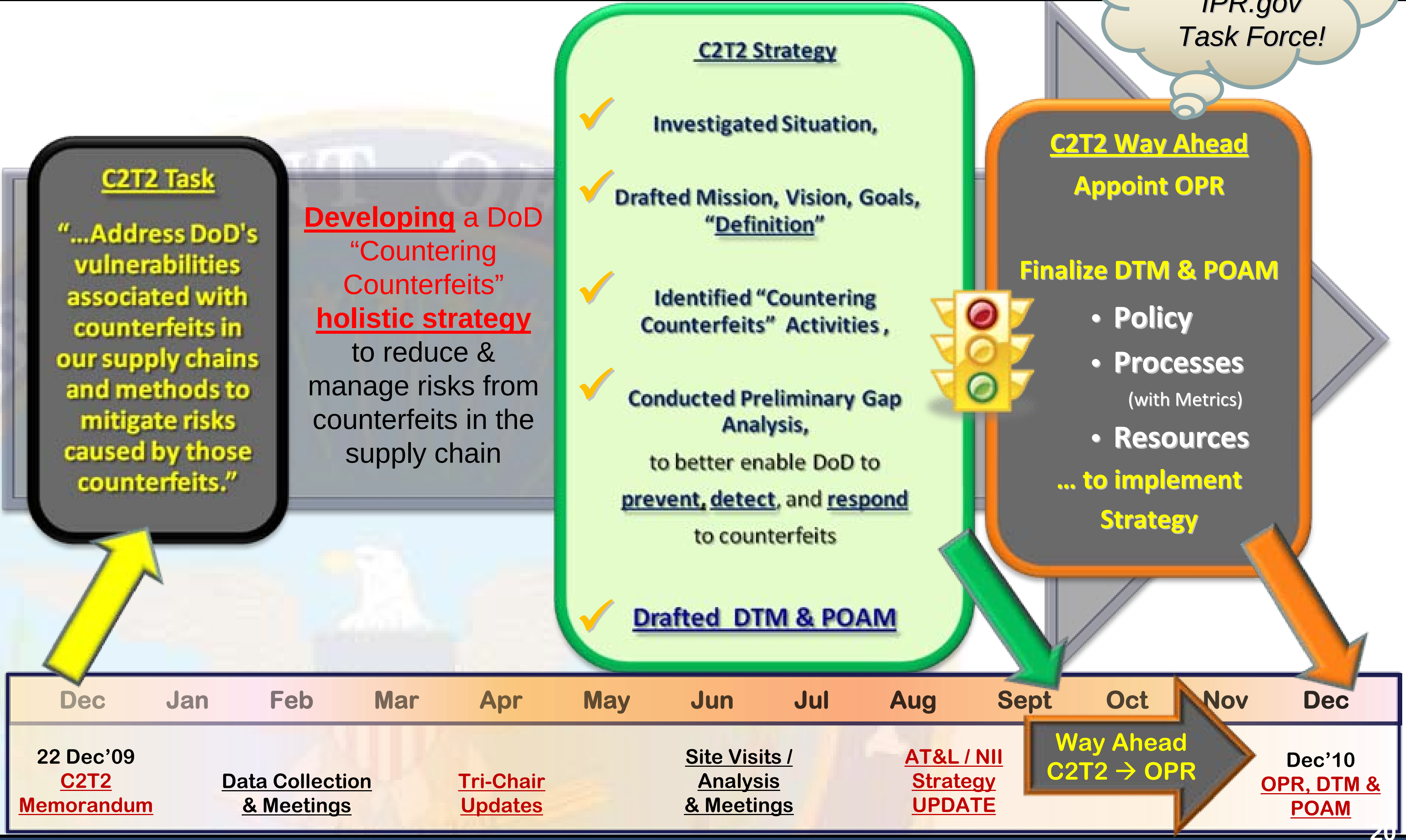
Examples

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

SCRM Activities

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

Task & Background

The Threat

Our Vulnerabilities

Potential Consequences

Counterfeiting is a Daily Media Topic and raises Congressional interest.

