



Trusting ICT in today's Global Supply Chain – Understanding and Implementing Government and Industry Best Practices

Michele Moss
SSTC Conference
May 17, 2010

Report Documentation Page

Form Approved
OMB No. 0704-0188

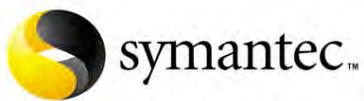
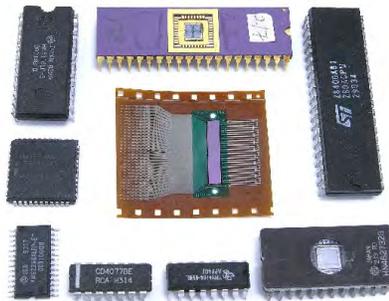
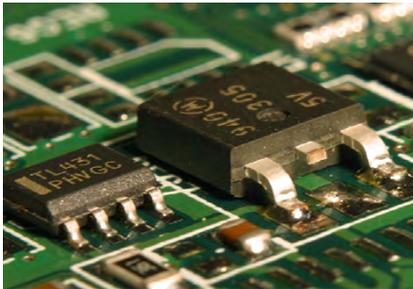
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 17 MAY 2010	2. REPORT TYPE	3. DATES COVERED 00-00-2010 to 00-00-2010			
4. TITLE AND SUBTITLE Trusting ICT in today's Global Supply Chain - Understanding and Implementing Government and Industry Best Practices		5a. CONTRACT NUMBER			
		5b. GRANT NUMBER			
		5c. PROGRAM ELEMENT NUMBER			
6. AUTHOR(S)		5d. PROJECT NUMBER			
		5e. TASK NUMBER			
		5f. WORK UNIT NUMBER			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Booz Allen Hamilton Inc,8283 Greensboro Dr,McLean,VA,22102		8. PERFORMING ORGANIZATION REPORT NUMBER			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)			
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)			
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES Presented at the 23rd Systems and Software Technology Conference (SSTC), 16-19 May 2011, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 38	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Table Of Contents

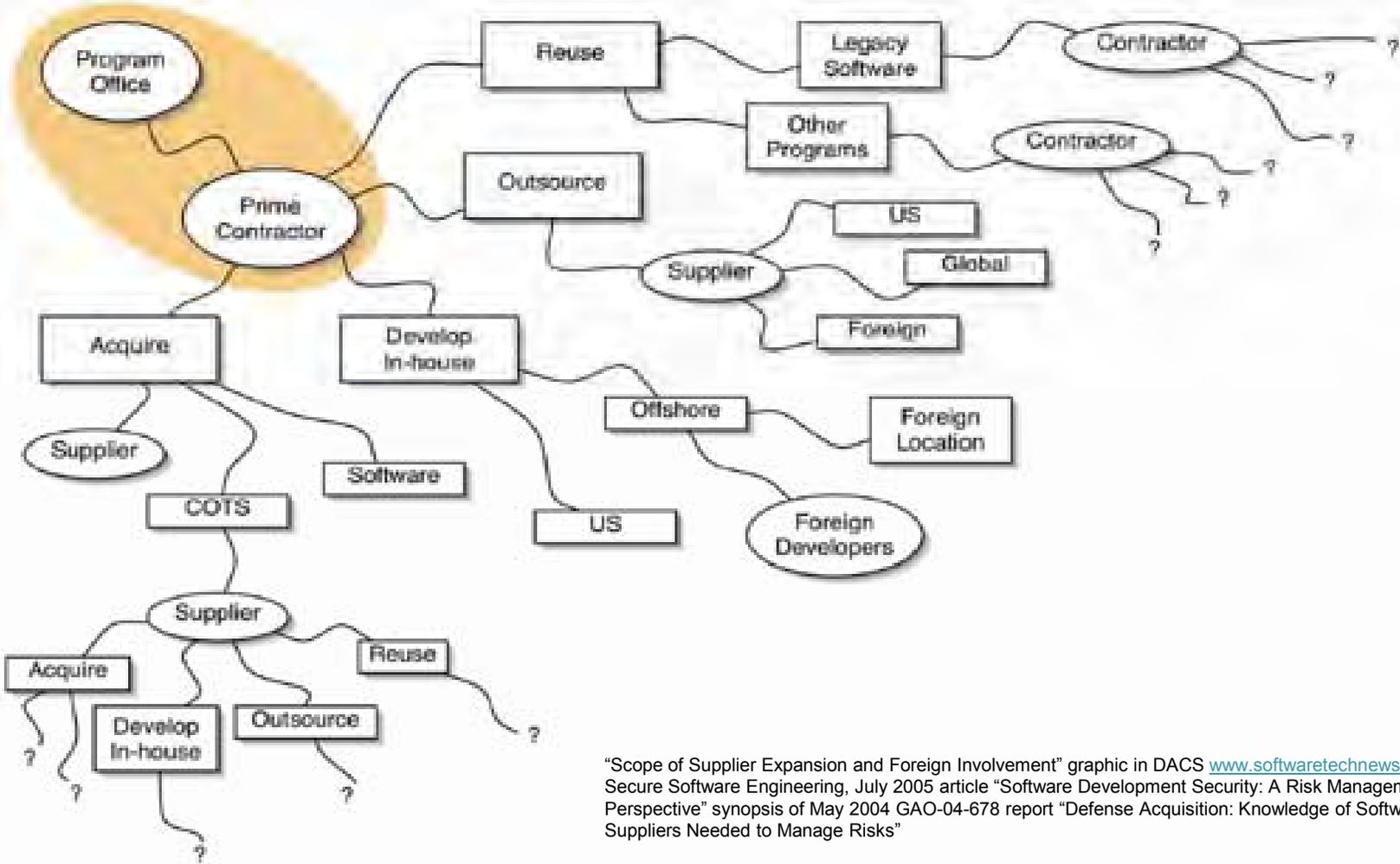
- ▶ Globalization Challenges
- ▶ Understanding The Problem
- ▶ DOD Tool Box for SCRM
- ▶ Working Towards A Solution

What is ICT?



Images extracted from a presentation on actual counterfeit IT products incidents

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”

System Delivery Example - Private Sector Scenario



\$7,474,793.00 - 85' custom-built motor yacht (4 state rooms, State-of-the-art galley, GPS System, Radar for navigation, Twin supercharged diesel engines)

Planned Delivery

- **Celebration (\$1500.00)**
 - Champagne
 - Chocolate covered strawberries with cream
 - Music dockside for the excited 'soon to be owner' and a small group of his friends
- **Logistics**
 - Two corporate representatives
 - Crane
 - Rigging \$2,500.00 a hour minimum

Courtesy of Don Davidson, OSD TMSN ,Chief of Outreach and Standardization

System Delivery Example - Private Sector (continued)



- ▶ Critical Component in the rigging contained a faulty \$25.00 dollar turnbuckle.

