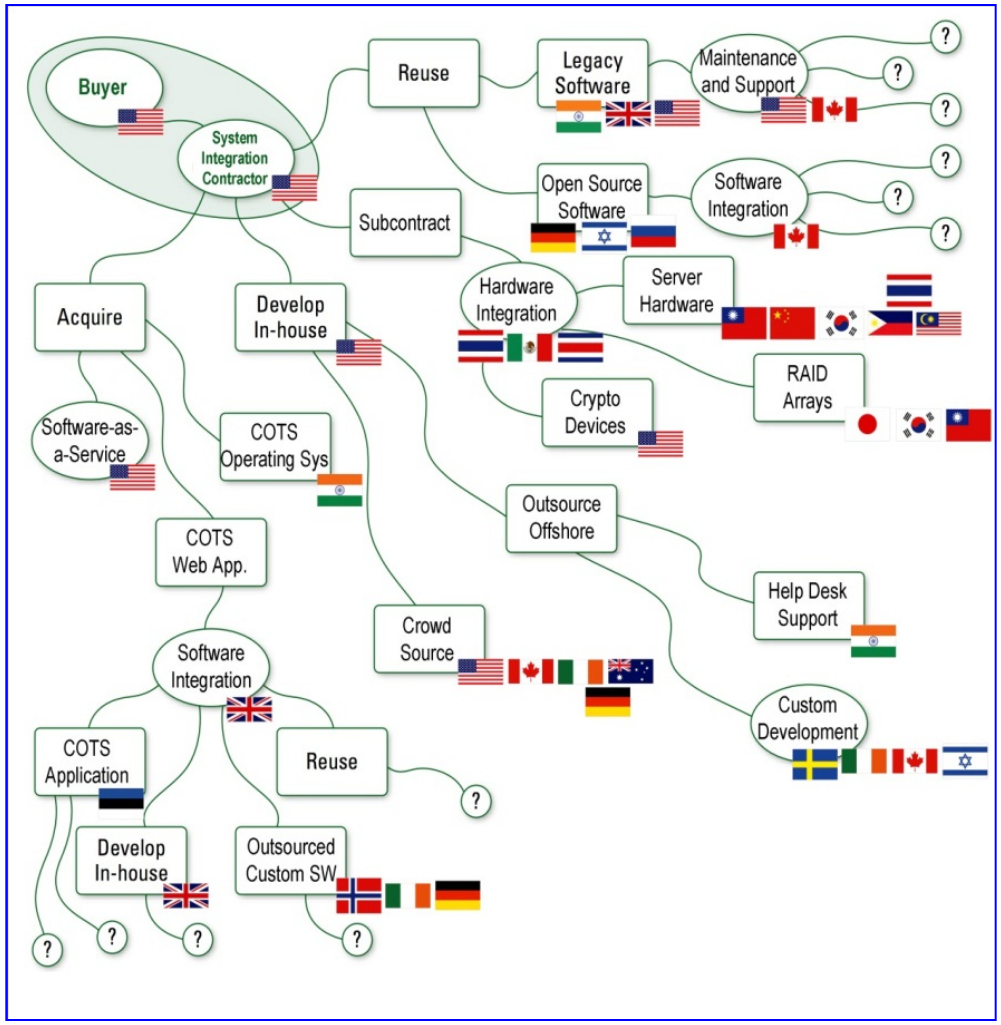
Do You Have The Right Practices In Your Cyber Supply Chain Tool Box?

NDIA Systems Engineering Conference
October 29, 2014

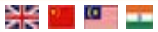
Today's Reality Is Deep & Complex Global ICT Supply Chains



IT and Communications products are assembled, built, and transported by multiple vendors around the world.

