NIST

National Institute of Standards and Technology
U.S. Department of Commerce

Information and Communications Technology Supply Chain Risk Management (ICT SCRM)

Jon Boyens
Computer Security Division
IT Laboratory

June 24, 2015

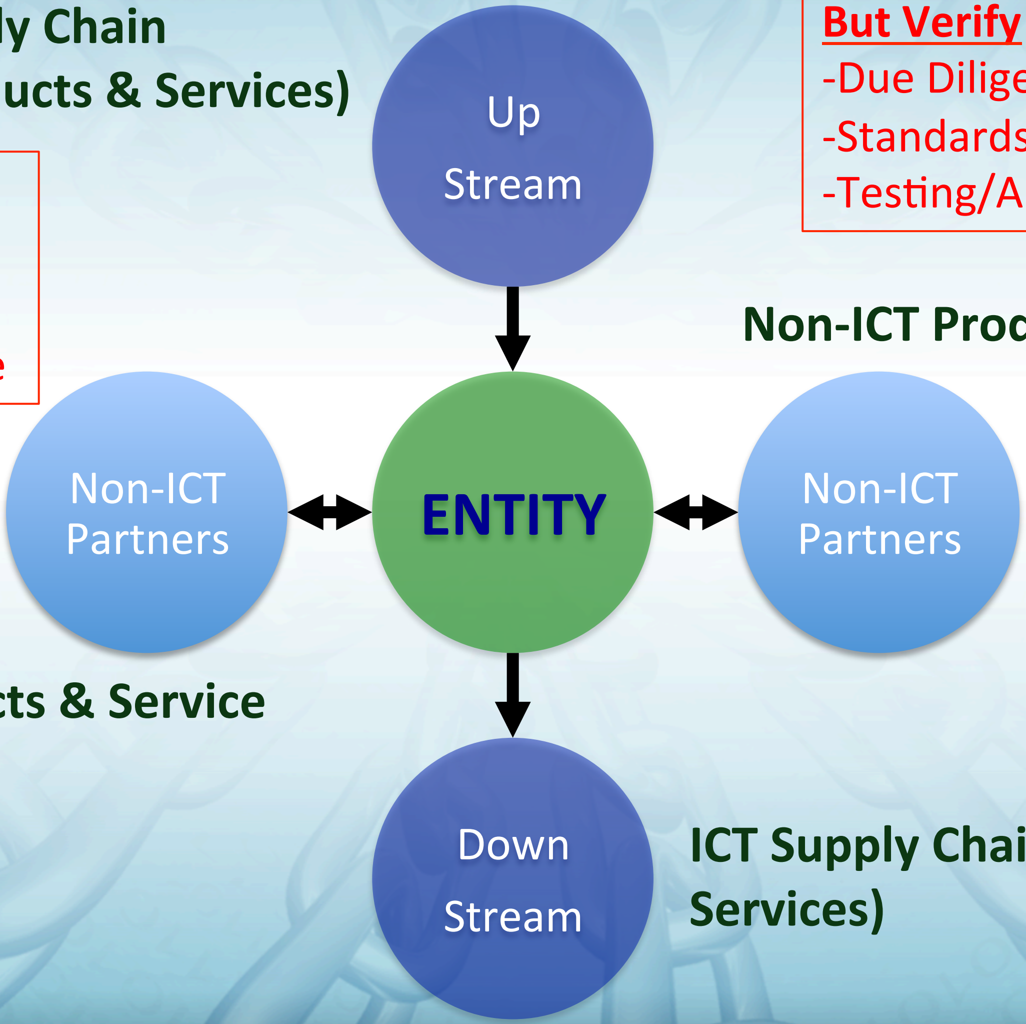
Agenda

- What is ICT SCRM and what is the Problem?
- ICT SCRM Landscape and Drivers
- NIST Work
- Current and Future Work

What is the Problem?

What is ICT SCRM?

ICT and Non-ICT External Dependencies



ICT Supply Chain
(ICT Products & Services)

TRUST
-Organization
-Process
-Products/Service

But Verify
-Due Diligence
-Standards/Conformity
-Testing/Audits

Non-ICT Products & Service

Non-ICT Products & Service

ICT Supply Chain (ICT Products & Services)

ICT SCRM Problem Definition

ICT

- Growing sophistication of ICT
- Number and scale of information systems
- Government's increasing reliance on COTS

Supply Chain

- Speed and scale of globalization
- Complex supply chain (logically long and geographically diverse)