Courtesy of Don Davidson, OSD TMSN , Chief of Outreach and Standardization

Table Of Contents

- ▶ Globalization Challenges
- ▶ Understanding The Problem
- ▶ DOD Tool Box for SCRM
- ▶ Working Towards A Solution

From *The World Is Flat* by Thomas Friedman

Dell Inspiron 600m Notebook: Key Components and Suppliers

Component	Supplier or Potential Suppliers
Intel Microprocessor	 US-owned factory in the Philippines, Costa Rica, Malaysia, or China (<i>Intel</i>)
Memory	 South Korea (<i>Samsung</i>), Taiwan (<i>Nanya</i>), Germany (<i>Infineon</i>), or Japan (<i>Elpida</i>)
Graphics Card	 China (<i>Foxconn</i>), or Taiwanese-owned factory in China (<i>MSI</i>)
Cooling fan	 Taiwan (<i>CCI and Auras</i>)
Motherboard	 Taiwan (<i>Compal and Wistron</i>), Taiwanese-owned factory in China (<i>Quanta</i>), or South Korean-owned factory in China (<i>Samsung</i>)
Keyboard	 Japanese company in China (<i>Alps</i>), or Taiwanese-owned factory in China (<i>Sunrex and Darfon</i>)
LCD	 South Korea (<i>Samsung, LG.Philips LCD</i>), Japan (<i>Toshiba or Sharp</i>), or Taiwan (<i>Chi Mei Optoelectronics, Hannstar Display, or AU Optronics</i>)
Wireless Card	 Taiwan (<i>Askey or Gemtek</i>), American-owned factory in China (<i>Agere</i>) or Malaysia (<i>Arrow</i>), or Taiwanese-owned factory in China (<i>USI</i>)
Modem	 China (<i>Foxconn</i>), or Taiwanese company in China (<i>Asustek or Liteon</i>)
Battery	 American-owned factory in Malaysia (<i>Motorola</i>), Japanese company in Mexico, Malaysia, or China (<i>Sanyo</i>), or South Korean or Taiwanese factory (<i>SDI and Simplo</i>)
Hard Disk Drive	 American-owned factory in Singapore (<i>Seagate</i>), Japanese-owned company in Thailand (<i>Hitachi or Fujitsu</i>), or Japanese-owned company in the Philippines (<i>Toshiba</i>)
CD/DVD	 South Korean company with factories in Indonesia and Philippines (<i>Samsung</i>), Japanese-owned factory in China or Malaysia (<i>NEC</i>), Japanese-owned factory in Indonesia, China, or Malaysia (<i>Teac</i>), or Japanese-owned factory in China (<i>Sony</i>)
Notebook Carrying Bag	 Irish company in China (<i>Tenba</i>), or American company in China (<i>Targus, Samsonite, and Pacific Design</i>)
Power Adapter	 Thailand (<i>Delta</i>), or Taiwanese-, South Korean-, or American-owned factory in China (<i>Liteon, Samsung, and Mobility</i>)
Power Cord	 British company with factories in China, Malaysia, and India (<i>Vollex</i>)
Removable Memory Stick	 Israel (<i>M-System</i>), or American company with factory in Malaysia (<i>Smart Modular</i>)

Technology Is A Focal Point Of Attacks

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

According to an article in the May 2010 National Defense Magazine, well funded nation states and terrorist organizations are engaging in cyber attacks against US government systems. Examples of those include 44,000 Turkish teenagers in a military style community of hackers learning from each other.

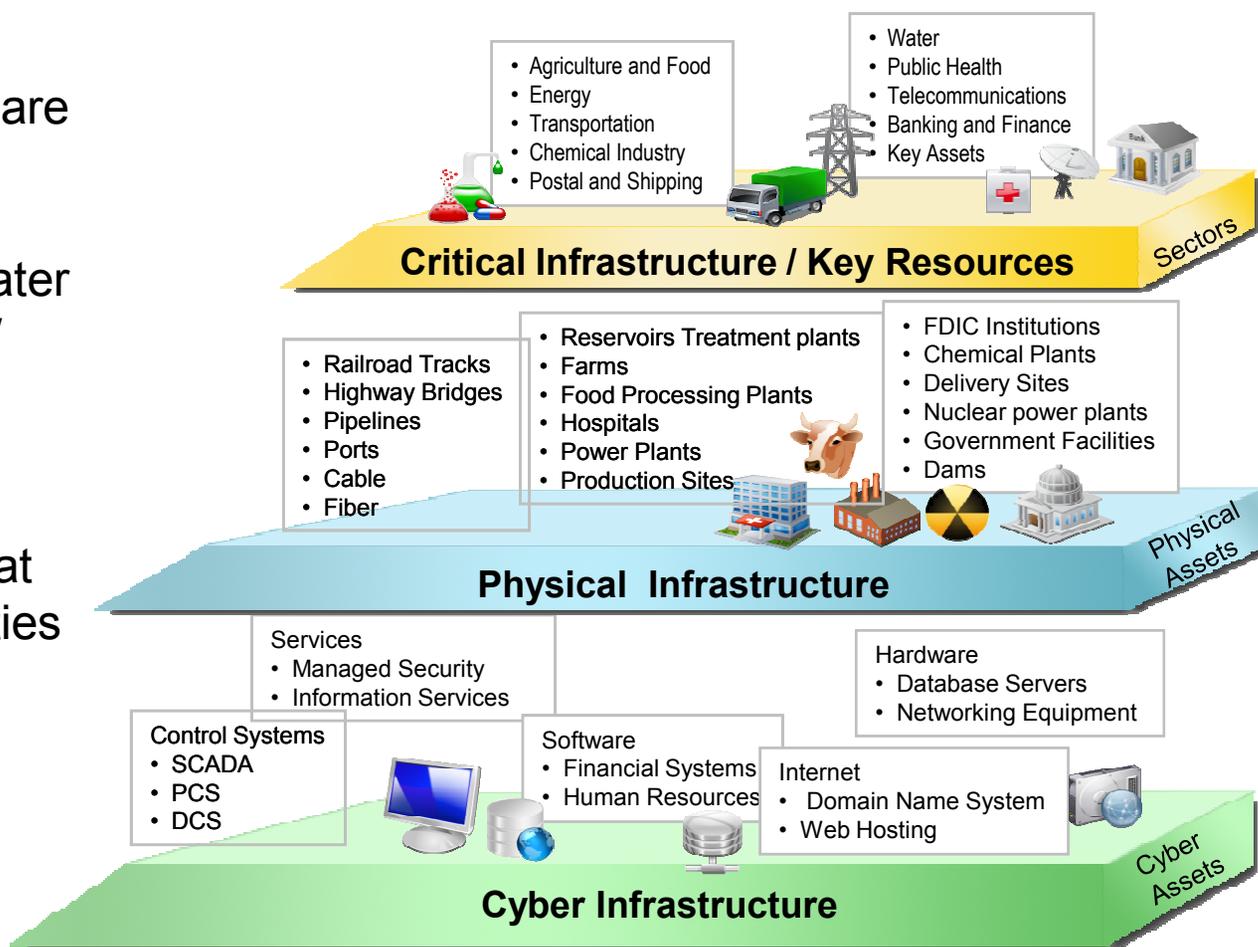
There are also 100,000 hackers learning from each other in Saudi Arabia, 40,000 in Iraq, and over 400,000 in China.

32%



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

- ▶ Dependencies on technology are greater than 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



Increased Priority for Program Protection

- ▶ *Threats*: Nation-state, terrorist, criminal, rogue developer who:
 - Gain control of systems through supply chain opportunities
 - Exploit vulnerabilities remotely
- ▶ *Vulnerabilities*: All systems, networks, applications
 - Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
 - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ▶ *Consequences*: Stolen critical data & technology; corruption, denial of critical warfighting functionality

Today's acquisition environment drives the increased emphasis:

<u>Then</u>		<u>Now</u>
Standalone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers

Source: Source: September 28, 2010 SwA Forum, DoD Trusted Defense Systems, Ms. Kristen Baldwin, DDR&E/Systems Engineering

“Maryland Man Sentenced to 84 Months in Prison for Defrauding Cisco Systems Inc. ”

INCIDENT:

Chinasa manufactured counterfeit computer networking and telecommunications equipment. He or Chambliss would then contact Cisco, falsely claiming that they were having trouble with a Cisco product covered by a warranty. Cisco would issue replacement parts, but its warranty required return of the allegedly defective product. To satisfy that return policy, Chinasa and Chambliss would send their counterfeit product to Cisco.