Software contributions include reusable libraries, custom code, commercial products, open source

Simplistic Representation of Component List for a Dell Laptop

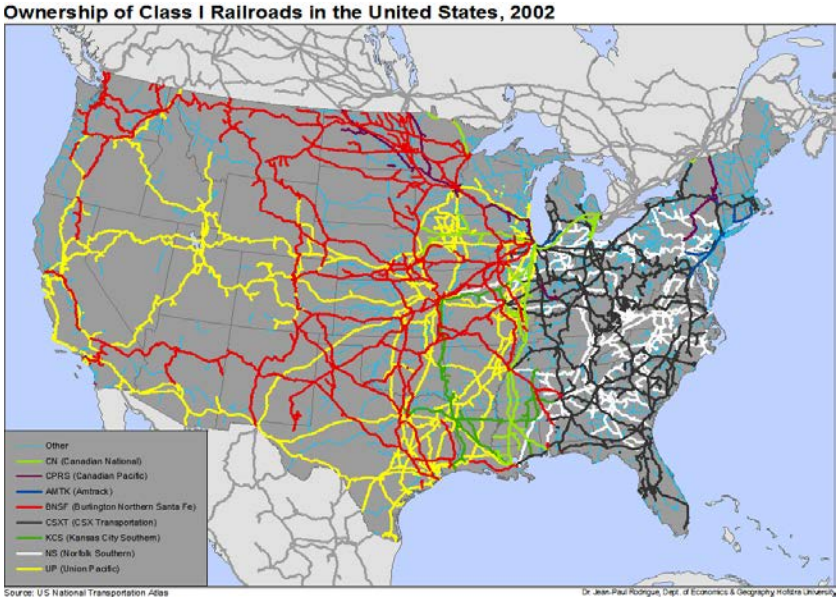
Component		Supplier or Potential Suppliers
Intel Microprocessor		US-owned factory in the Philippines, Costa Rica, Malaysia, or China *(Intel)*
Memory		South Korea *(Samsung)*, Taiwan *(Nanya)*, Germany *(Infineon)*, or Japan *(Elpida)*
Graphics Card		China *(Foxconn)*, or Taiwanese-owned factory in China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

From *The World Is Flat by Thomas Friedman*
Dell Inspiron 600m Notebook: Key Components and Suppliers

Supply Chain: PERSPECTIVES

Supply Chain SECURITY

- Nodes of storage & throughput
- Lines of transport (& communication)



Courtesy of Don Davidson, DOD

Supply Chain RESILIENCE

- Multi-sources
- Multi-nodes
- Multi-routes

Supply Chain: PERSPECTIVES

Product INTEGRITY

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

Courtesy of Don Davidson, DOD

What is the 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***

- Challenges range from poor acquirer practices to lack of transparency into the supply chain
  - **Substantial number of organizations or people can "touch" an ICT product without being identified**
  - No standardized methodology or lexicon exists for managing ICT supply chain risks
  - Poor ICT products and services acquisition practices contribute to acquirers' lack of understanding what is in their supply chain
  - Counterfeit hardware and software proliferate
  - Acquirers do not have a framework to help enforce security and assurance compliance for vendors

Why Standards?

