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

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

Celia Paulsen
Computer Security Division
IT Laboratory

August 19, 2014

Agenda

- What is ICT SCRM and what is the Problem?
- NIST's Work
- NIST SP 800-161
  - Overview
  - Status

What is ICT SCRM?

What is the Problem?

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

The Problem

- Counterfeit products
- Vulnerabilities within the supply chain
- Software or hardware delivered with known vulnerabilities
- Malware that is inserted into software or firmware (by various means)

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 networks all over the world.

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

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.

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)*

Threats	Vulnerabilities
Adversarial: e.g., insertion of counterfeits, tampering, theft, and insertion of malicious software.	External: e.g., weaknesses to the supply chain, weaknesses within entities in the supply chain, dependencies (power, comms, etc.)
Non-adversarial: e.g., natural disaster, poor quality products/services and poor practices (engineering, manufacturing, acquisition, management, etc).	Internal: e.g., information systems and components, organizational policy/processes (governance, procedures, 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

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)

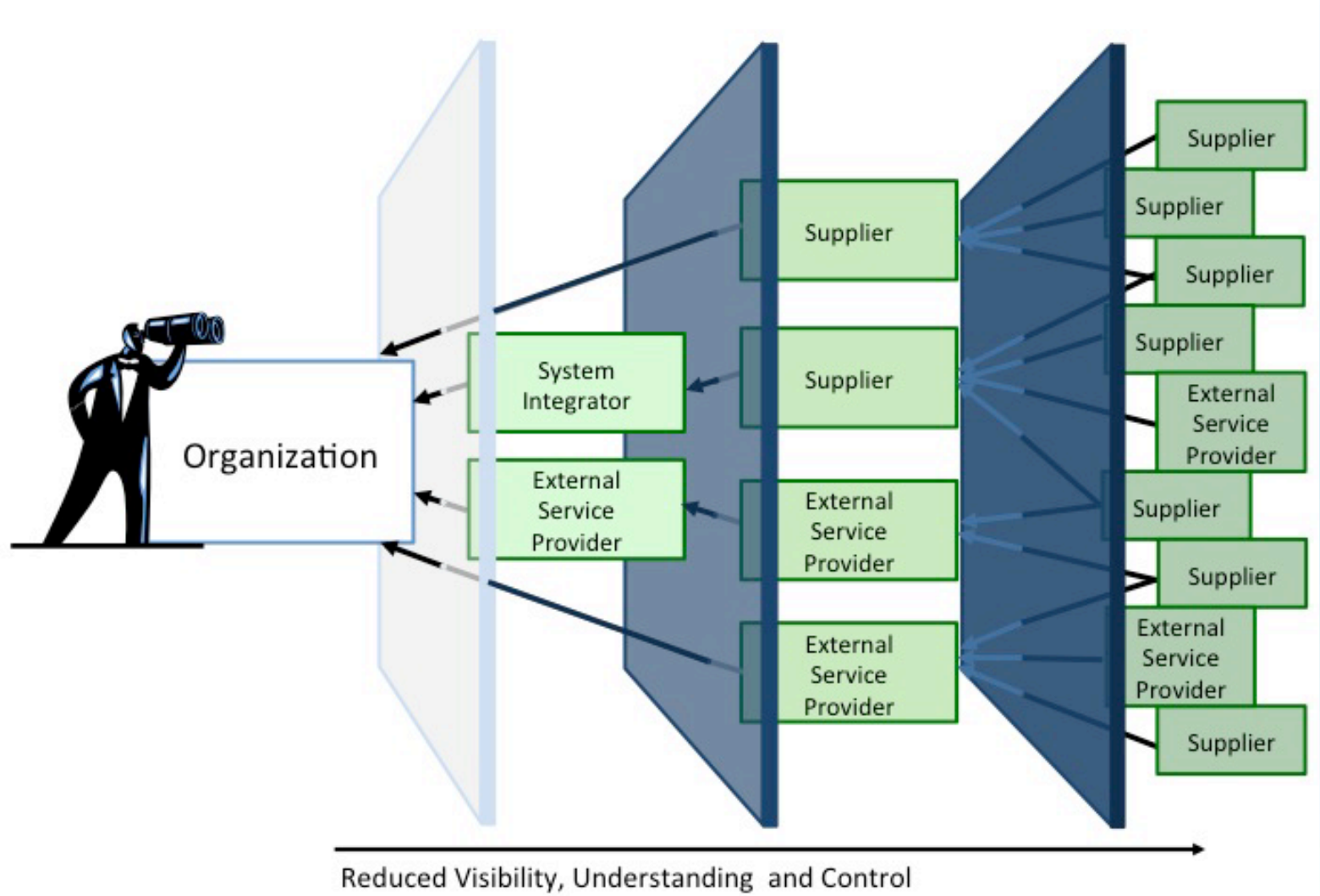
Risk

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

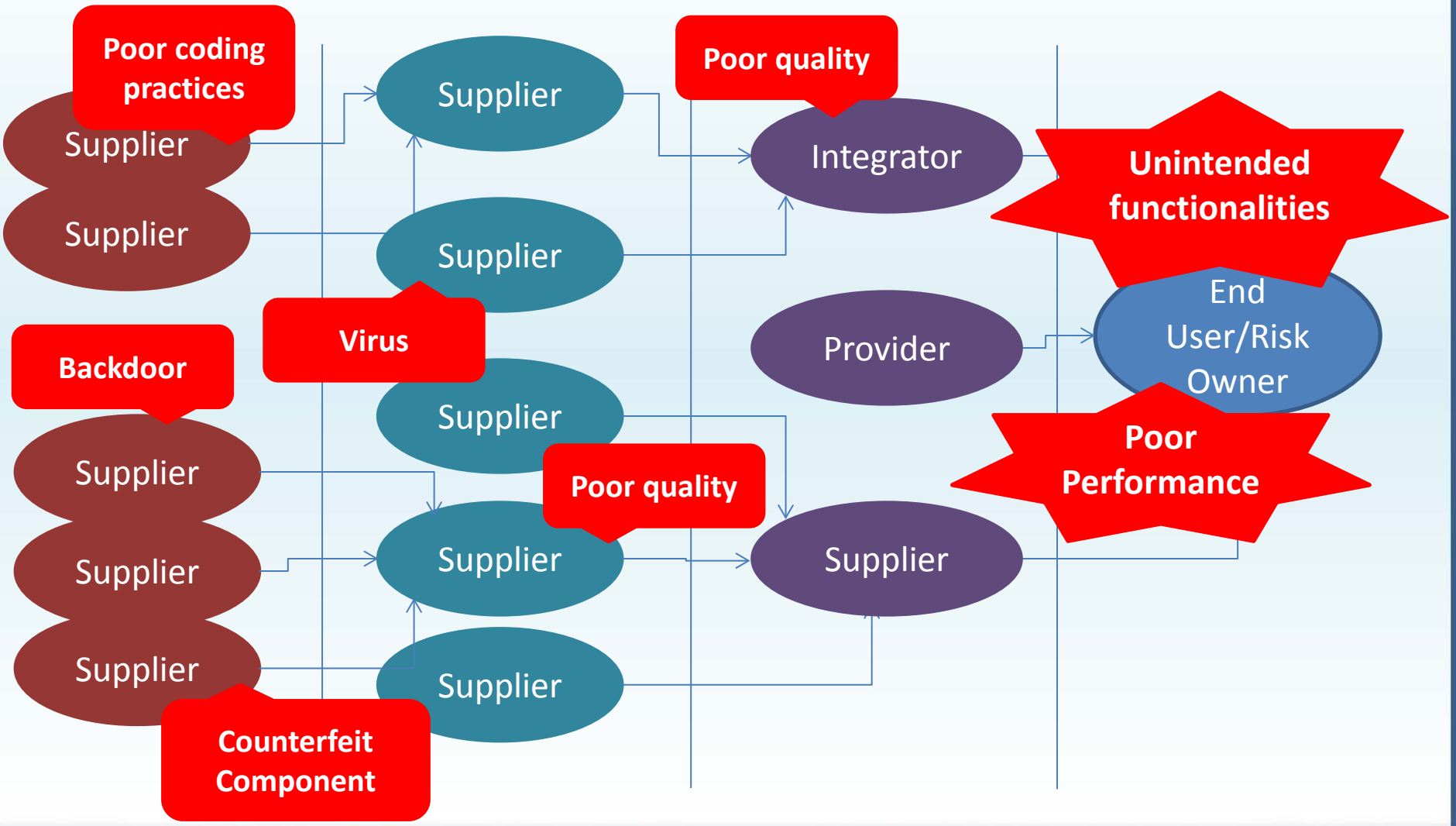
Management

- 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.