MITIGATION:

Iheanyi Frank Chinasa, 39, of Gaithersburg, Md., and Chambliss, 31, of Henrico, Va., were indicted on Aug. 18, 2010. Chambliss pleaded guilty on Jan. 12, 2011, to conspiring to commit mail fraud and wire fraud. Chambliss was sentenced on April 13, 2011, to 12 months and one day in prison and ordered to pay \$18,761,825 in restitution. Chinasa was sentenced to 84 months in prison for his participation in a scheme to defraud Cisco Systems Inc.,

IMPACT:

Cisco was defrauded of over \$27 million in assets and impacted consumer reliability.



<http://richmond.fbi.gov/dojpressrel/pressrel11/ri050511.htm>

“U.S. charges Florida pair with selling counterfeit computer chips from China to the U.S. Navy and military”

INCIDENT:

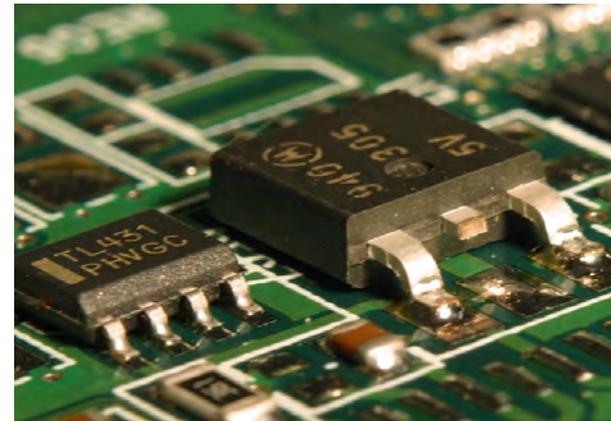
On September 14, 2010 Federal prosecutors in Washington unsealed charges accusing a Florida pair of selling more than 59,000 counterfeit computer microchips from China to the U.S. Navy and other clients for military use aboard American warships, fighter planes, missile and antimissile systems. Wren, owner of VisionTech Components and related companies, and McCloskey, an administrator, were charged with conspiracy, trafficking in counterfeit goods and mail fraud.

MITIGATION:

In January the Commerce Department reported that the number of counterfeit incidents discovered by the military and its suppliers more than doubled between 2005 to 2008, to more than 9,356 cases. Meanwhile, lawmakers and congressional investigators have called on the Pentagon and law-enforcement agencies to combat the problem more aggressively.

IMPACT:

The case marked the latest effort by U.S. authorities to stem the flow of fake electronics into the U.S. military supply chain, as warnings mount that fake chips could be defective or "electronic Trojan horses" that would allow hackers to disable them or track their use. Several recent government reports warn that computer chips marked with false brands or mislabeled as military-grade may include imperfections that could cripple or degrade weapons systems in combat or over time.



<http://www.washingtonpost.com/wp-dyn/content/article/2010/09/14/AR2010091406468.html>

“California MVP MICRO, INC. Owner pleads guilty in connection with sales of counterfeit high tech parts to the U.S Military”

INCIDENT:

On January 14, 2010 Mustafa Abdul Aljaff, 30, of Newport Coast, California, plead guilty to Counts One and Six of an Indictment charging him and others with conspiracy to traffic in counterfeit computer chips. Aljaff and others entered into contracts with the U.S. Navy and other government agencies for the sales of integrated circuits. Subsequently, they shipped integrated circuits bearing false, counterfeit trademarks to the U.S. Navy, in Washington, D.C

MITIGATION:

The collaborative efforts of Immigration Customs Enforcement (ICE), Naval Criminal Investigative Service (NCIS), Washington, D.C., Special Agent in Charge Andre Martin, Internal Revenue Service (IRS), and Office of Inspector General (DOT OIG). These organizations continue to aggressively pursue individuals and organizations engaging in intellectual property rights crimes.

IMPACT:

Integrated circuits are used in a wide array of modern electronic products including consumer electronics and transportation, medical, aircraft, spacecraft, and military applications. The use of counterfeit integrated circuits can result in product malfunction or failure, and can also cause serious bodily injury from electrocution and, in some circumstances, death. Counterfeit goods creates a risk to public safety and national security.



<http://www.iacc.org/news-media-resources/news-archive/california-mvp-micro-inc-owner-pleads-guilty.php>