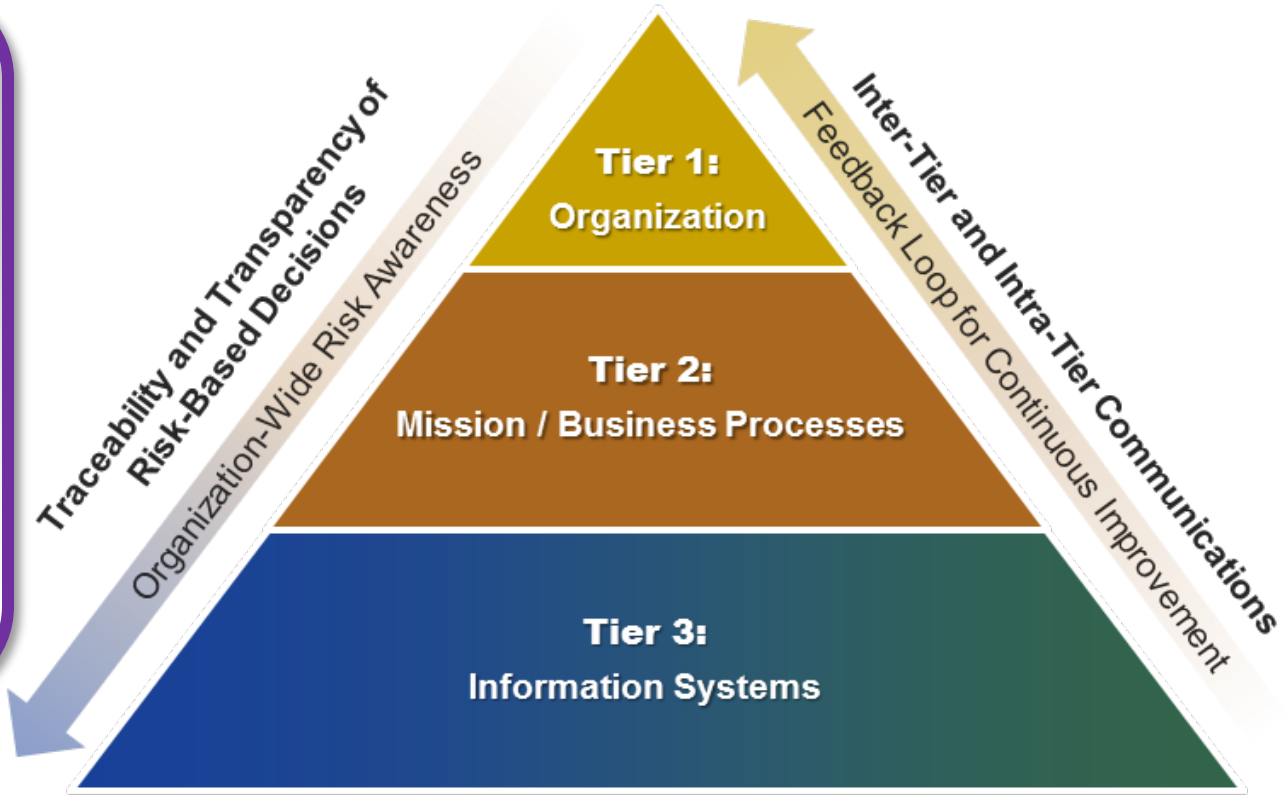
- **Standards are a common language used to communicate expected levels of performance for products and services**
- Countries use international **standards compliance as a trade barrier** and differentiator for their companies
- Standards are Essential to Global Economy
  - Ensuring **interoperability** among trade partners
  - Facilitating increased efficiencies in the **global economy**
  - Making the development, manufacturing, and supply of products and services more efficient, safer and cleaner
  - Providing governments with a technical base for health, safety and environmental legislation
  - **Safeguarding consumers**, and users in general, of products and services - as well as to make their lives simpler

Essential Security and Foundational Practices

- **Management Systems:** ISO 9001 - Quality, ISO 27001 – Information Security, ISO 20000 – IT Service Management, ISO 28000 – Supply Chain Resiliency
- **Security Controls**: ISO/IEC 27002, NIST 800-53
- **Lifecycle Processes:** ISO/IEEE 15288 - Systems, ISO/IEEE 12207 – Software
- **Risk Management**: ISO 31000 - overall, ISO/IEC 27005 - security, and ISO/IEC 16085 - systems
- **Industry Best Practices:** CMMI, Assurance Process Reference Model, Resiliency Management Model (RMM), COBIT, ITIL, PMBOK