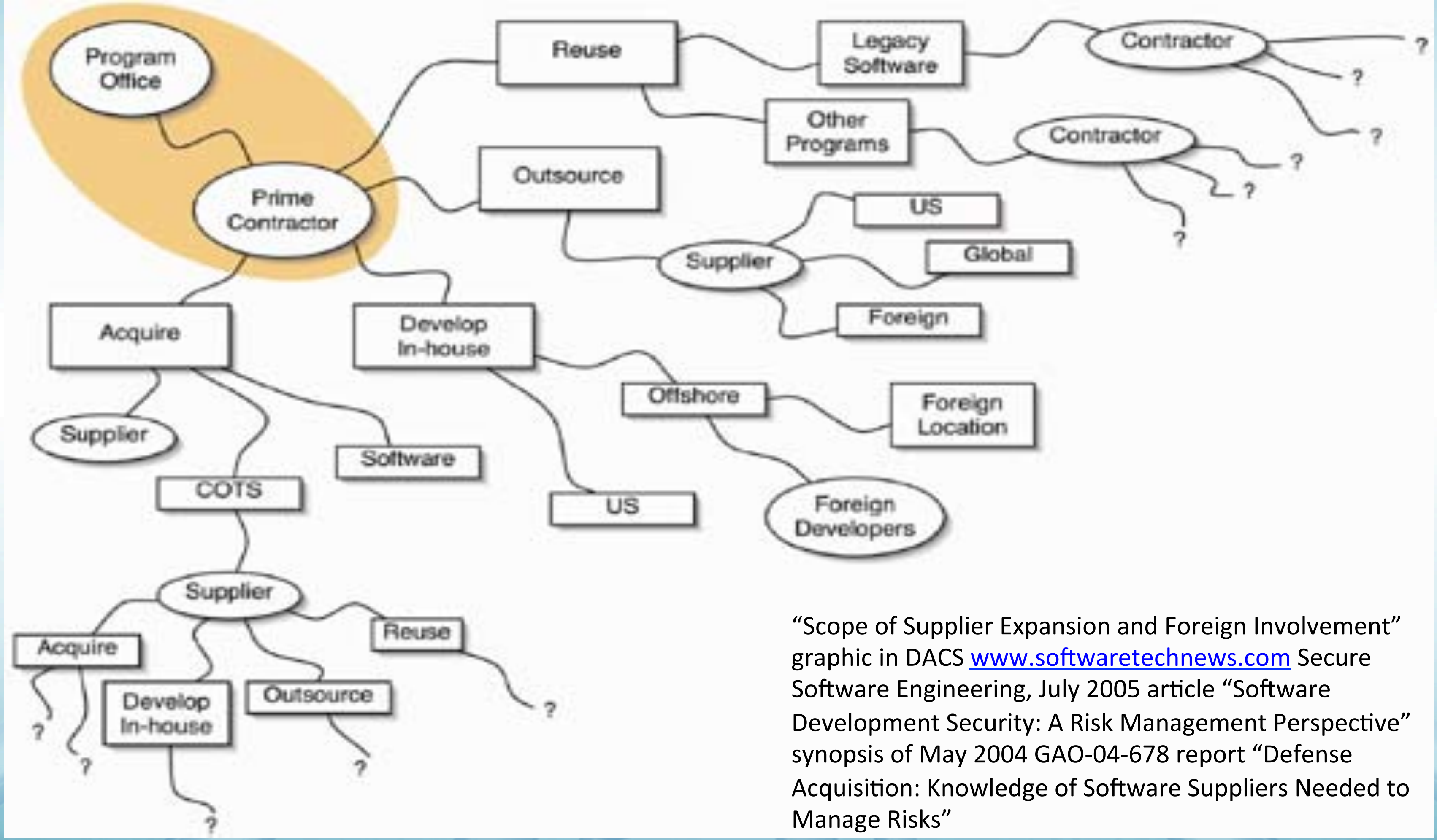
Risk

- Significant increase in the number of entities who 'touch' products and services
- Natural disasters, poor product/service quality and poor security practices

Manage ment

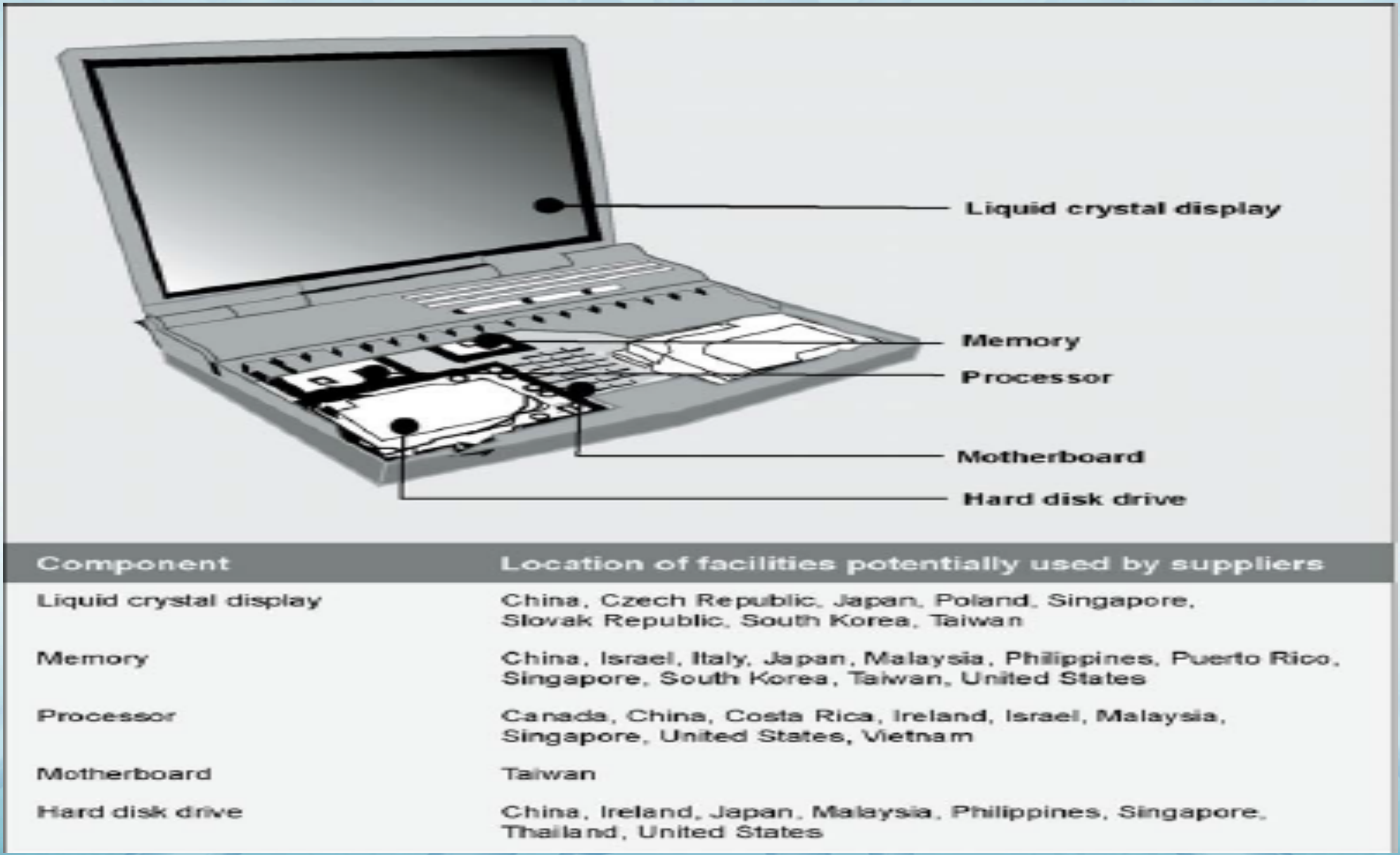
- Lack of *visibility* and *understanding*: how technology is developed, integrated and deployed and practices to assure security.
- A lack of *control* of the decisions impacting the inherited risks and ability to effectively mitigate those risks.