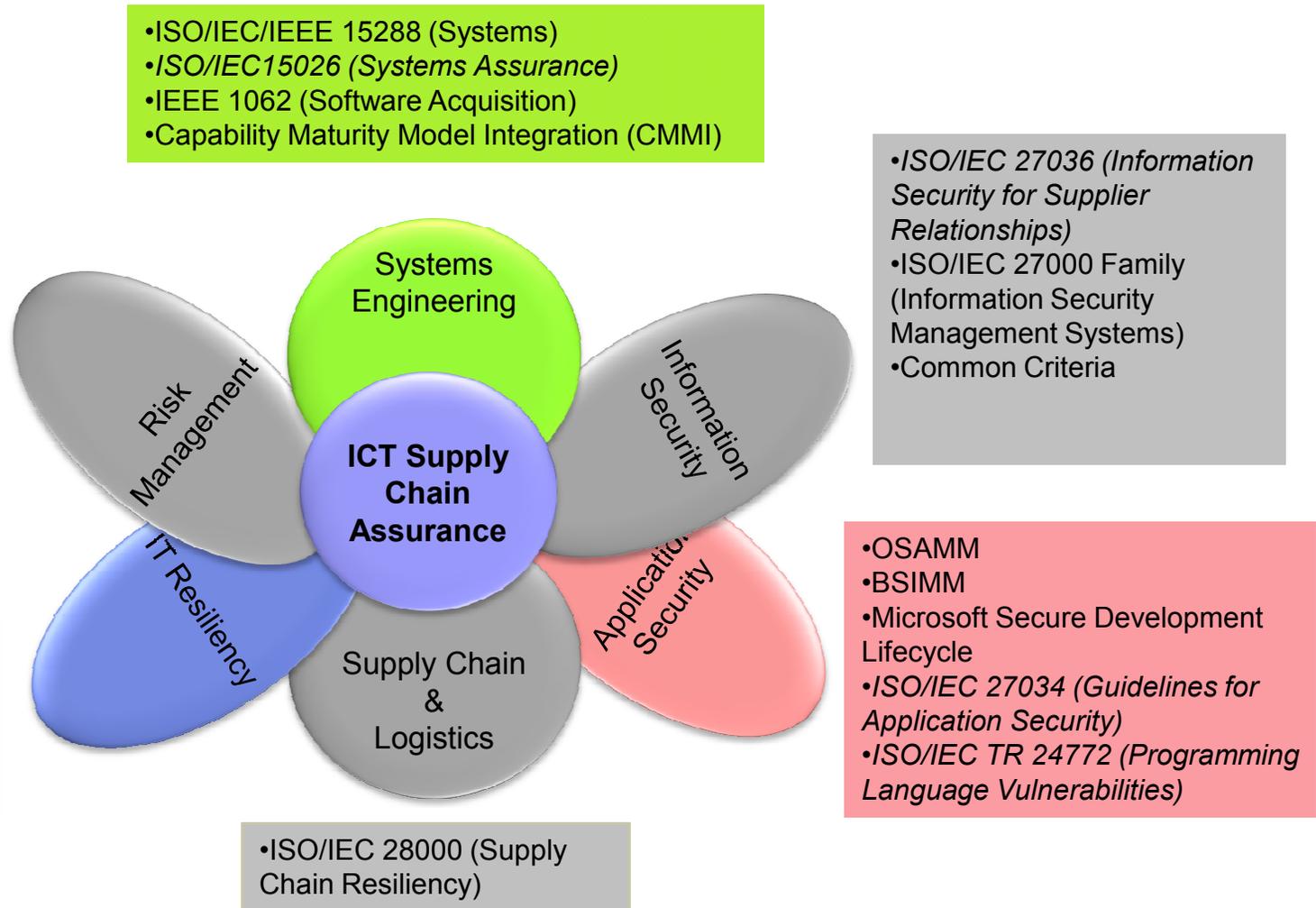
Table Of Contents

- ▶ Globalization Challenges
- ▶ Understanding The Problem
- ▶ DOD Tool Box for SCRM
- ▶ Working Towards A Solution

Why is ICT SCRM standardization Important to the USG?

“**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.**”

ICT Supply Chain Risk Management requires contributions and collaboration among many disciplines with recognized standards



ICT Supply Chain Assurance: *An IATAC State-of-the-Art Report*

The following link is available to personnel accessing from within a .mil or .gov domain:

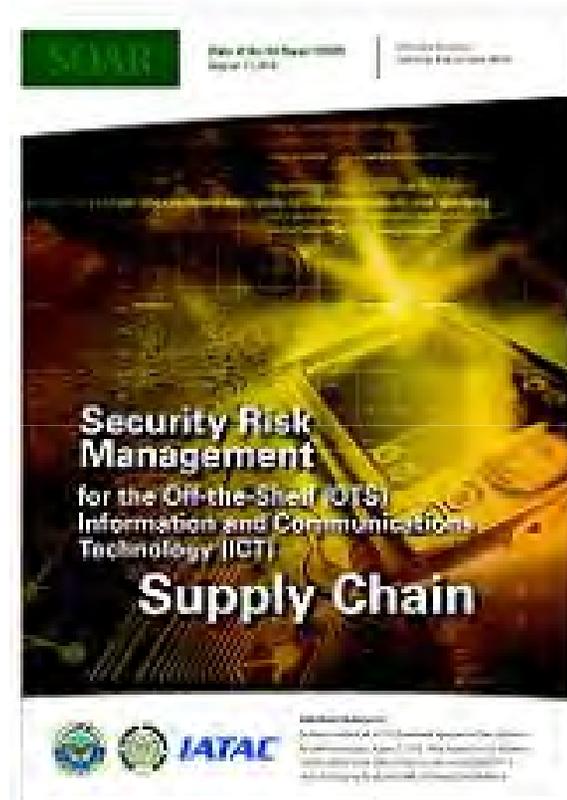
URL: http://iac.dtic.mil/iatac/pdf/supply_chain.pdf

You may also contact IATAC directly to obtain access to this report. The easiest way for you and the IATAC team to get you the report is for you to

**Information Assurance Technology Analysis Center
(IATAC)**

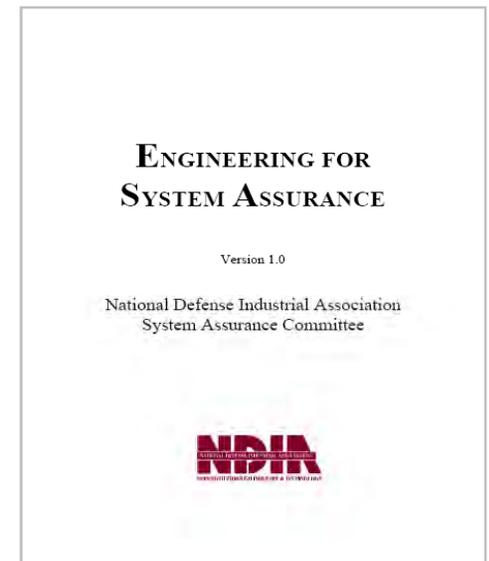
Email: iatac@dtic.mil

URL: <http://iac.dtic.mil/iatac/>



National Defense Industrial Association Guidebook on Engineering for System Assurance

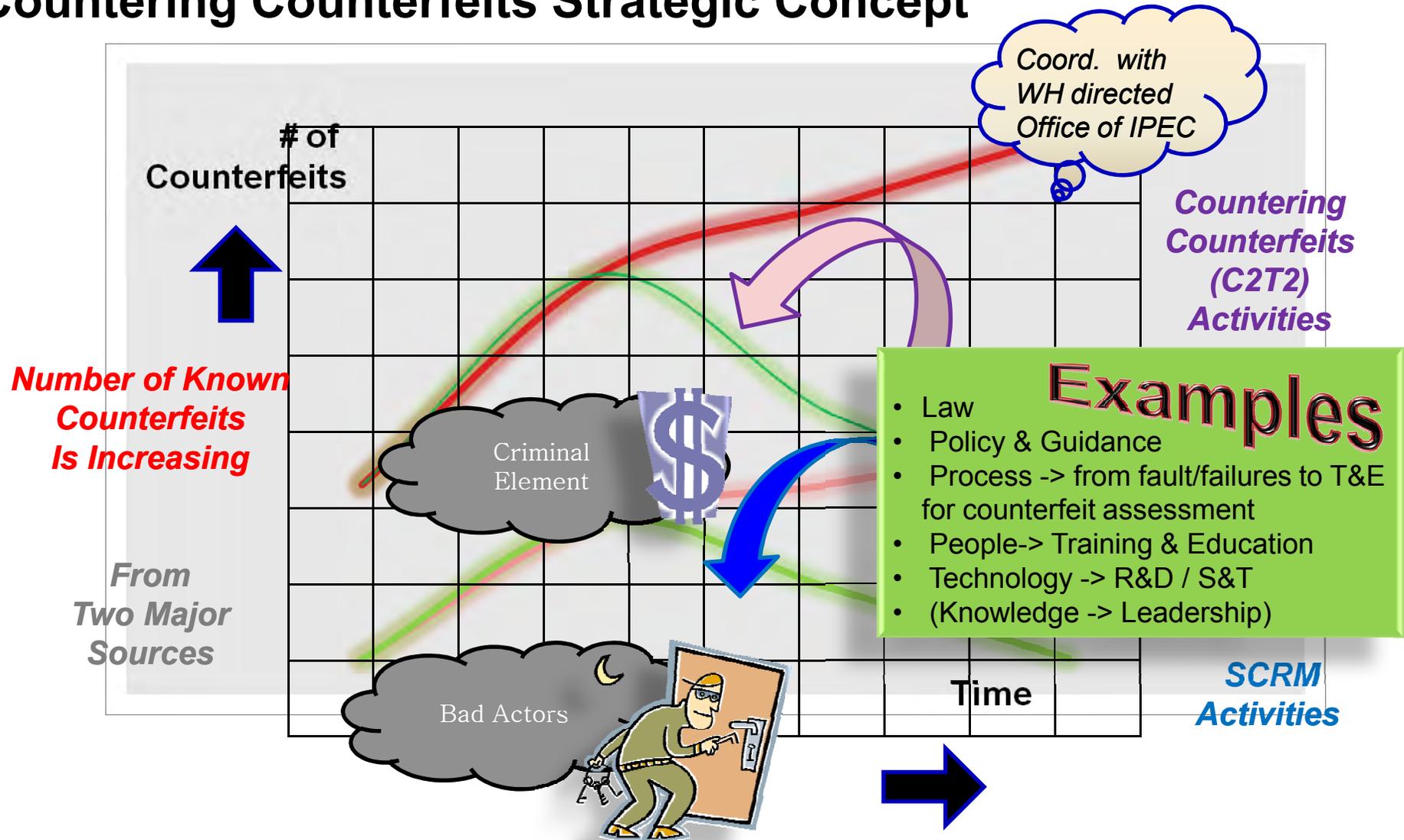
- ▶ Intended to supplement the knowledge of systems (and software) engineers who have responsibility for systems for which there are assurance concerns
- ▶ General Guidance mapped to ISO/IEC/IEEE 15288, System Life Cycle Processes
 - DoD Specific Guidance, mapped to DoD Acquisition Life Cycle
 - Anti-Tamper
 - DAG Lifecycle Framework
 - Technology Development Phase
 - System Development & Demonstration Phase
 - Production, Deployment, Operations, & Support Phases
 - Supporting Processes
 - Periodic Reports
 - Supplier Assurance
 - Mappings
 - Correspondence with Existing Documentation, Policies, and Standards
 - Executive Policy, Services Standards, NIST/NSA (NIAP) Standards, GEIA, AIA, IEEE, ISO Standards, Best Practice (e.g., DHS/DOD SwABOK)
 - Adopted as NATO AEP-67, Engineering for System Assurance in NATO Programmes, February 2010