Supply Chain Visibility, Understanding, and Control



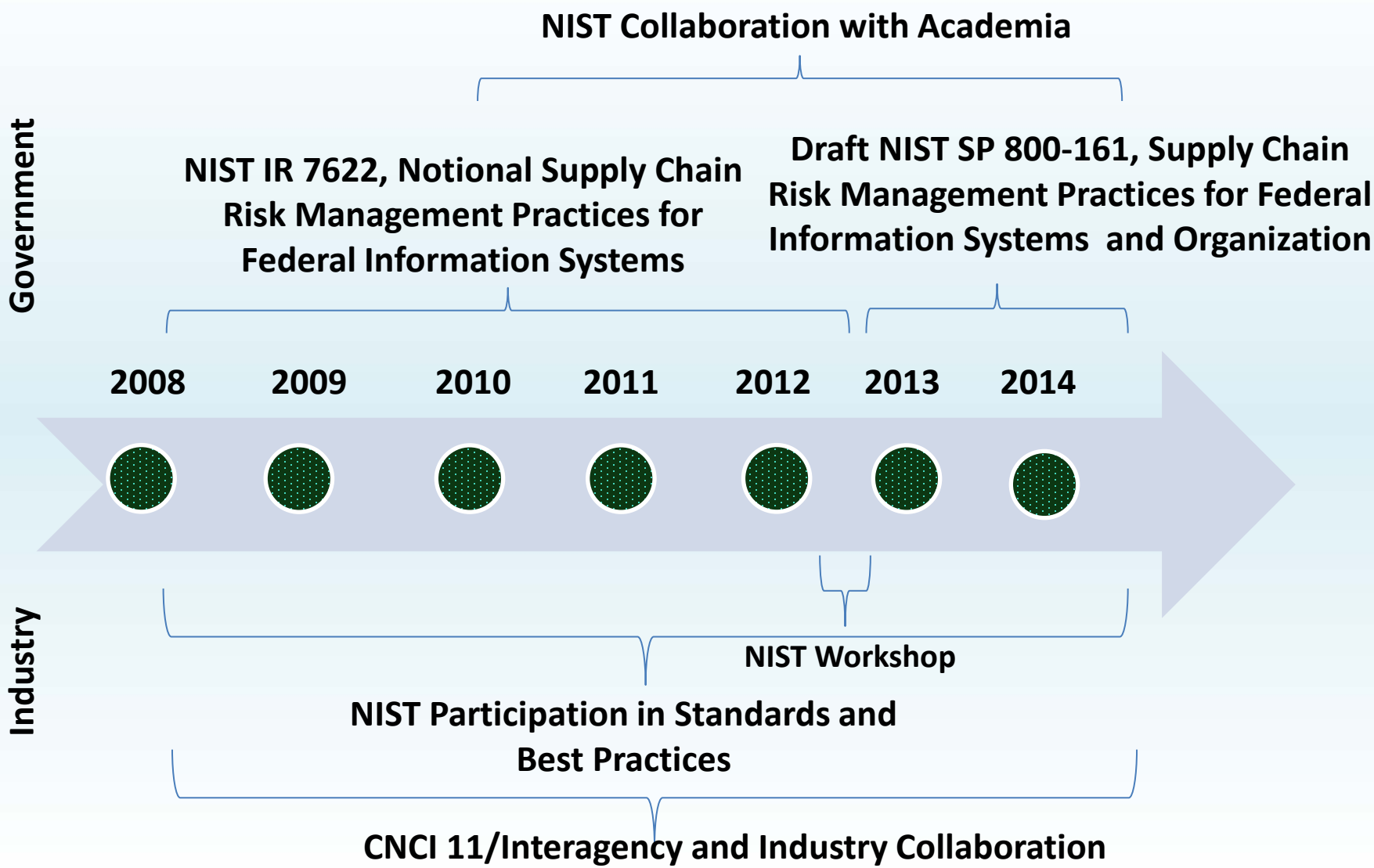
Counterfeits, Intentional Insertion of Malware and Poor Practices