Focus Areas: SDLC/Internal/External



"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"

Global Supply Chain



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

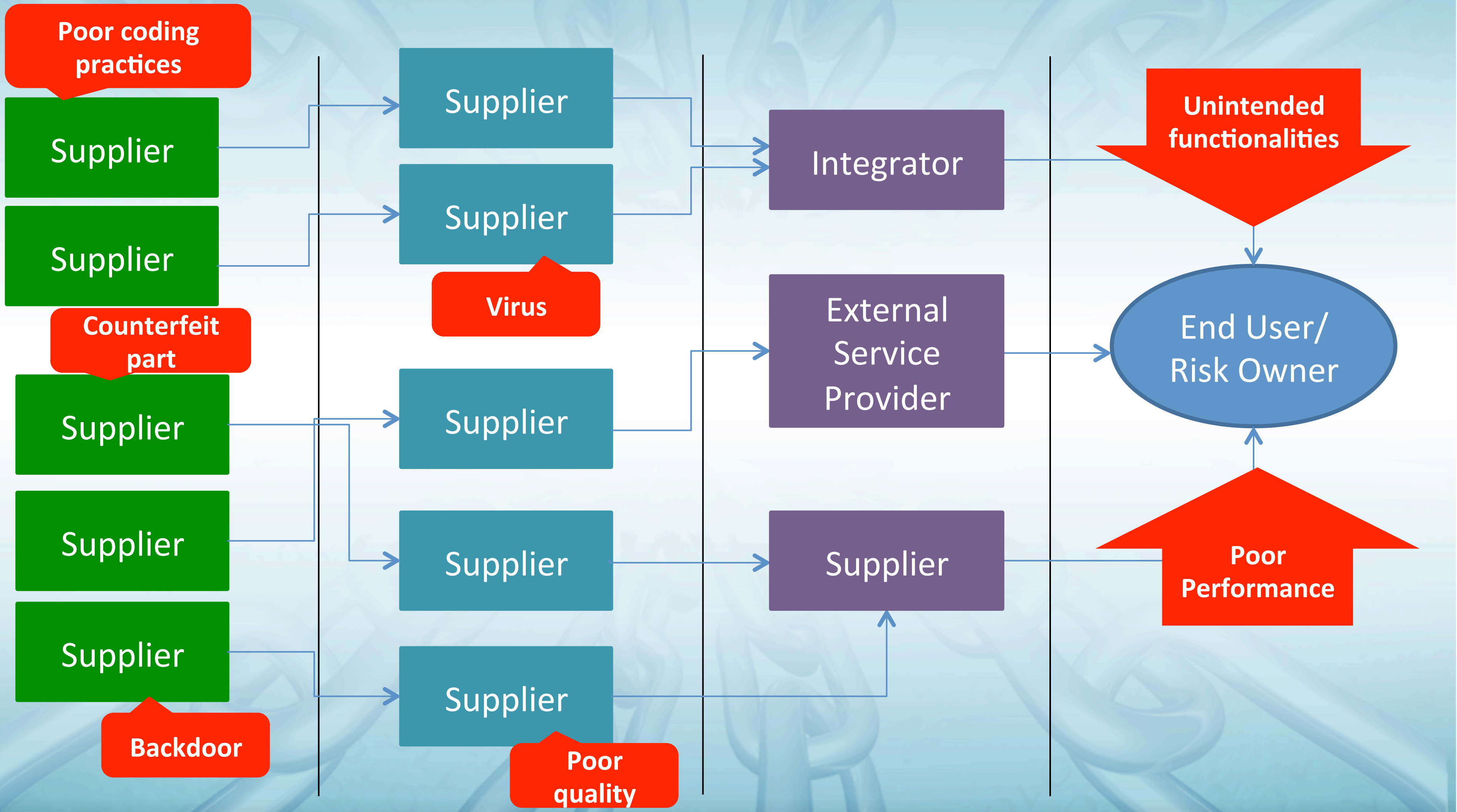
From *The World Is Flat by Thomas Friedman*