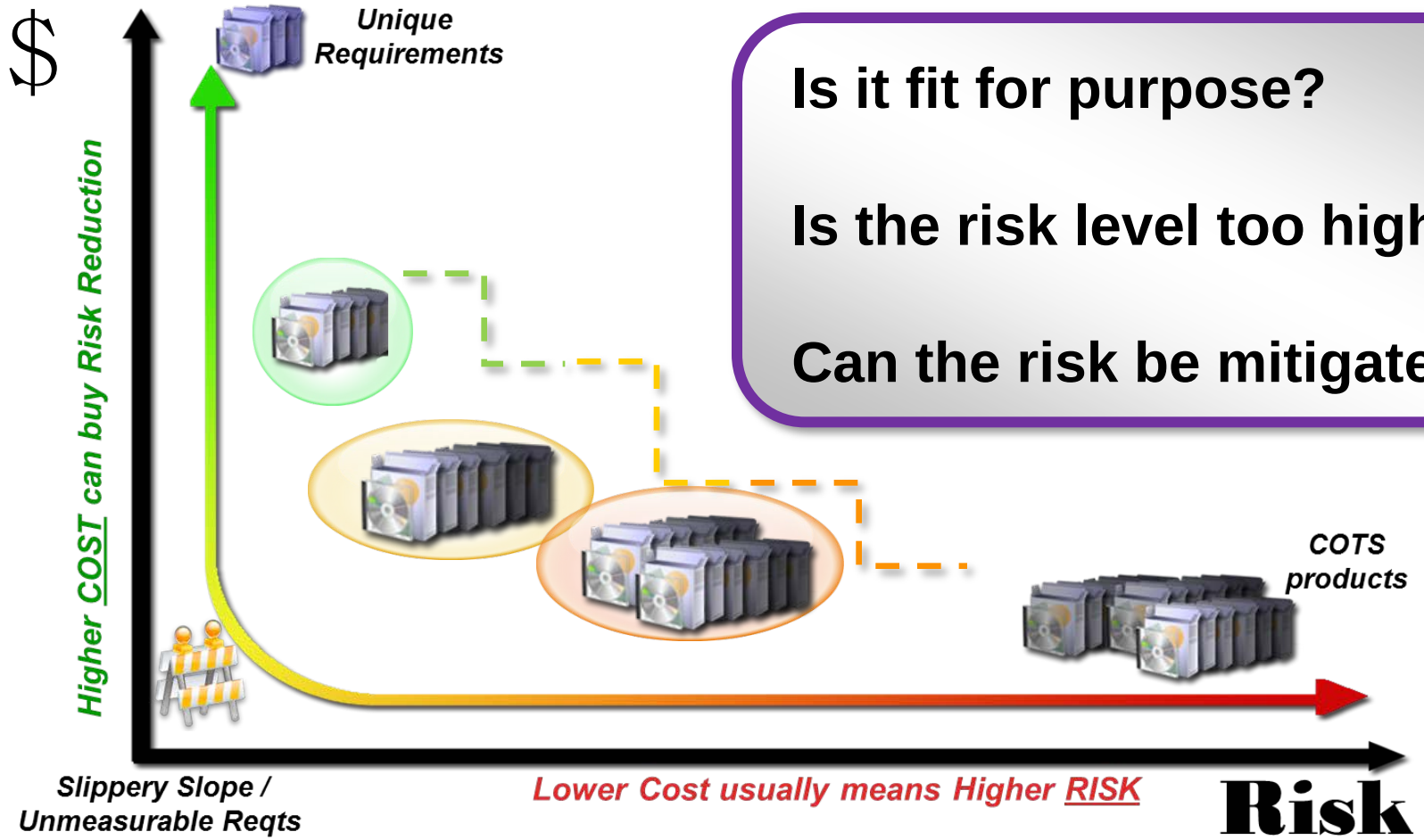
Addressing Product Integrity Requires Standards for Multiple Tiers of Enterprise Risk Management

Acquirers need standards as a way 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.



The NIST SP 800-39* Model for Information Security Risk

Success Involves Selecting Multiple Standards To Address Unique Program Risks



Is it fit for purpose?