<http://www.acq.osd.mil/sse/docs/SA-Guidebook-v1-Oct2008.pdf>

Courtesy of Paul Croll, IEEE

Countering Counterfeits Strategic Concept



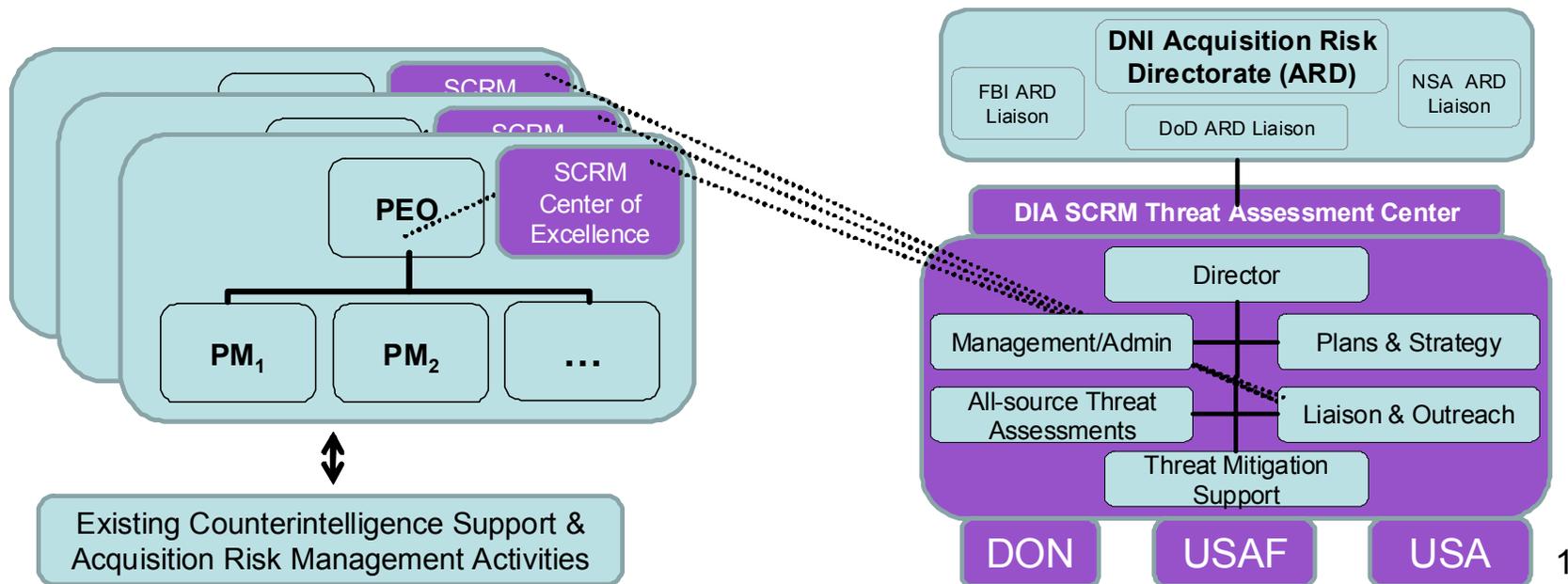
Courtesy of Don Davidson, OSD TMSN , Chief of Outreach and Standardization

DoD SCRM Pilot Program Objectives

- ▶ Enhance the capacity to produce and use supplier threat information
- ▶ Define and incrementally implement SCRM capability
 - Ensure DoD capability aligns with evolving federal capability
- ▶ Gather lessons learned
- ▶ Identify changes needed to policy, guidance, and statute
 - Proposed gap-fillers (e.g., SCRM technical controls, OMB Guidance, DoD procurement guidance)
- ▶ Create infrastructure for supporting SCRM across DoD
 - Toolkit of key practices, supporting instructions and TTPs, and possible mitigations
- ▶ Identify capability scaling factors and sensitivities

DoD SCRM Pilot Capability

- ▶ Established all-source threat assessment capability at DIA
- ▶ Established SCRM Center of Excellence in each Military Service
- ▶ SCRM Key Practices Guide



Completed over 30 DoD SCRM Pilot Projects

▶ Army

- Ground Soldier Ensemble
- Sky Warrior / One System Ground Control Station Program
- Program Executive Office, Enterprise Information Systems (PEO EIS)
- Program Executive Office Command Control Communications Tactical (PEO C3T)
- Intelligence, Electronic Warfare & Sensors (IEWIS)
- Ground Combat Vehicle

▶ Air Force

- ESSG Software Buys
- Air Force Smart Operations for the 21st Century (AFSO21) Hardware Buys

▶ Navy

- Joint Stand Off Weapon (JSOW-C)
- OB1 Integrated Network Security Levels (OBINSL)
- Joint Services IT Equipment Commodity Strategy (JSIECS)

▶ ASD/NII

- National and Nuclear Command Capabilities (N2CC)