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 *(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)*

Source: Booz Allen Hamilton and DoD

Counterfeits, Malware and Poor Practices

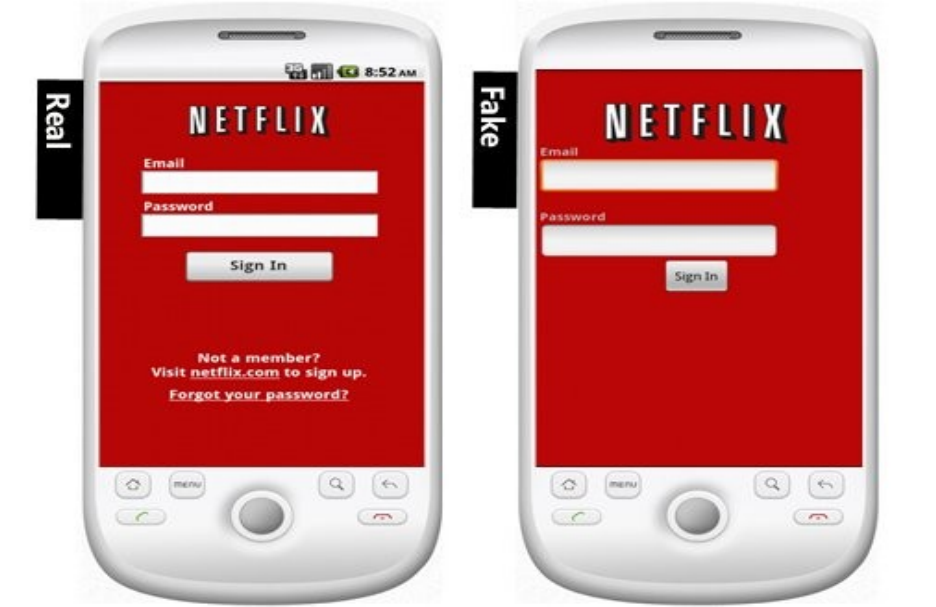


The Problem

- Counterfeit products
- Malware that is inserted into software or hardware (by various means)
- Hardware that is delivered with malware installed on it already
- Vulnerabilities in software applications and networks within the supply chain
- Poor manufacturing and development practices

Fake Apps on Mobile Devices

- http://www.networkworld.com/article/2174903/smb/pre-installed-malware-turns-up-on-new-phones.html
- http://us.norton.com/fake-android-apps/article



Not a member?
Visit netflix.com to sign up.
Forgot your password?

Example of Supply Chain Threats: Counterfeits

- Integrated circuits:
  - In 2010, a Florida company (Vision Tech) sold 60,000 counterfeit integrated circuits that went into DOD missile programs, DHS radiation detectors and DOT high speed trains.
  - Situations where failures in IT systems can be catastrophic.

    **(Hsu, Spencer, Washington Post, September 14, 2010)*
- Routers:
  - Between 2003-2005, eGlobe Solutions Inc. sold $788,000 of counterfeit equipment, primarily routers.
  - Sold to: DoD, GSA, defense contractors, power companies
  - These routers power U.S. Government and critical infrastructure networks all over the world.

    **(U.S. Attorney's Office Press Release on Indictment, November 2006)*

Example of Supply Chain Threats: Natural Disasters

- 2011 earthquake and tsunami in Japan
  - Major supplier to China, S. Korea, Taiwan, elsewhere
  - 25% world decline in chips
  - 75% world decline in the chemicals to make chips

    **(Yoneyama, Hidetaka, "The Lessons of the Great Tohoku Earthquake and Its Effects on Japan's Economy," Fujitsu Research Institute, April 8, 2011.)*

- 2011 Floods in Thailand
  - 2nd largest producer of hard-drives
  - 30% decrease in manufacturing
  - ~1 year to restore production

    **(Zhang, Fang, "Thai Floods Continue to Impact Hard Drive Manufacturing," Applied Market Intelligence, February 12, 2012)*