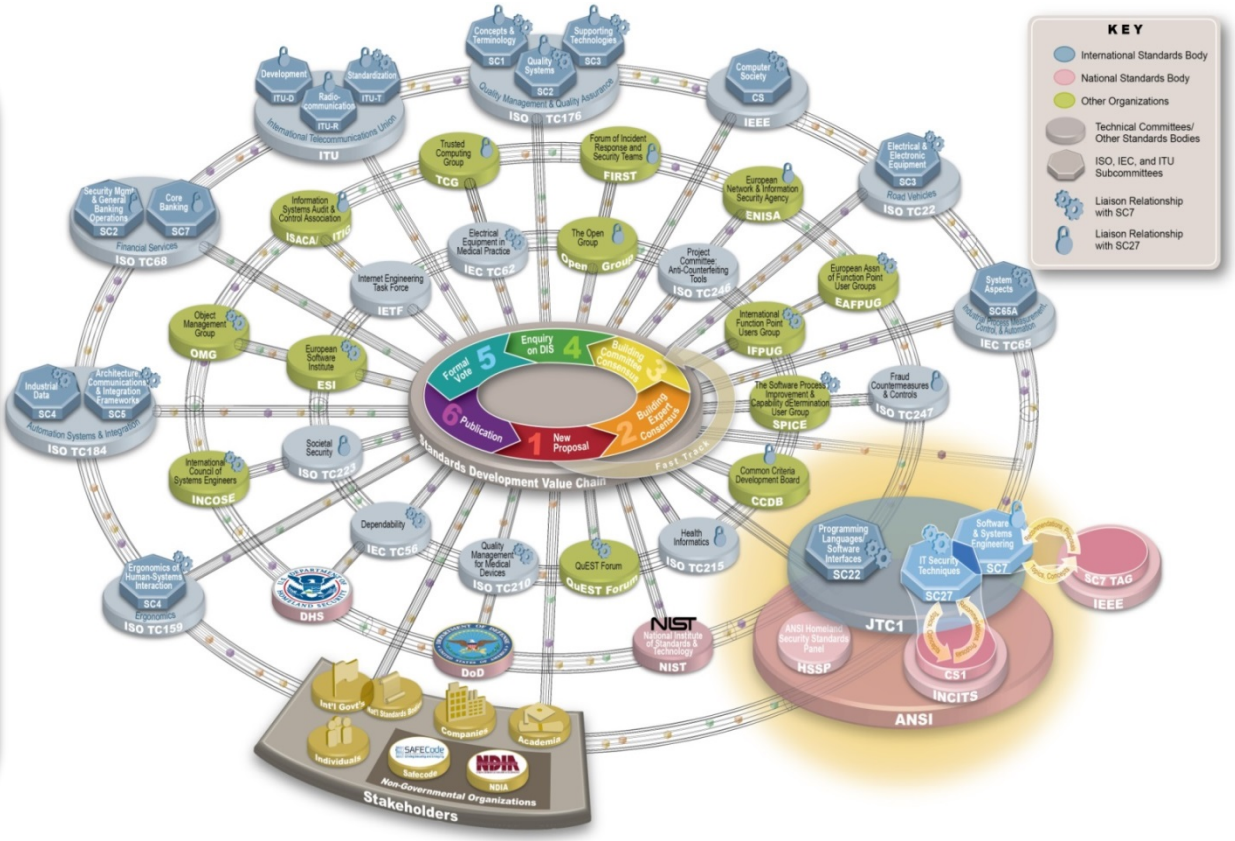
Is the risk level too high?

Can the risk be mitigated?

Graphic courtesy of Don Davidson

Where Are New Standards Being Developed?

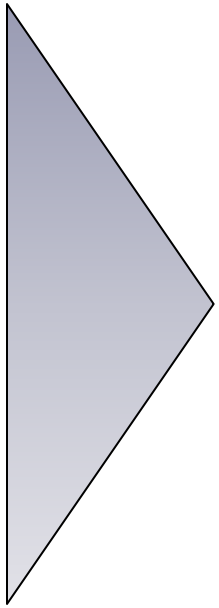
OMB 119A
federal agencies are to "use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical."



Courtesy of Department of Defense

The Definition Of Security In The Context Of Systems Engineering Is Evolving

- 15288:2008
  - all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of a system



- Draft 15288 DIS as of May 2014
  - protection against intentional subversion or forced failure. A composite of four attributes – confidentiality, integrity, availability, and accountability – plus aspects of a fifth, usability, all of which have the related issue of their assurance.

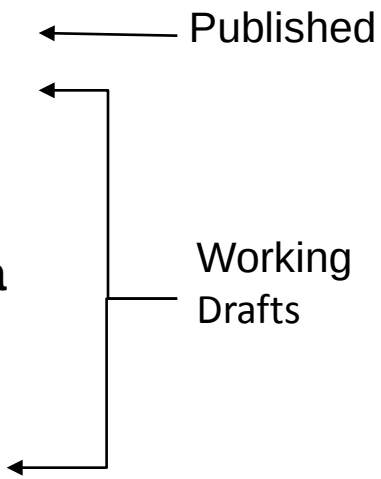
Security Functionality And Enhancements To ISO/IEC 15288 – Highlights