NIST's Work: Enabling innovation, competitiveness and security

ICT SCRM Program

Evolution of NIST ICT SCRM Work

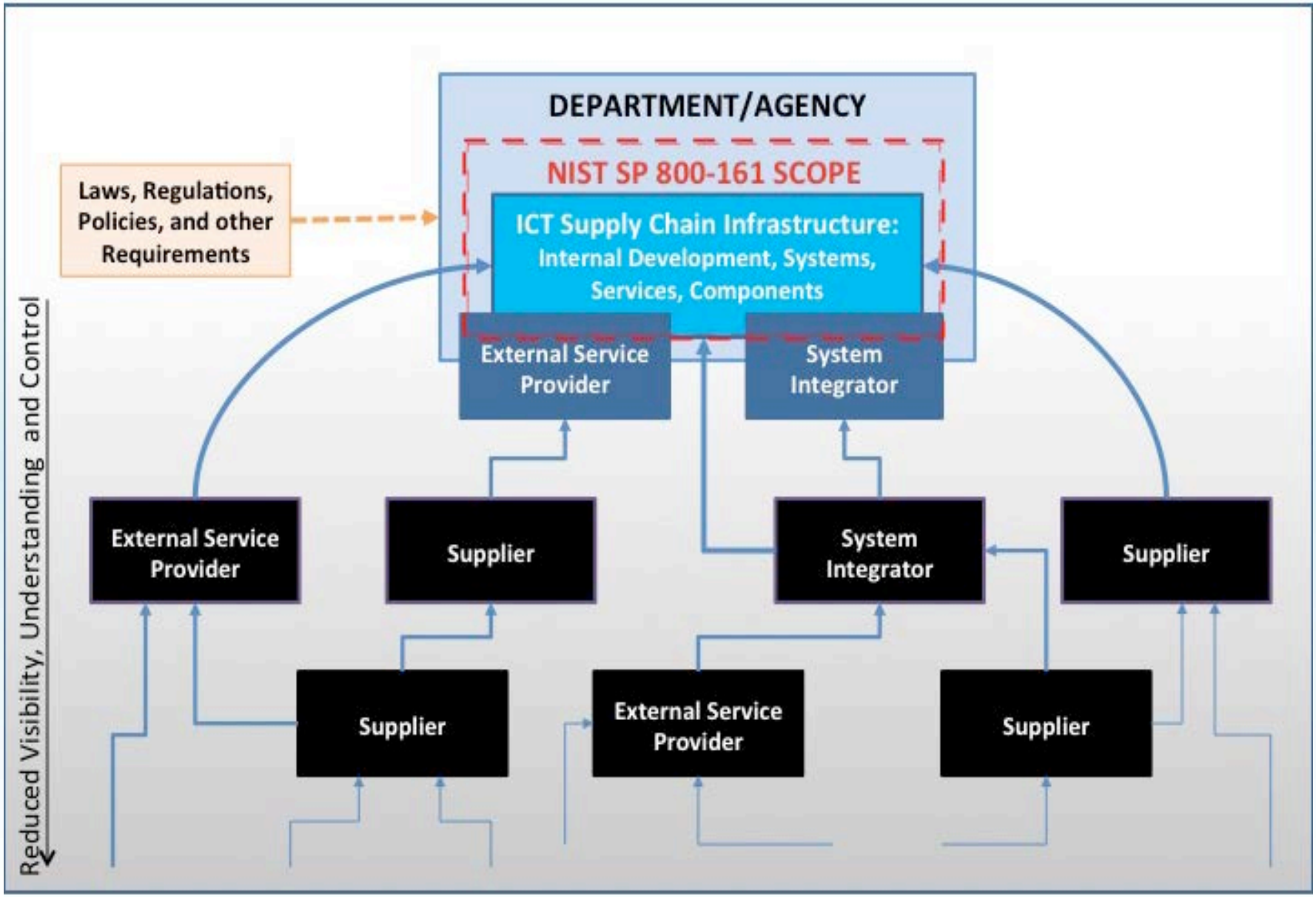


NIST SP 800-161 (Draft)