Example of Supply Chain Threats: Network Communications

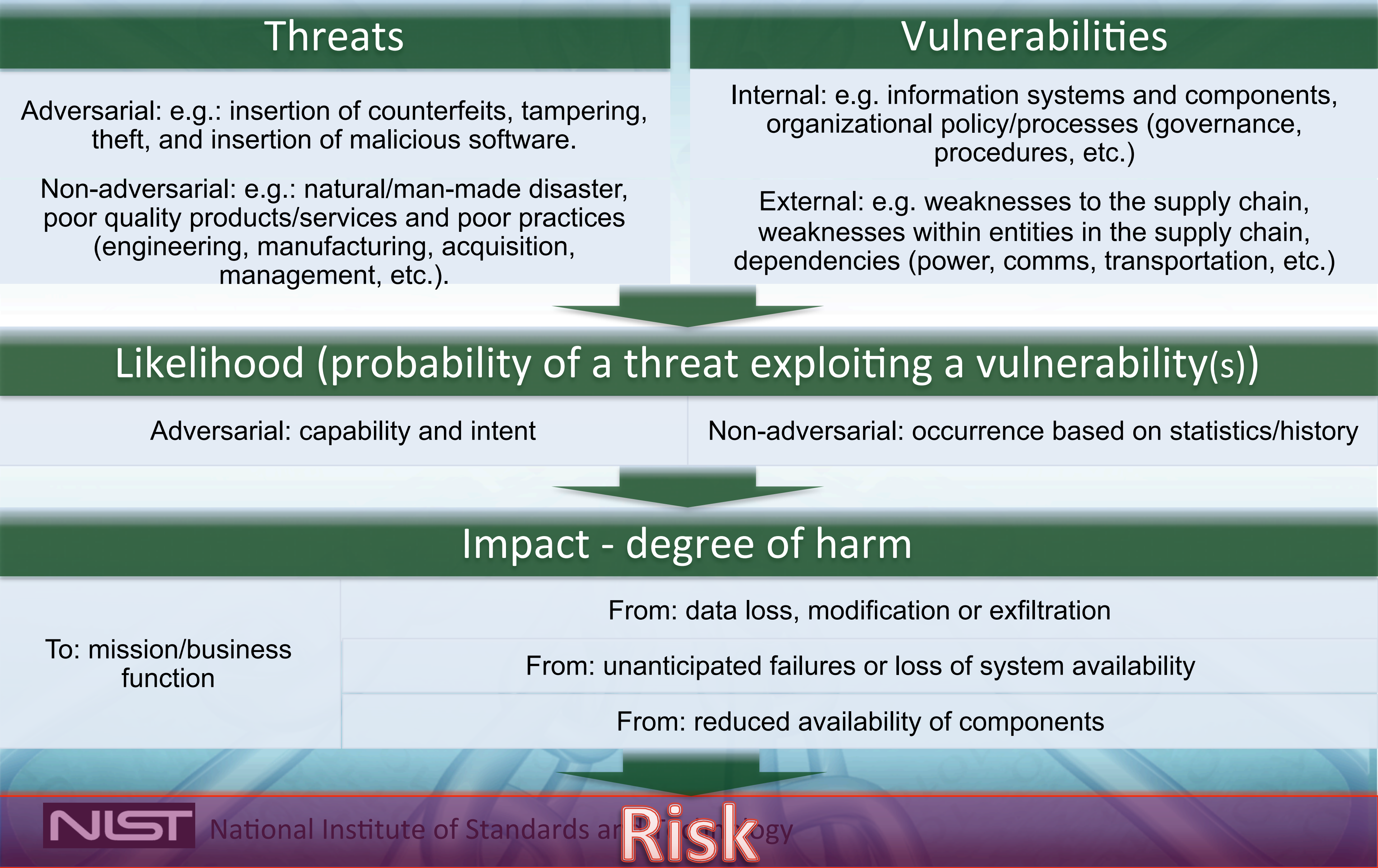
Symantec's 2013 Internet Security Threat Report

- Attacks against *GOVERNMENT*
  - Down: *25%* in 2011 to *12%* in 2012
- Attacks against *MANUFACTURERS*, largely SMEs
  - Up: *15%* in 2011 to *24%* in 2012

Mandiant 2013 Threat Report

- Outside In: Attackers are increasingly using outsourced service providers as a means to gain access to their targets.

ICT Supply Chain Risk Defined



Threats

Adversarial: e.g.: insertion of counterfeits, tampering, theft, and insertion of malicious software.

Non-adversarial: e.g.: natural/man-made disaster, poor quality products/services and poor practices (engineering, manufacturing, acquisition, management, etc.).

Vulnerabilities

Internal: e.g. information systems and components, organizational policy/processes (governance, procedures, etc.)

External: e.g. weaknesses to the supply chain, weaknesses within entities in the supply chain, dependencies (power, comms, transportation, etc.)

Likelihood (probability of a threat exploiting a vulnerability(s))

Adversarial: capability and intent

Non-adversarial: occurrence based on statistics/history

Impact - degree of harm

To: mission/business function

From: data loss, modification or exfiltration

From: unanticipated failures or loss of system availability

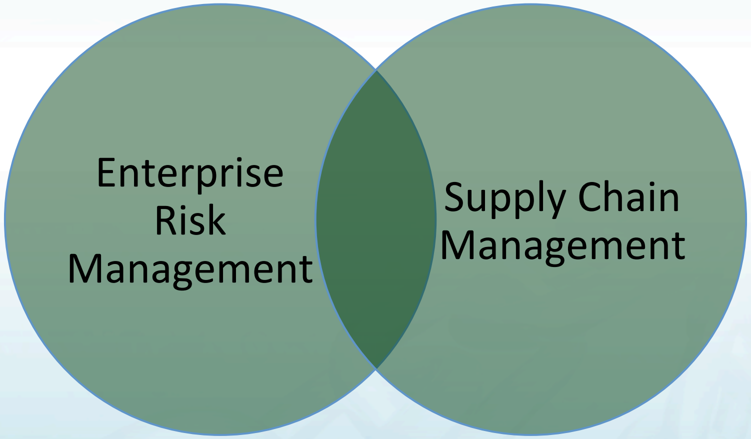
From: reduced availability of components