- Consideration of security practices of **suppliers**
- Consideration of security of **outsourced infrastructure**
- Consideration of **reusable code libraries**
- Assurance implications of the design in the context of the **planned operational environment**
- Configuration management **across tiers of the supply chain**
- Architectural considerations that the system will be **compromised intentionally or unintentionally via a threat agent**
- **Secure design principles**
- Consideration of **anti-counterfeit, anti-tamper**, system and software and the achievement of critical quality characteristics
- Predictability in the intended environment
- Consideration of preventing **expired, non-reusable, or inadequate elements from getting back into the supply chain**

ISO/IEC 27034 - Application Security

Scope: specify an application security life cycle, incorporating the security activities and controls for use as part of an application life cycle, covering applications developed through internal development, external acquisition, outsourcing/offshoring, or a hybrid of these approaches

PART 1 – Overview and concepts
PART 2 – Organization normative framework
PART 3 – Application security management process
PART 4 – Application security validation
PART 5 – Protocols and application security control data structure
PART 6 – Security guidance for specific applications
Part 7 - Application Security Control Predictability



Adapted from Jed Pickel, Microsoft

ISO/IEC TR 24772: Programming Language Vulnerabilities

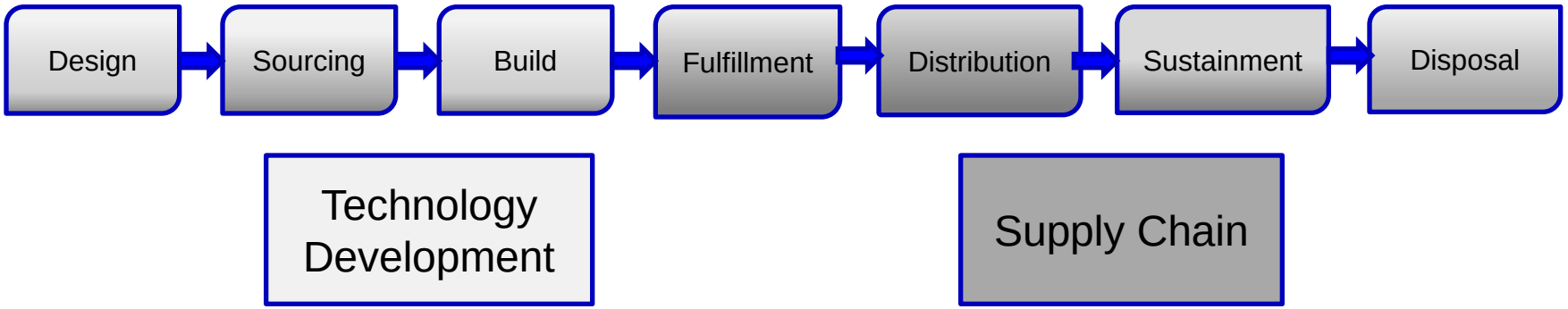
- Targets building software that is inherently less vulnerable through improving the programming languages, or, at least, improve the usage of them in coding
- A catalog of 60+ issues that arise in coding when using any language and how those issues may lead to security and safety vulnerabilities
- Each discussion includes
  - Description of the mechanism of failure
  - Recommendations for programmers: How to avoid or mitigate the problem.
  - Recommendations for standardizers: How to improve programming language specifications.

http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

O-TTPS: Mitigating Maliciously Tainted and Counterfeit Products

- The Open Trusted Technology Provider Standard (O-TTPS) released in April, 2013 – set of requirements for organizational best practices

- Apply across product life cycle. Some highly correlated to threats of maliciously tainted and counterfeit products - others more foundational but considered essential.



Source: Sally Long, OTTF Forum Director, The Open Group
OTTF Presentation Software & Supply Chain Assurance Workshop - December 17, 2013