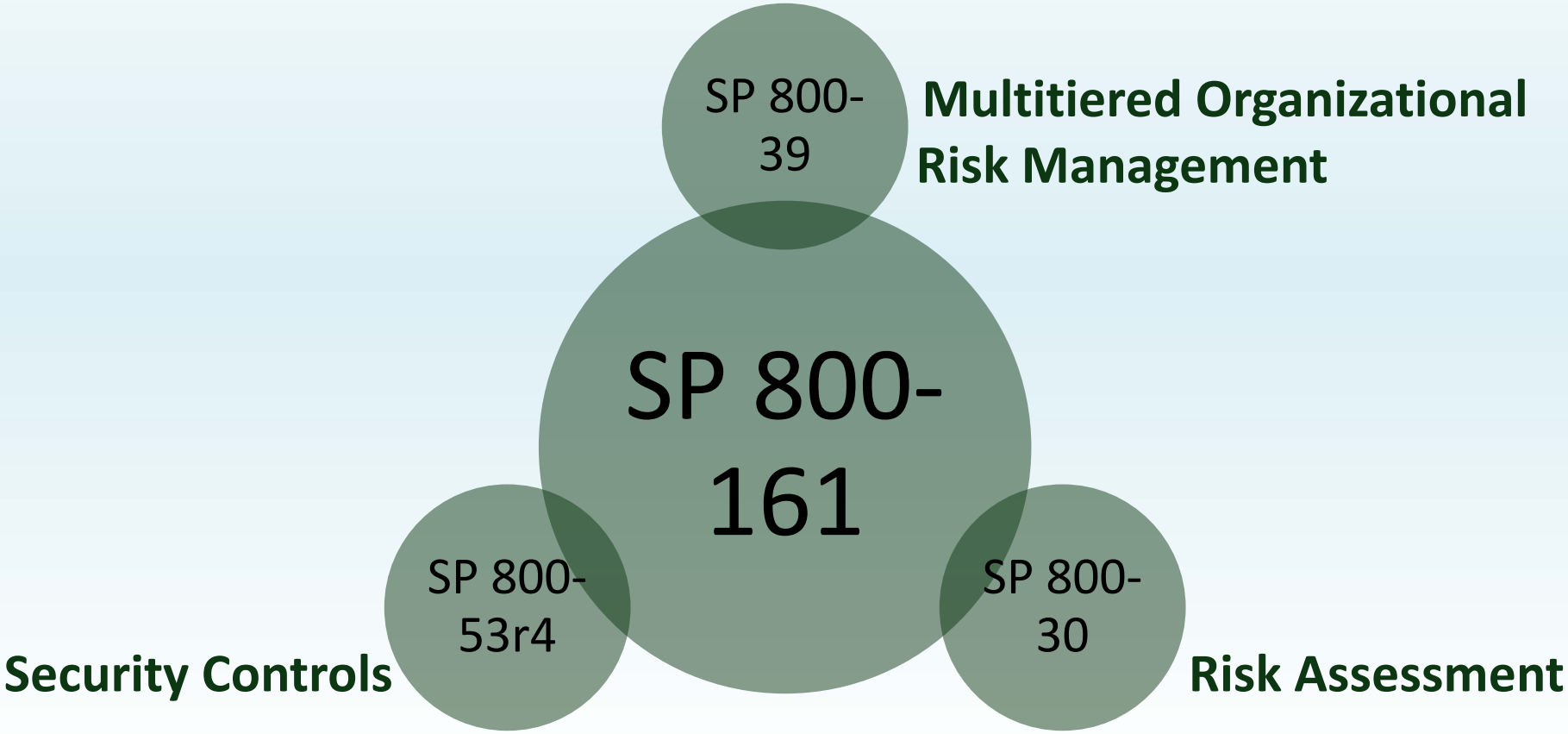
NIST SP 800-161 Overview

- Scope, Purpose, Background, Methodology
- Multi-tiered Approach
- Risk Management Process
- ICT SCRM Controls

- Associated NIST 800-53 Rev. 4 Controls
- Threat Events / Scenarios
- SCRM Plan Template


DEPARTMENT/AGENCY
NIST SP 800-161 SCOPE
Laws, Regulations, Policies, and other Requirements
ICT Supply Chain Infrastructure: Internal Development, Systems, Services, Components
External Service Provider
System Integrator
External Service Provider
Supplier
System Integrator
Supplier
Supplier
External Service Provider
Supplier
Reduced Visibility, Understanding and Control