DoD SCRM Pilot Projects Findings

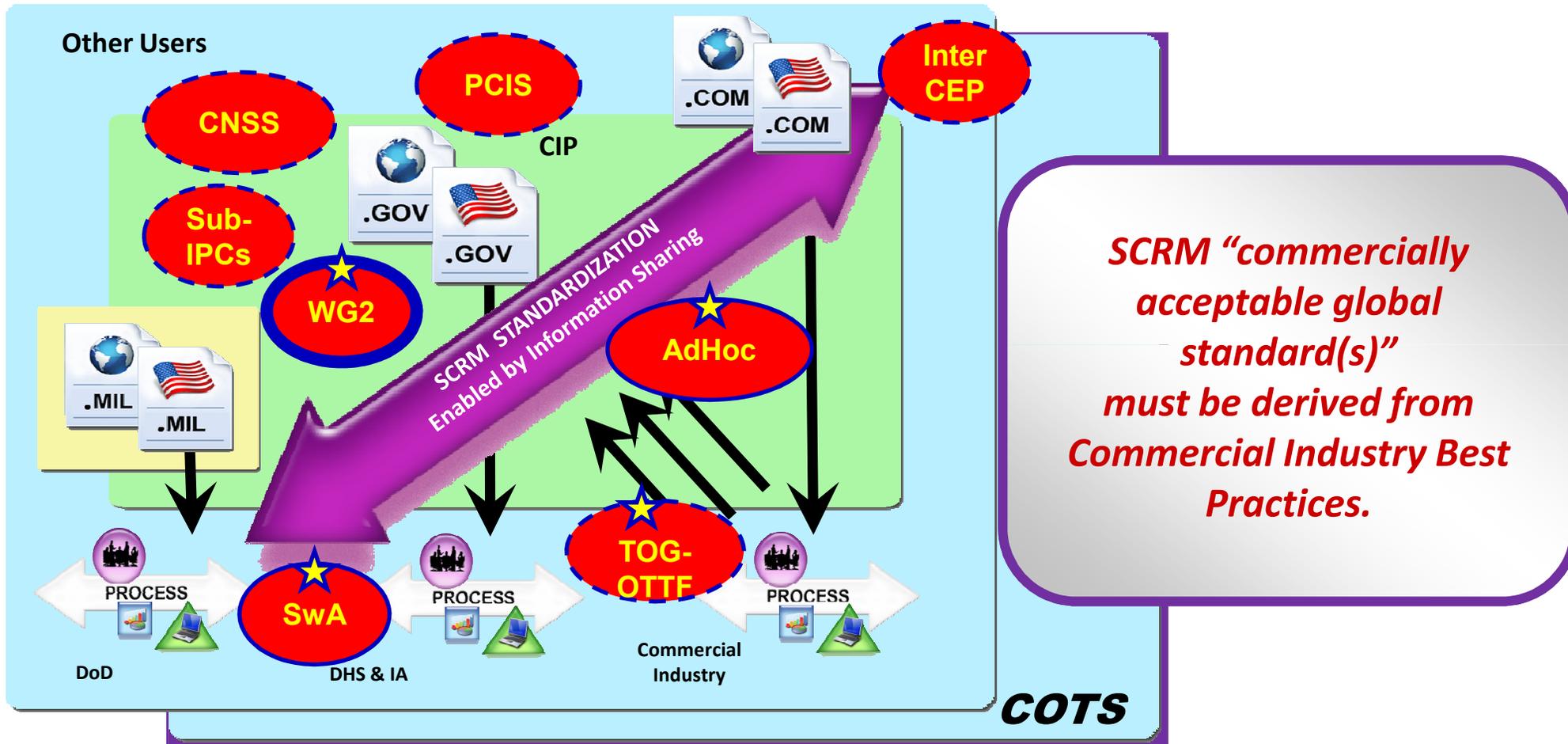
- ▶ SCRM is an essential element of acquisition, systems engineering and sustainment and must be appropriately staffed and funded
- ▶ Need for an enterprise governance of SCRM issues and mitigations
- ▶ Processes must evolve to include trust assumptions that are valid in a global supply chain
- ▶ Technology solutions to enhance trust and reduce risk to support SCRM have not been fully examined or implemented within the DoD
- ▶ Legal and contractual methods are needed to avoid those suppliers determined to present elevated supply chain risk, in addition to legislative and regulatory guidance for managing supply chain risk
- ▶ DoD policies are insufficient to address SCRM issues

What's Next for DoD SCRM Pilot Program

- ▶ Formal release of the SCRM Pilot Report and Findings
- ▶ Further integration of Test and Evaluation (T&E) capability in SCRM infrastructure
- ▶ Expand SCRM Pilots into the DoD Agencies
- ▶ Formalize SCRM Practices across all DoD Programs
- ▶ Introduce SCRM at beginning of Acquisition Lifecycle
 - Identify vulnerabilities and threats early
 - Develop mitigation strategies before impact cost, schedule and performance
 - Integrate SCRM as an iterative process that matures as program matures

A collaborative landscape exists to share best practices and lessons learned across government and industry

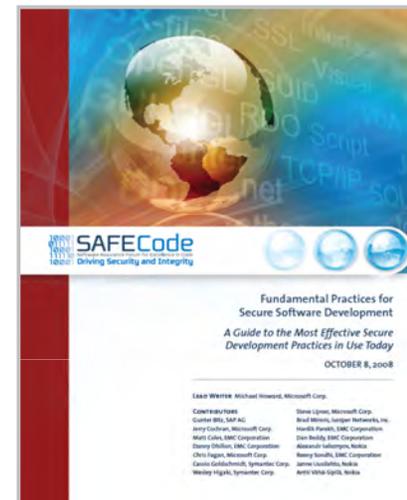
US has vital interest in the global supply chain.



Courtesy of Don Davidson, OSD TMSN ,Chief of Outreach and Standardization

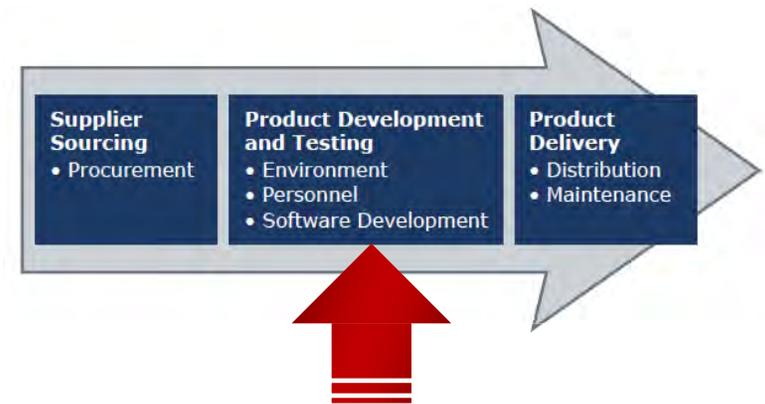
SAFECode (www.safecode.org)

- ▶ SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services
- ▶ White papers
 - Software Assurance: An Overview of Current Industry Best Practices
 - Fundamental Practices for Secure Software Development
 - Security Engineering Training: A Framework for Corporate Training Programs on the Principles of Secure Software Development
 - Framework for Software Supply Chain Integrity
 - Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain



Describing the Software Supply Chain

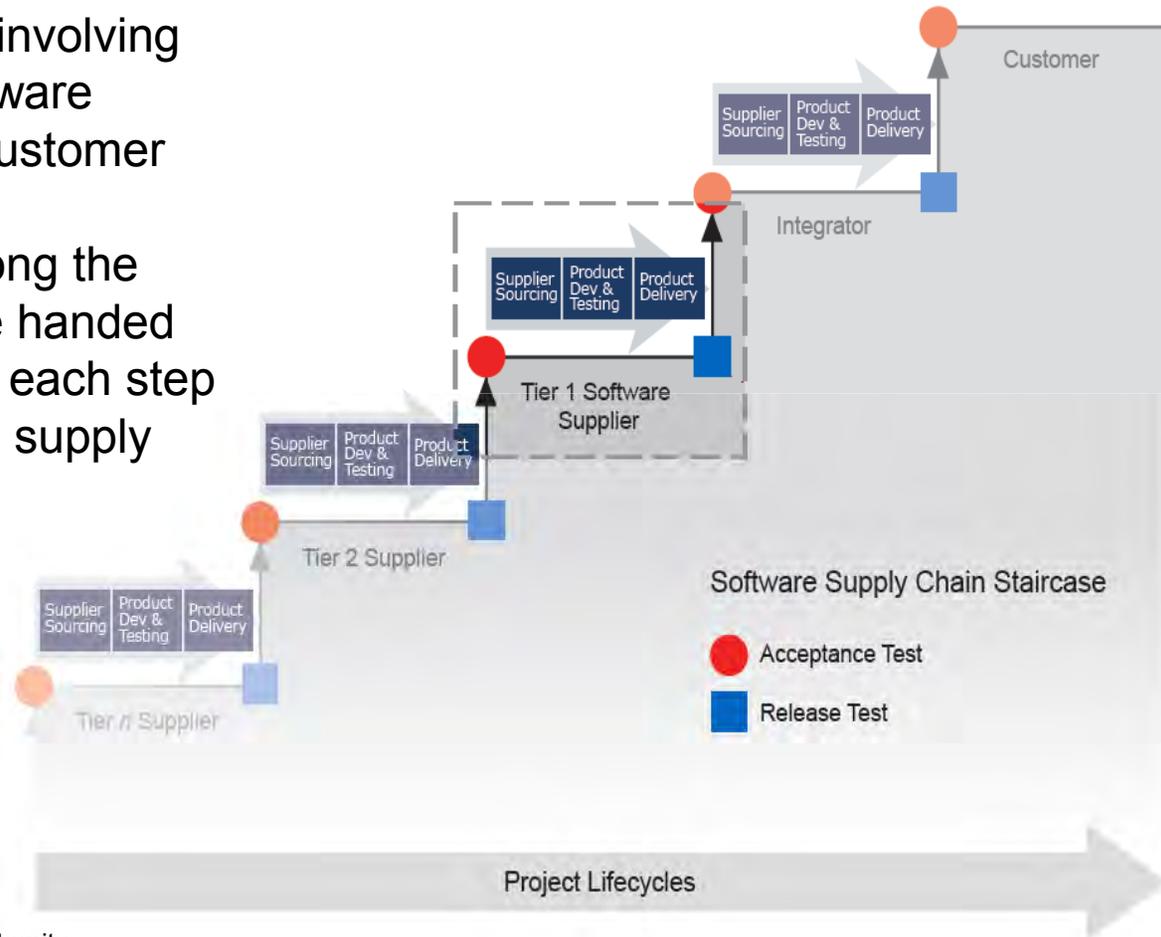
- ▶ Sophisticated IT solutions are composed of a **collection of components**
- ▶ Each component or its parts can be:
 - **Developed** by its supplier or on that supplier's behalf by their subcontractors; or
 - **Licensed** to the supplier by another vendor or obtained from Open Source repositories; or
 - **Acquired** outright by the supplier
- ▶ **Regardless of the development scenario, each software supplier in the supply chain must manage three sets of controls:**
 - 1. **Supplier Sourcing** — Select the suppliers, establish the specification for the supplier's deliverables, and receive software/hardware deliverables from the suppliers;
 - 2. **Product Development and Testing** — Build, assemble, integrate and test components and finalize for delivery; and,
 - 3. **Product Delivery** — Deliver and maintain their product components to their customer.



Source – SAFECode: Framework for Software Supply Chain Integrity

Software Supply Chain Staircase

- ▶ Figuratively, an IT solution supply chain can resemble a collection of staircases involving the successive transmission of software components from a supplier to its customer
- ▶ In this figure, components move along the “staircase” supply chain as they are handed off from one supplier to the next. At each step a supplier controls three links in the supply chain:
 1. Goods received from suppliers;
 2. Their product production; and
 3. What is delivered to their customers



Source – SAFECode: Framework for Software Supply Chain Integrity

Fundamental Software Supply Chain Integrity Controls

- ▶ Software supply chain integrity controls address the access, storage and handling of development assets throughout the supply chain – supplier sourcing, product development and testing, and product delivery.
- ▶ Some fundamental software supply chain integrity controls, derived from established security and integrity principles, include:

Control Title	Description
Chain of Custody	The confidence that each change and handoff made during the source code's lifetime is authorized, transparent and verifiable
Least Privilege Access	Personnel can access critical data with only the privileges needed to do their jobs.
Separation of Duties	Personnel cannot unilaterally change data, nor unilaterally control the development process
Tamper Resistance and Evidence	Attempts to tamper are obstructed, and when they occur they are evident and reversible.
Persistent Protection	Critical data is protected in ways that remain effective even if removed from the development location.
Compliance Management	The success of the protections can be continually and independently confirmed
Code Testing and Verification	Methods for code inspection are applied and suspicious code is detected.

Source – SAFECode: Framework for Software Supply Chain Integrity

NIST IR 7622, Piloting Supply Chain Risk Management for Federal Information Systems

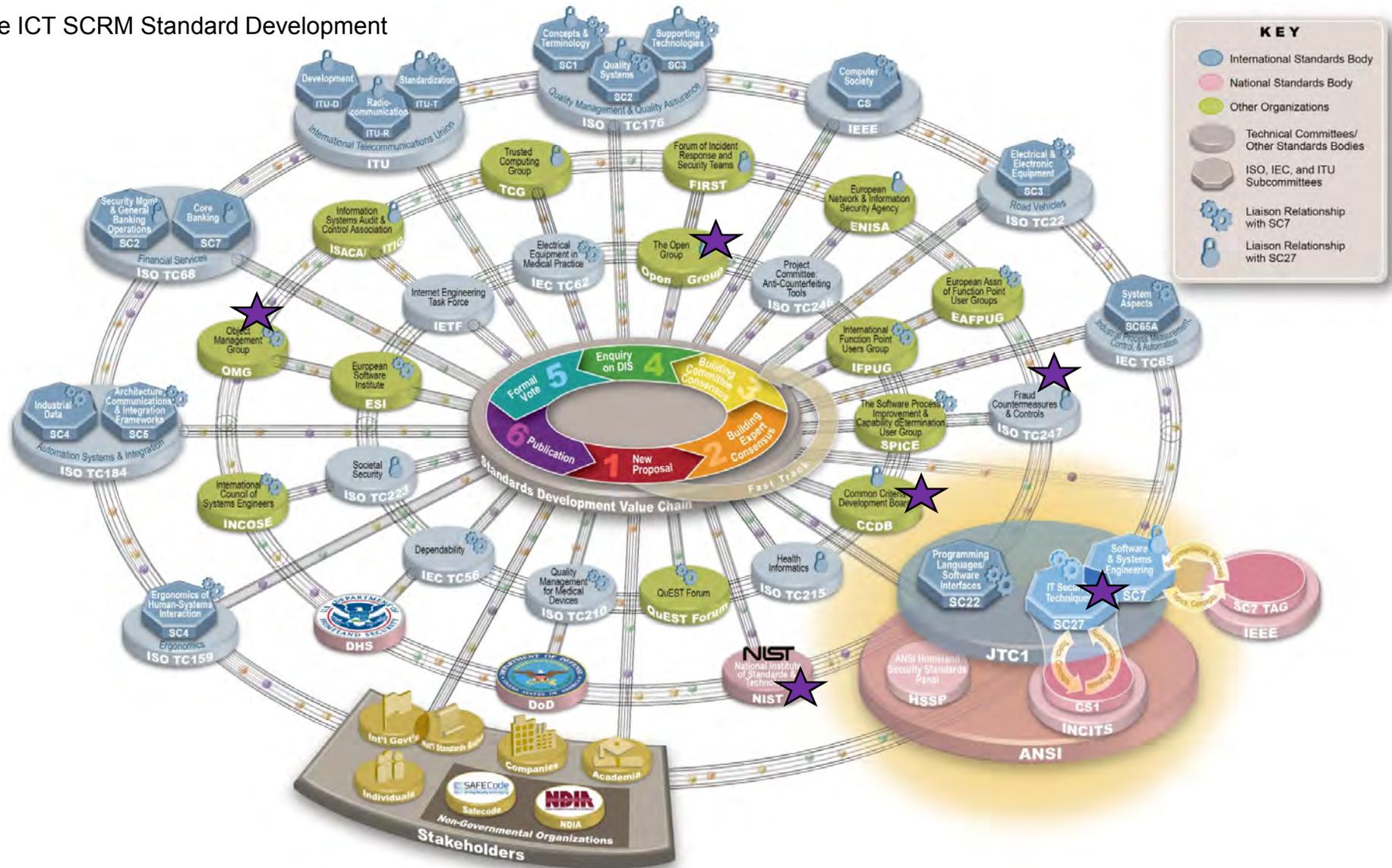
- ▶ Initially based on DoD ICT SCRM Key Practices document and developed in close collaboration with the industry
- ▶ Introduces the notion of supply chain players
 - Acquirer - For this document, the acquirer is always a government agency (including those agencies taking on the role of integrator).
 - Integrator – A third-party organization that specializes in combining products/elements of several suppliers to produce elements (information systems).
 - Supplier – Third-party organization providing individual elements. *Synonymous with vendor and manufacturer; also applies to maintenance/disposal service providers*
- ▶ Lays out pre-requisites of being able to address ICT SCRM challenge
- ▶ States specific practices that are consistent with DoD guidance and ISO frameworks
- ▶ Publication schedule:
 - 2nd draft mid-year
 - Workshop to discuss government and industry comments
 - Final by the end of 2011
 - Serve as the basis for a special publication, release date TBD