SAE International, formerly the Society of Automotive Engineers

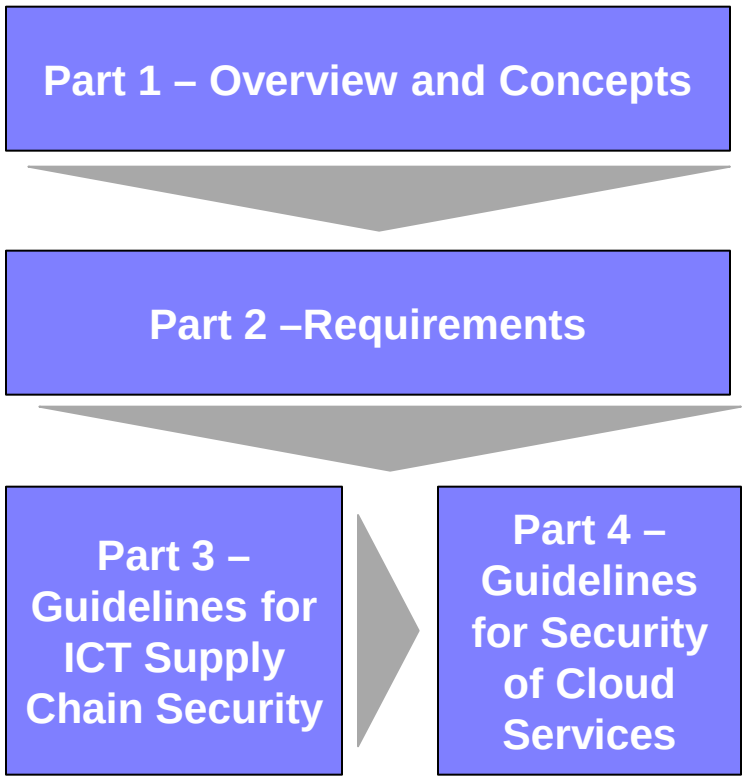
- **SAE AS5553 Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition**
- SAE AS6081 Counterfeit Electronic Parts Avoidance – Distributors
- SAE AS6171 Test Methods Standard; Counterfeit Electronic Parts
- SAE ARP6178 Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors
- SAE AS6462 AS5553 Verification Criteria

27002:2013 New Controls A “Quick List”

- 6.1.5- Information security in project management
- 14.2.1- **Secure development policy**
- 14.2.5- **Secure system engineering principles**
- 14.2.6- **Secure development environment**
- 14.2.8- **System security testing**
- 15.1.1- **Information security policy for supplier relationships**
- 15.1.2- **Addressing security within supplier agreements**
- 15.1.3- **Information and communication technology supply chain**
- 16.1.4- Assessment of and decision on information security events
- 16.1.5- Response to information security incidents
- 17.1.1- Planning information security continuity
- 17.1.2- Implementing information security continuity
- 17.2.1- Availability of information processing facilities

ISO/IEC 27036 – Supplier Relationships

General overview



Requirements for information security activities for any supplier relationship to acquire any products and services

Part 2 requirements + Part 3 guidance to manage ICT supply chain security risks for ICT products and services

Part 2 requirements + Part 3 guidance + Part 4 guidelines to structure cloud security services risks

Courtesy of Nadya Bartol, UTC

New standards for use with the Common Criteria

- Study Period Topics
  - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408
  - High-assurance evaluation under ISO/IEC 15408/18045 high-assurance
  - Competence of individuals performing evaluation, testing and certification
  - Operational test guideline of cryptographic module in environment

- Standards Under development/revision
  - ISO/IEC 1st WD 20004-1 — Refining Software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045 — Part 1: Using publicly available information security resources
  - ISO/IEC 1st WD 20004-2 — Refining Software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045 — Part 2: CWE and CAPEC based software penetration testing
  - ISO/IEC 2nd WD 19249 — Catalogue of architectural and design principles for secure products, systems, and applications

Draft NIST SP 800-161Supply Chain Risk Management Practices for Federal Information Systems and Organizations