Risk

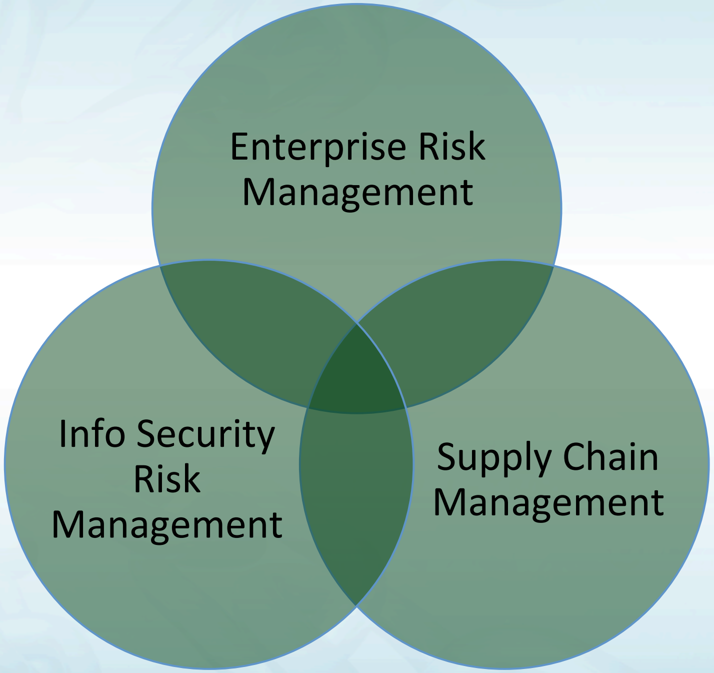
Traditional SCRM vs. ICT SCRM

Traditional Supply Chain Risk Management	ICT SCRM
Supply Chain: Will my physical product get to me on time *efficiently* and with *quality*?	Will my product (physical or logical) get to me as it was shipped and as I ordered? Does it include additional functionality?
Risk Management: Is my supply chain *resilient* and will it continue delivering what I need in case of disaster?	Is my supply chain infiltrated by someone who is inserting extra features into my hardware and software to exploit my systems and get to my information now or later?
What is the risk ***TO*** my supply chain that delivers critical products and services that I need to mitigate?	What is the risk ***TO*** **and** ***FROM*** my supply chain to my business and mission that I need to mitigate?

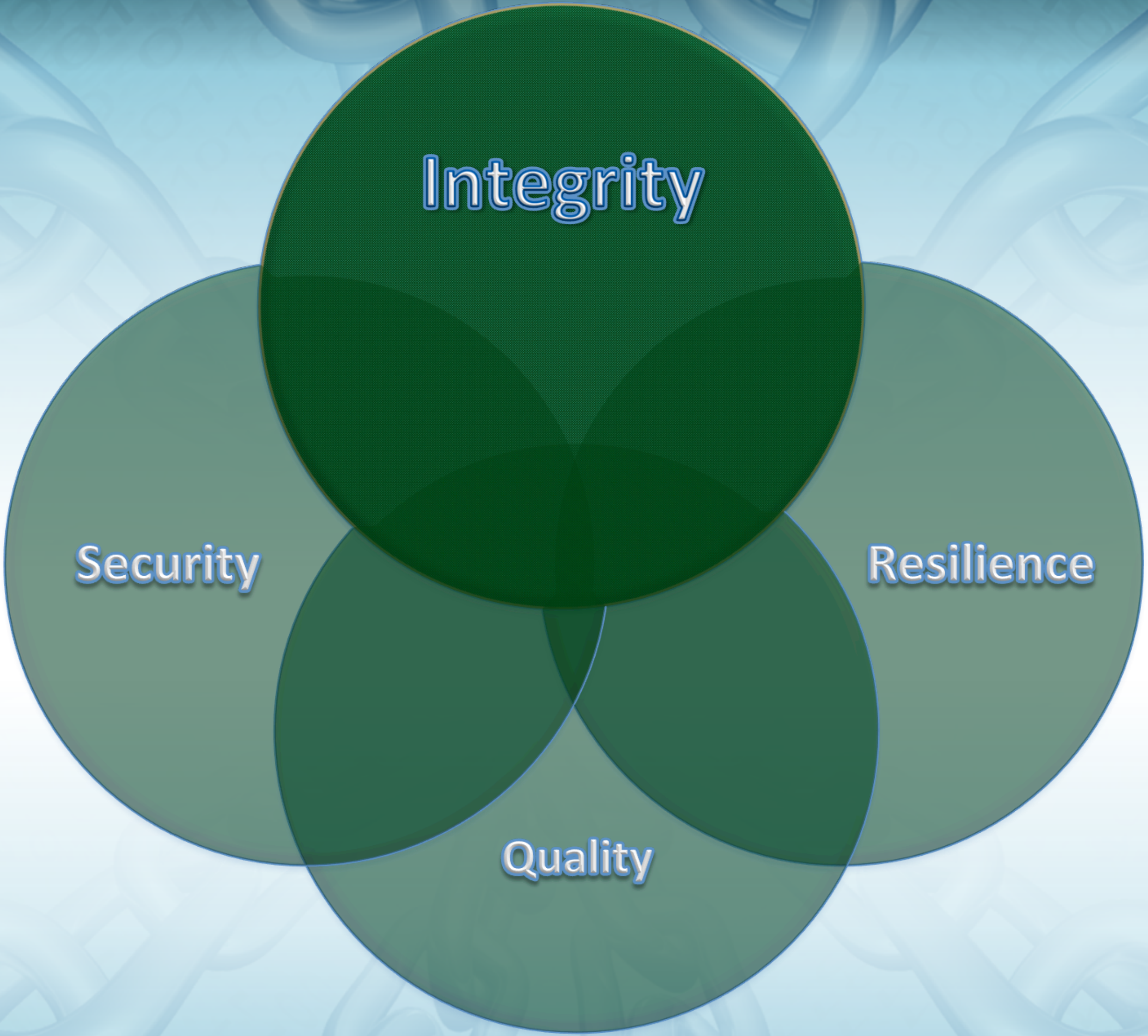
Birth of ICT Supply Chain Risk Management (ICT SCRM)