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

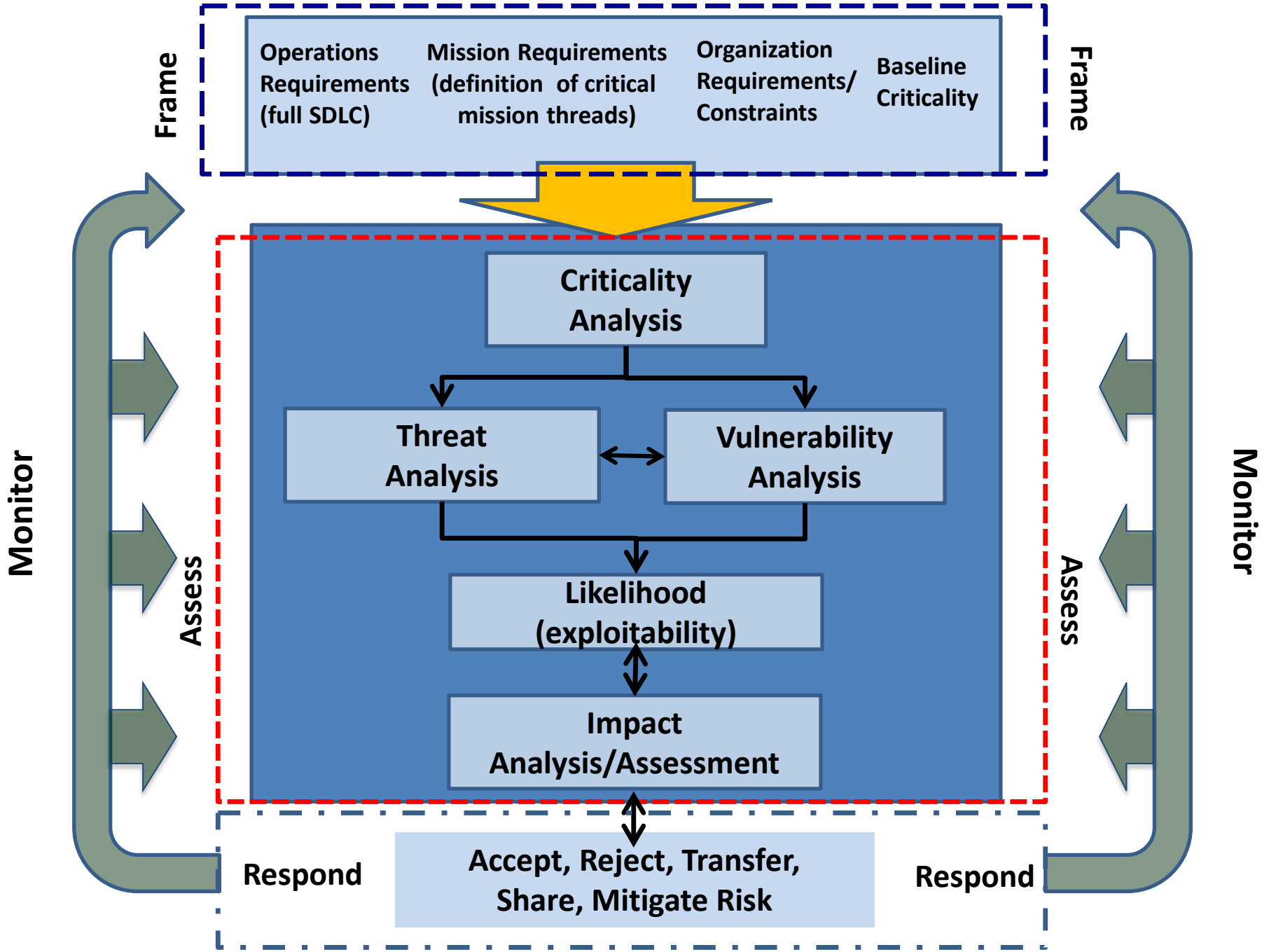


Multi-tiered Approach

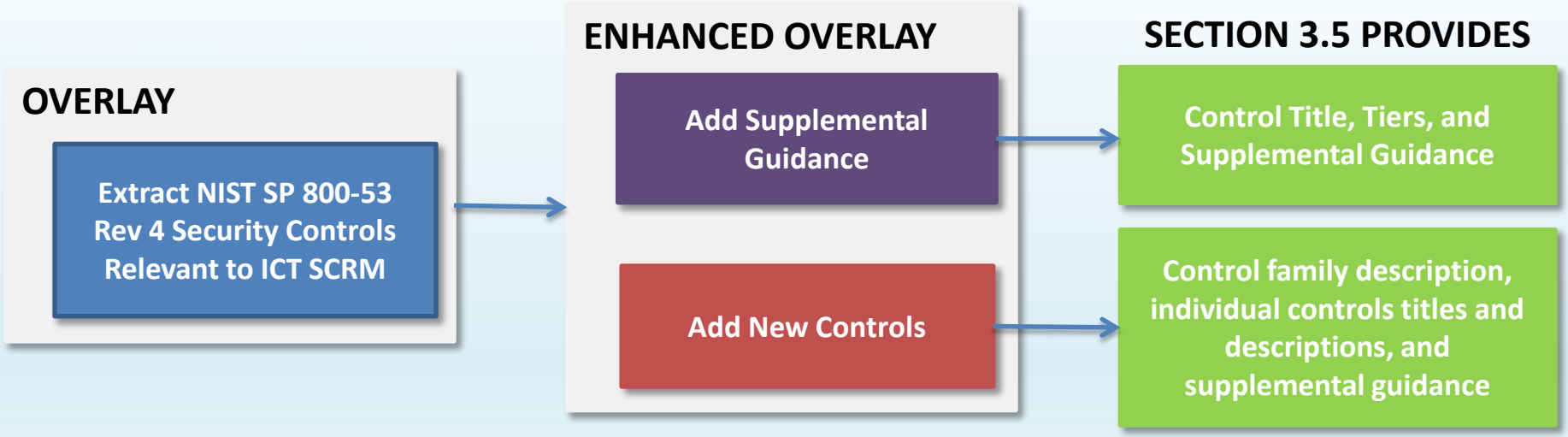
- ICT SCRM responsibilities at each level
- ICT SCRM Plans span all three tiers

Organizational Roles and Activities

Tiers	Tier Name	Type of Role	Activities
1	Organization	• Executive Leadership – CEO, CIO, COO, CFO • Risk executive	• Corporate Strategy • Policy
2	Mission	• Business Management (includes PM, R&D, and Engineering/SDLC oversight) • Procurement • Cost Accounting • ”ility” management – reliability, safety, quality	• Actionable policies and procedures • Guidance • Constraints
3	Operation	• Systems Management – architects, developers, QA/QC, testing • Contracting/procurement – approving selection, payment and approach for obtaining, • Maintenance • Disposal	• Policy implementation • Requirements • Constraints • Implementation


Frame
Operations Requirements (full SDLC)
Mission Requirements (definition of critical mission threads)
Organization Requirements/ Constraints
Baseline Criticality
Frame
Monitor
Assess
Criticality Analysis
Threat Analysis
Vulnerability Analysis
Likelihood (exploitability)
Impact Analysis/Assessment
Assess
Monitor
Respond
Accept, Reject, Transfer, Share, Mitigate Risk
Respond

ICT SCRM Controls



- 6 new controls/supplements
- New family – "Provenance"