Task: Develop DoD Response(s) to:

- *Department of Commerce Report*
- ***GAO Reports***
- Continuing Media Coverage
- **2010 National Security Strategy**
- Draft Legislation NDAA 2011
- ***Draft Executive Order***
- *Congressional Interest*

TASK: Counter effects of Counterfeits in DoD

Challenges in Acquisition & Procurement

Uncertainty with Respect to Numbers

Lack of Trust in Supplier Base

Background: Data Collection

- Collected Data on “countering counterfeits” efforts
- Examined efforts and Produced “Counterfeits” Report

  -Documenting anti-counterfeiting activities / reports

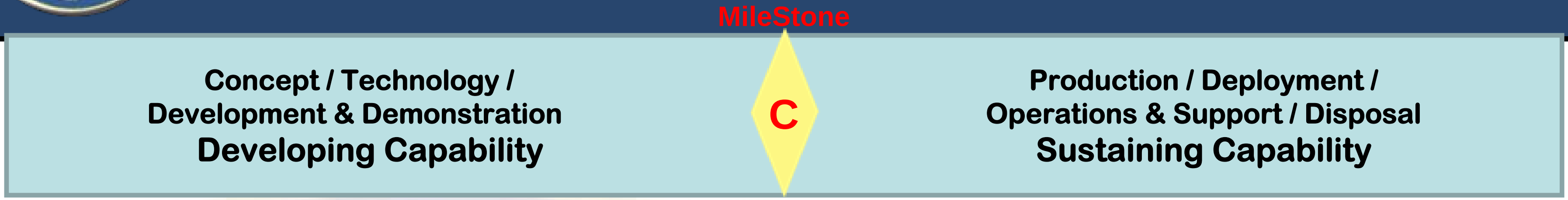
  (117 total, including 21.mil + 42.gov + 28.org/.com)

- Conducted Site Visits (Industry, Depots & DMEA)
- Documented Best Practices

- Shared briefings / information from DoD organizations
- Developed DRAFT Mission, Vision, Goals (POAM & DTM)
- Still exploring Definition & Office of Primary Responsibility (OPR)

Background: Analysis

Where do we have trade space / How do we manage risk?



MileStone

C

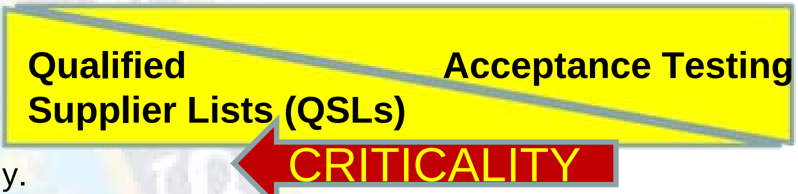
Concept / Technology /
Development & Demonstration
Developing Capability

Production / Deployment /
Operations & Support / Disposal
Sustaining Capability

Who's "managing" the supply chain to enable Systems / Mission Assurance?
What's the industry perspective & what's the DoD perspective?
Are the perspectives different, pre & post Milestone C?

Supplier Control: Trusted / Quality Suppliers vs. Acceptance Testing

If acquirer has previous (documented) trust and confidence in a supplier's ability to deliver "quality" / legitimate product(s), then the acquirer may not need to spend as much time & resources on acceptance testing.



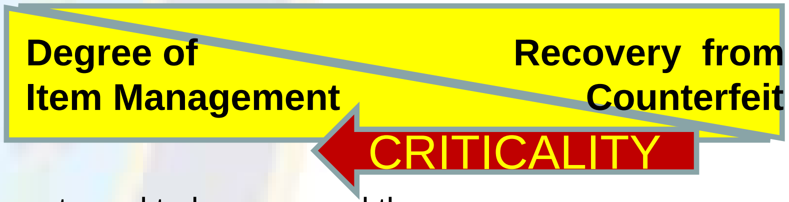
Qualified Supplier Lists (QSLs)

Acceptance Testing

CRITICALITY

Part(s) Control: Managing Resupply / Parts

Acquirer / user has flexibility in management of "parts" / resupply.
  - ***Parts*** can be individually managed (i.e. IUID) from manufacturing to disposal (or subset). Parts can be managed by manufactured lots, batches etc., and can be mixed and managed by new "sets" / purchased groupings.
  - ***Parts / Resupply*** may be mixed and not managed, where traceability of individual items, lots, purchases are lost (while it costs more to manage by item, there are risks associated with migrating from individual parts management because of a potential loss of larger "contaminated" sets.)



Degree of Item Management

Recovery from Counterfeit

CRITICALITY

Variability: Commodities & Classes of Supply

All commodities & classes of supply are not created equal & may not need to be managed the same.

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