SCRM



ICT SCRM



4 Pillars of ICT SCRM

USG and Industry Drivers: Push for Solutions

Existing and Emerging Policy, Standards and Practices

Government

Software & Supply Chain Assurance (SSCA) Forum (Public-Private Partnership)

CNCI Stood Up

UMD Research

DoD ICT SCRM Key Practices

NIST IR 7622

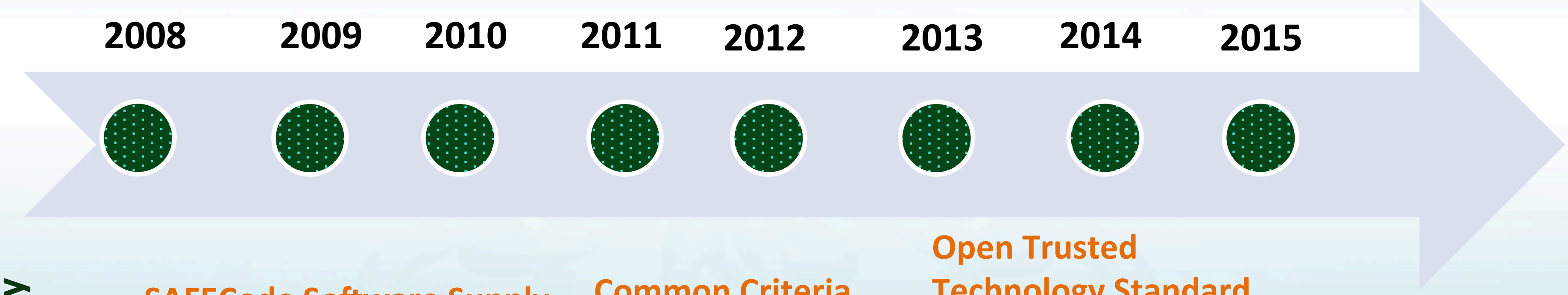
PMOs developed in DOJ and DOE

Sec 515/516 for CJS

Cybersecurity Framework And Roadmap

GAO Report

NIST SP 800-161



Industry

SAFECode Software Supply Chain Integrity papers

Common Criteria Supply Chain Security Assurance

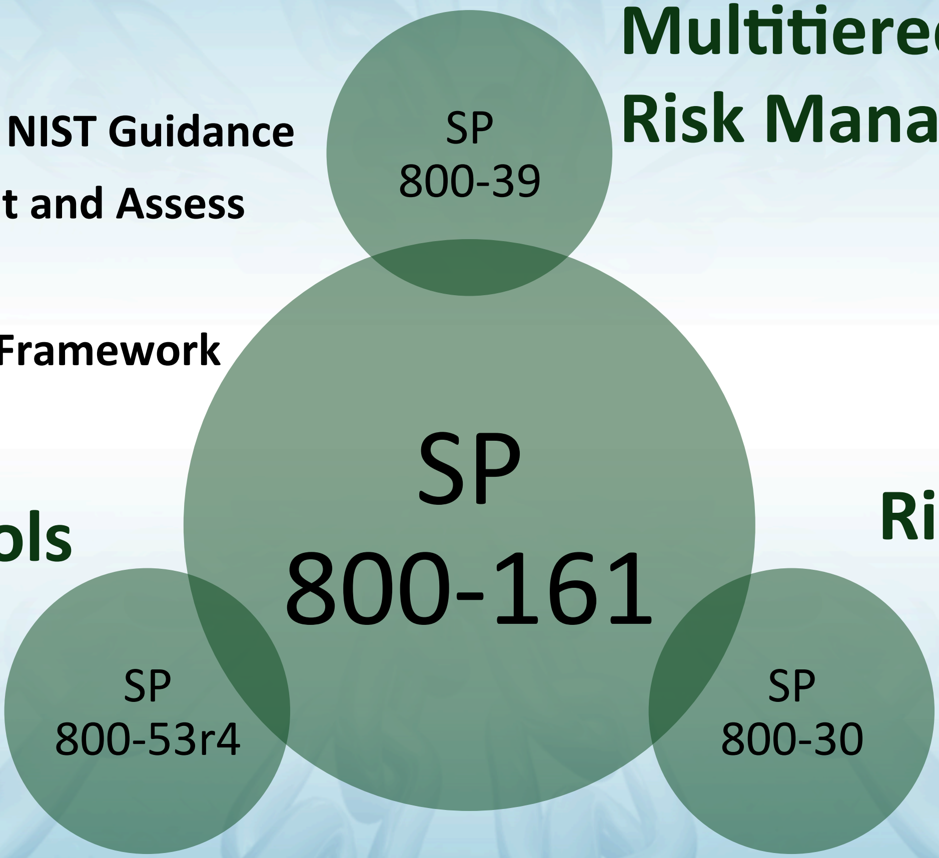
Open Trusted Technology Standard

IEC 62443-2-4 – Industrial-process measurement, control and automation

ISO/IEC 27036 – Information Security in Supplier Relationships

Approach: SP 800-161, Supply Chain Risk Management for Federal Information Systems and Organizations