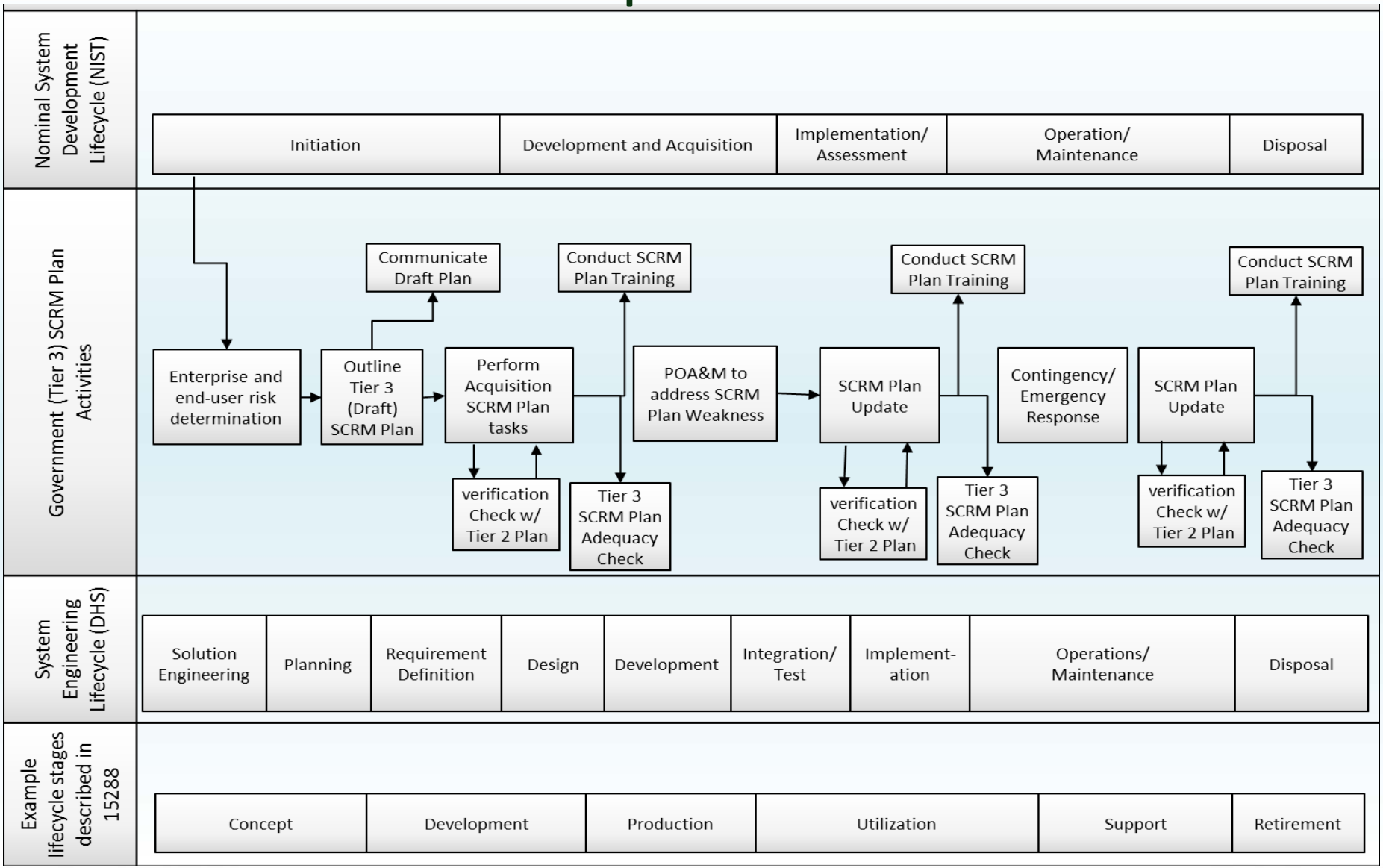
SCRM Control Summary

NIST SP 800-161 SCRM CNTL NO.	800-53 REV. 4 CNTL NO.	CONTROL NAME	800-53 REV. 4 HIGH BASELINE	SCRM BASELINE	TIERS		
		CONTROL ENHANCEMENT NAME			1	2	3
SCRM_AC-1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	X	X	X	X	X
SCRM_AC-2	AC-2	ACCOUNT MANAGEMENT	X	X		X	X
SCRM_AC-3	AC-3	ACCESS ENFORCEMENT	X	X		X	X
SCRM_AC-3(1)	AC-3 (8)	ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS		X		X	X
SCRM_AC-3(2)	AC-3 (9)	ACCESS ENFORCEMENT | CONTROLLED RELEASE		X		X	X
SCRM_AC-4	AC-4	INFORMATION FLOW ENFORCEMENT	X	X		X	X
…							

Threat Events/Scenarios

- Threat events from NIST SP 800-30
- Scenario framework
  - To aid in Risk Analysis
  - 4 example scenarios

ICT SCRM Plan Template



Status

- 2nd public draft comment review period ended
- Over 400 comments received
- Final draft
  - XML format

Contact

Jon Boyens

jon.boyens@nist.gov

Celia Paulsen

celia.paulsen@nist.gov

http://csrc.nist.gov/scrm/