Table Of Contents

- ▶ Globalization Challenges
- ▶ Understanding The Problem
- ▶ DOD Tool Box for SCRM
- ▶ Working Towards A Solution

The ICT SCRM Standard Development Organization Landscape

★ Active ICT SCRM Standard Development



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

- ▶ Scope: This international standard covers information security in relationships between acquirers and suppliers to provide appropriate information security management for all parties. In particular, it also includes management of information security risks related to these relationships.

- ▶ The standard will be subdivided into the following parts:
 - Part 1 – Overview and Concepts
 - Part 2 – Common Requirements
 - Part 3 – Guidelines for ICT Supply Chain
 - Part 4 – Guidelines for Outsourcing

- ▶ Contributed relevant industry documents
 - **The Software Supply Chain Integrity Framework**, Software Assurance Forum for Excellence in Code (SAFECode)
 - **Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain**, Software Assurance Forum for Excellence in Code (SAFECode)
 - **Software Supply Chain Security**, Microsoft; 16 slides, was briefed by Chris Fagan, Microsoft to CS1 and ISO; Chris Fagan was a key contributor to the SAFECode documents, as well as active participant in TTPF work
 - **NIST IR 7622, Piloting Supply Chain Risk Management for Federal Information Systems**, NIST

What is the Problem and Gaps We Are Trying to Address?

Problem

- ▶ Information and Communication Technology (ICT) products are assembled, built, and transported by multiple vendors around the world before they are acquired ***without the knowledge of the acquirer***
- ▶ Abundant opportunities exist for malicious actors to tamper with and sabotage products, ultimately compromising system integrity and operations ***evidenced by multiple recently publicized incidents*** (counterfeit hardware sold to government agencies)
- ▶ Organizations acquiring hardware, software, and services are not able to understand and manage the security risks associated with the use of these products and services

Need

- ▶ Provide a common language for addressing the problem
- ▶ Provide a resource that would help acquirers ***articulate requirements*** to product and service providers and ***monitor implementation*** in a recognizable manner that is vetted internationally
 - Increase confidence in acquired products and services from security risk point of view
 - Create a common language to articulate expectations regarding security risks associated with product and service acquisition
- ▶ Provide a resource that would help product and service providers ***demonstrate responsible practices, regardless of where they are located***

The Open Group

Trusted Technology Provider Framework (TTPF)

Purpose

Identify and gain consensus on common processes, techniques, methods, product and system testing procedures, and language to describe and guide product development and supply chain management practices that can mitigate vulnerabilities which could lead to exploitation and malicious threats to product integrity.

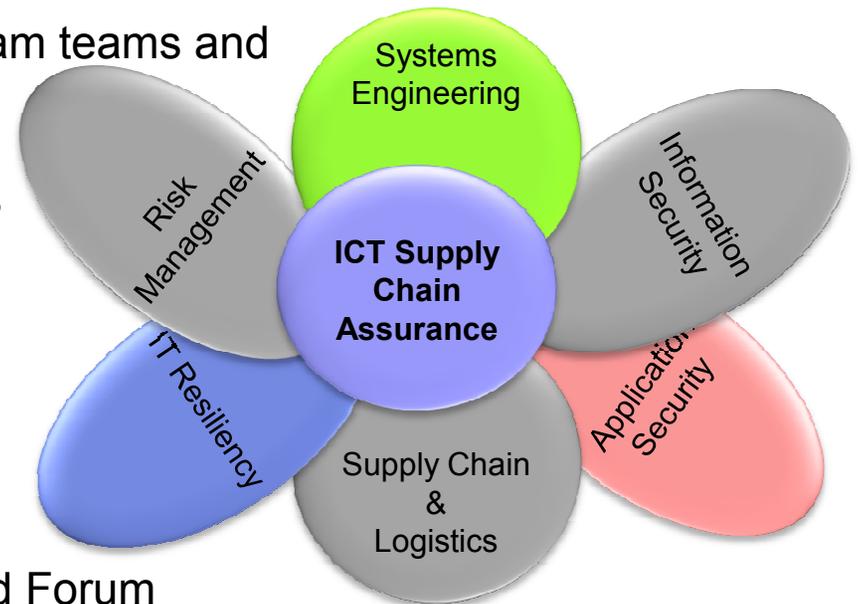
Objectives

- Identify product assurance practices that should be expected from all commercial technology vendors based on the baseline best practices of leading trusted commercial technology suppliers
- Help establish expectations for global government and commercial customers when seeking to identify a trusted technology supplier
- Leverage existing globally recognized information assurance practices and standards
- Share with commercial technology consumers secure manufacturing and trustworthy technology supplier best practices
- Harmonize language used to describe best practices

Source: Source: September 28, 2010 SwA Forum, DoD Trusted Defense Systems, Ms. Kristen Baldwin, DDR&E/Systems Engineering

What's next?

- ▶ Continued collaboration to:
 - Reach and enable program teams
 - Reach and enable executives
 - Develop and promote resources for us by program teams and executives
- ▶ Participation in international standardization efforts
 - SC7 TAG intersections through your SC7 TAG
 - CS1/SC27
 - IEEE representative to the SC7 TAG
 - SC22
- ▶ Participation through the SwA Working Groups and Forum
- ▶ Participation through the newly formed NDIA Cyber Division
- ▶ Stay Tuned ...



Michele Moss

Lead Associate

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
8283 Greensboro Dr
McLean, VA 22102
703-377-1254
moss_michele@bah.com