- Building on existing NIST Guidance
- Ability to Implement and Assess
- SDLC
- Threat Scenarios & Framework
- ICT SCRM Plan



Multitiered Organizational Risk Management

SP 800-39

SP 800-161

Security Controls

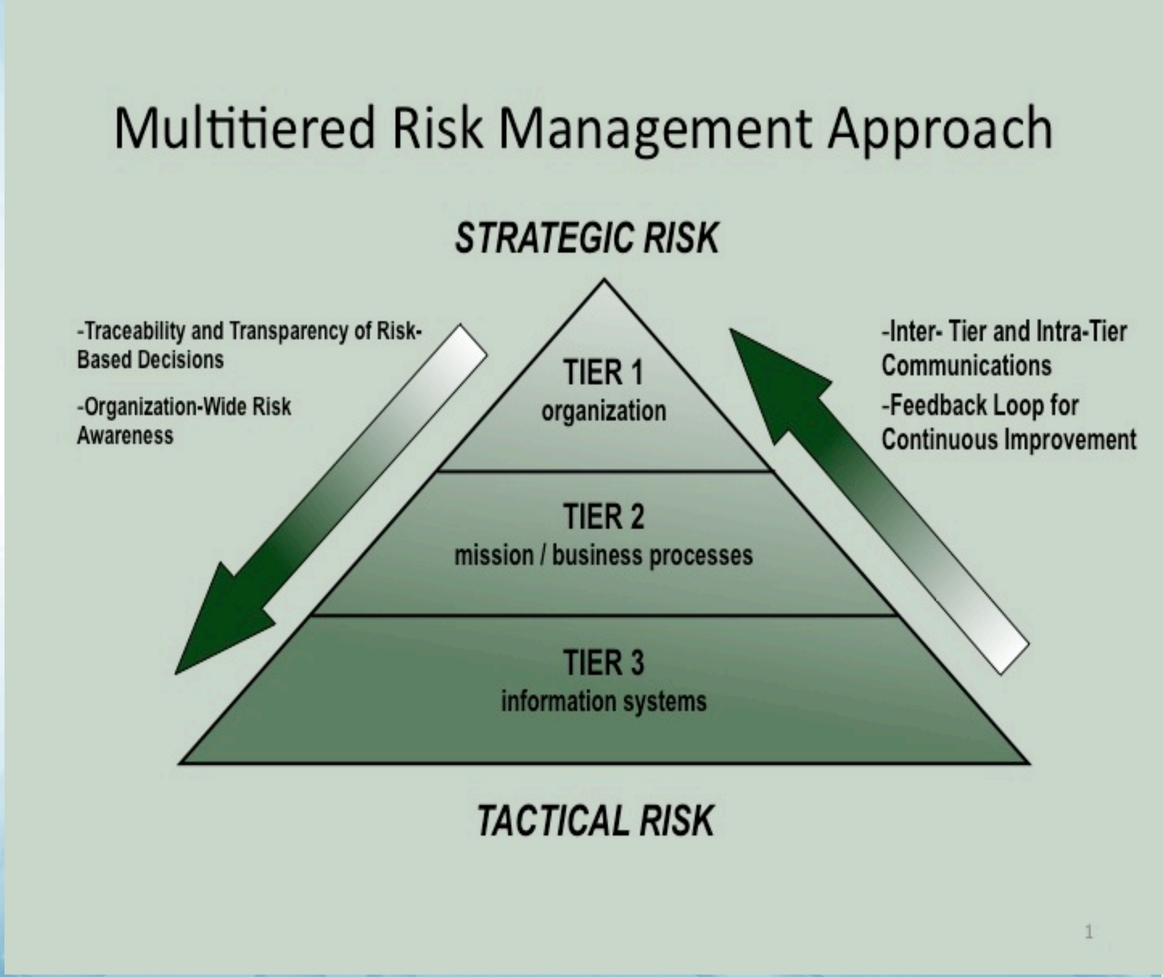
SP 800-53r4

Risk Assessment

SP 800-30

What is Meant by Tier 1, 2, & 3

- SP800-161 defines SCRM responsibilities at each level
- ICT SCRM Plans span all three tiers



Multitiered Risk Management Approach

STRATEGIC RISK

-Traceability and Transparency of Risk-Based Decisions

-Organization-Wide Risk Awareness

TIER 1
organization

TIER 2
mission / business processes

TIER 3
information systems

-Inter- Tier and Intra-Tier Communications

-Feedback Loop for Continuous Improvement

TACTICAL RISK

1

Current and Future Work

Current and Future Work

- Cross-sector Research on Industry ICT Supply Chain Best Practices
  - Organizational strategy
  - Executive communication
  - Case Studies
  - Standards, best practices and guidelines mapping
  - Anything needed wrt SCRM in Framework 2.0?
  - SCRM Workshop: ~ October 1-2, 2015
  - Final Organizational Strategy based on findings
- NIST IRs on Criticality Analysis and Metrics

Current Findings on Industry Best Practices

- Companies interviewed use a federated approach to SCRM, including ICT SCRM
- Use internal corporate standards along with national and international standards and best practices – For example:
  - ISO 27001 for information security
  - ISO 9001/ TL9000 Quality management system (Certified)
  - Common Criteria product certifications
  - ISO14001 Environmental management

Thank you!!

“Just because you're paranoid doesn't mean they aren't after you.”
— Joseph Heller (Catch-22)

Contact: Jon Boyens – jon.boyens@nist.gov

http://scrm.nist.gov