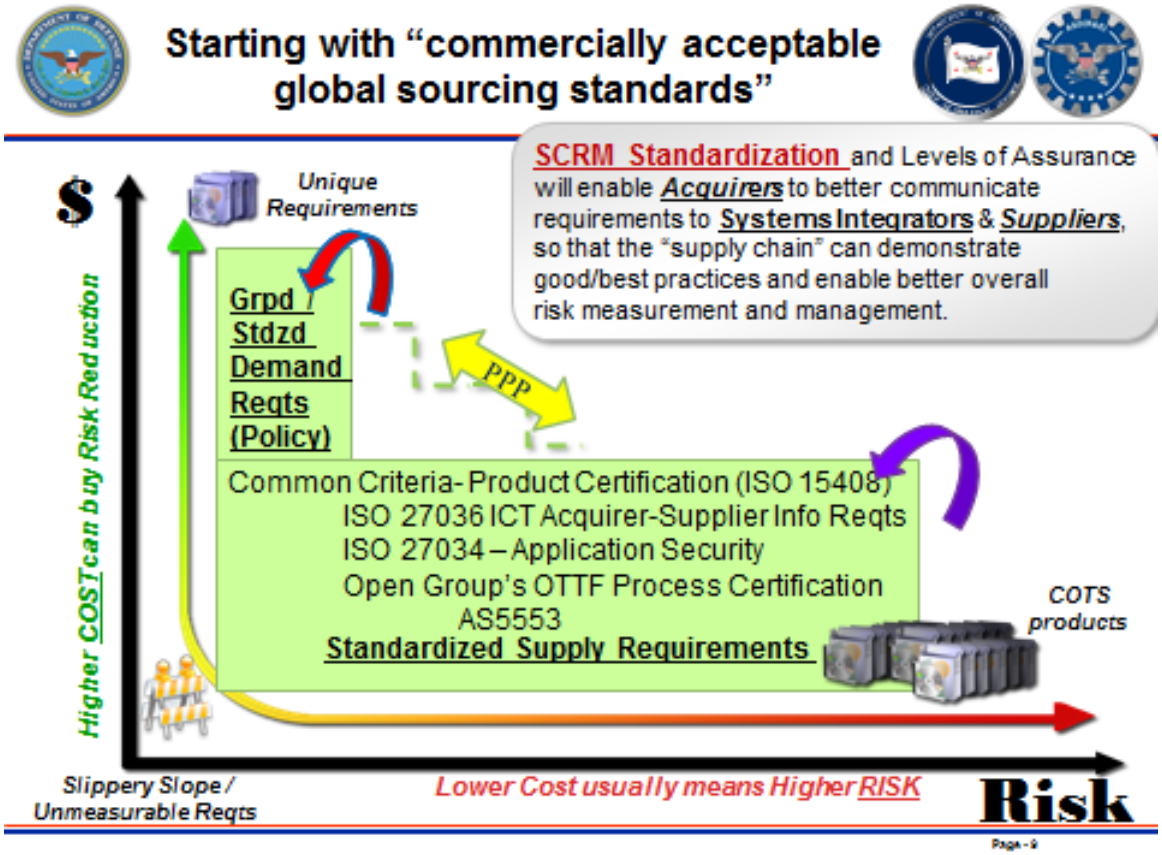
- Provides **guidance to federal agencies** on selecting and implementing mitigating processes and controls at all levels in their organizations to help manage risks to or through ICT supply chains for systems categorized as **HIGH** according to Federal Information Processing Standard (FIPS) 199, *Standards for Security* 367 *Categorization of Federal Information and Information Systems*

- Applies the **multi-tiered risk management** approach of NIST SP 800-39, 355 *Managing Information Security Risk: Organization, Mission, and Information System View*

- Refines and expands NIST SP 800-53 Rev4 controls, adds new controls that specifically address ICT SCRM, and offers SCRM-specific supplemental guidance where appropriate

Extracted from http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf

Success Involves Selecting Multiple Standards To Address Program Risks



NIST Cyber Framework

- Promotes private sector development of conformity assessments
- **SCRM is called out as an emerging discipline** characterized by diverse perspectives, disparate bodies of knowledge, and fragmented standards and best practices

Industry efforts continue to mature the SCRM Discipline

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

www.safecode.org

OWASP
The Open Web Application Security Project
http://www.owasp.org

www.owasp.org

http://bsimm.com/

www.microsoft.com/sdl

Homeland Security

Build Security In
Setting a higher standard for software assurance
Sponsored by DHS National Cyber Security Division

BuildSecurityIn.us-cert.gov

CERT | Software Engineering Institute | Carnegie Mellon

http://www.cert.org/secure-coding/

QUESTIONS?

Contact Information

Michele Moss
Lead Associate

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
8283 Greensboro Drive
Mclean, VA 22102
Tel (703) 377-1254
moss_michele@bah.com