

NIST

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

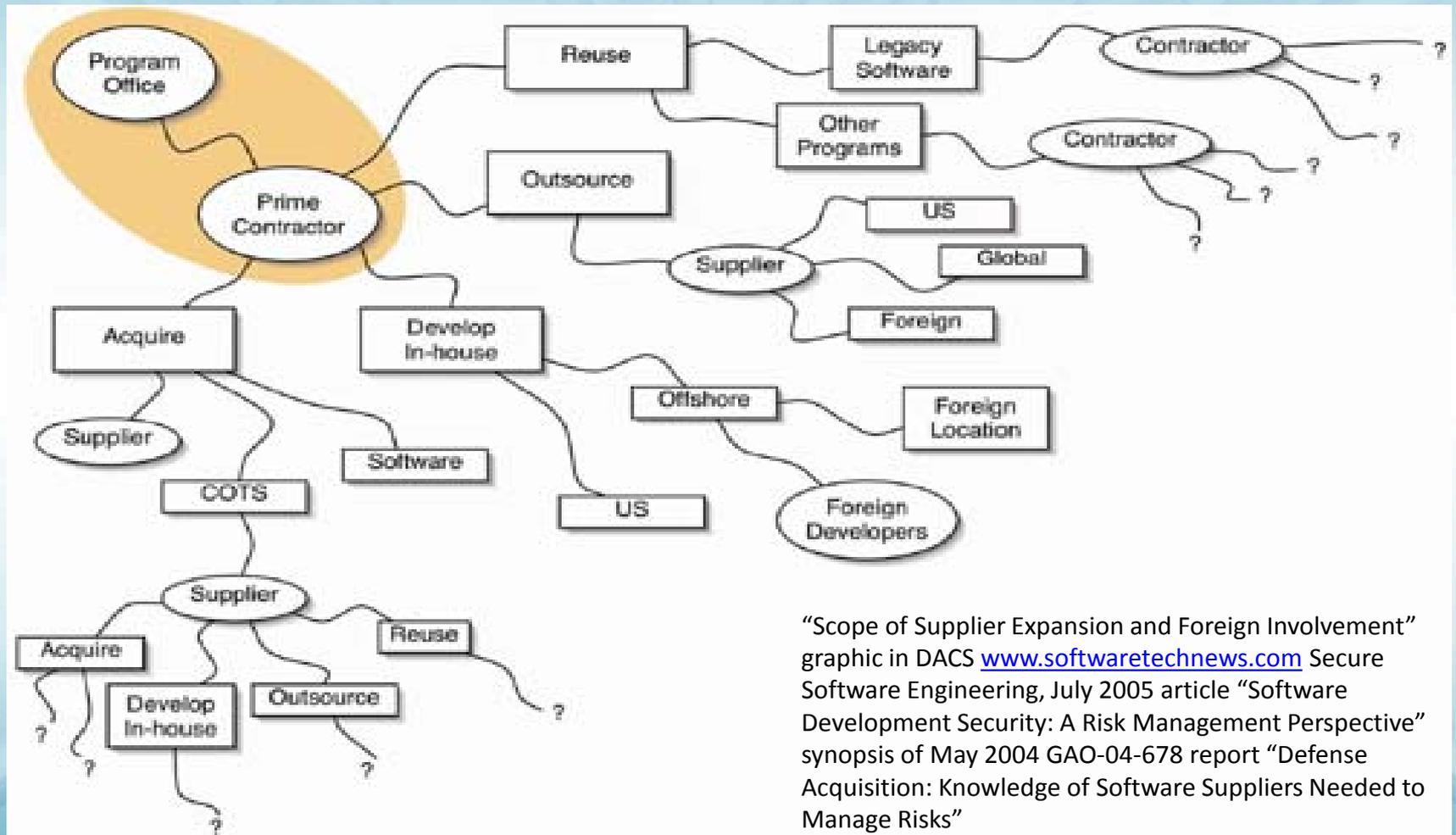
ICT Supply Chain Risk Management

Celia Paulsen
Computer Security Division
IT Laboratory



Manager's Forum
June 4, 2013

General Problem Definition



“Scope of Supplier Expansion and Foreign Involvement” graphic in DACS www.softwarettechnews.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”

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.

ICT Supply Chain Risk

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 failure rates or loss of system availability

From: reduced availability of components



ICT Supply Chain Risk Management

ICT SCRM Approach

➤ SDLC

- Design, development, acquisition, integration, operation, and disposal

➤ Enterprise Risk Management

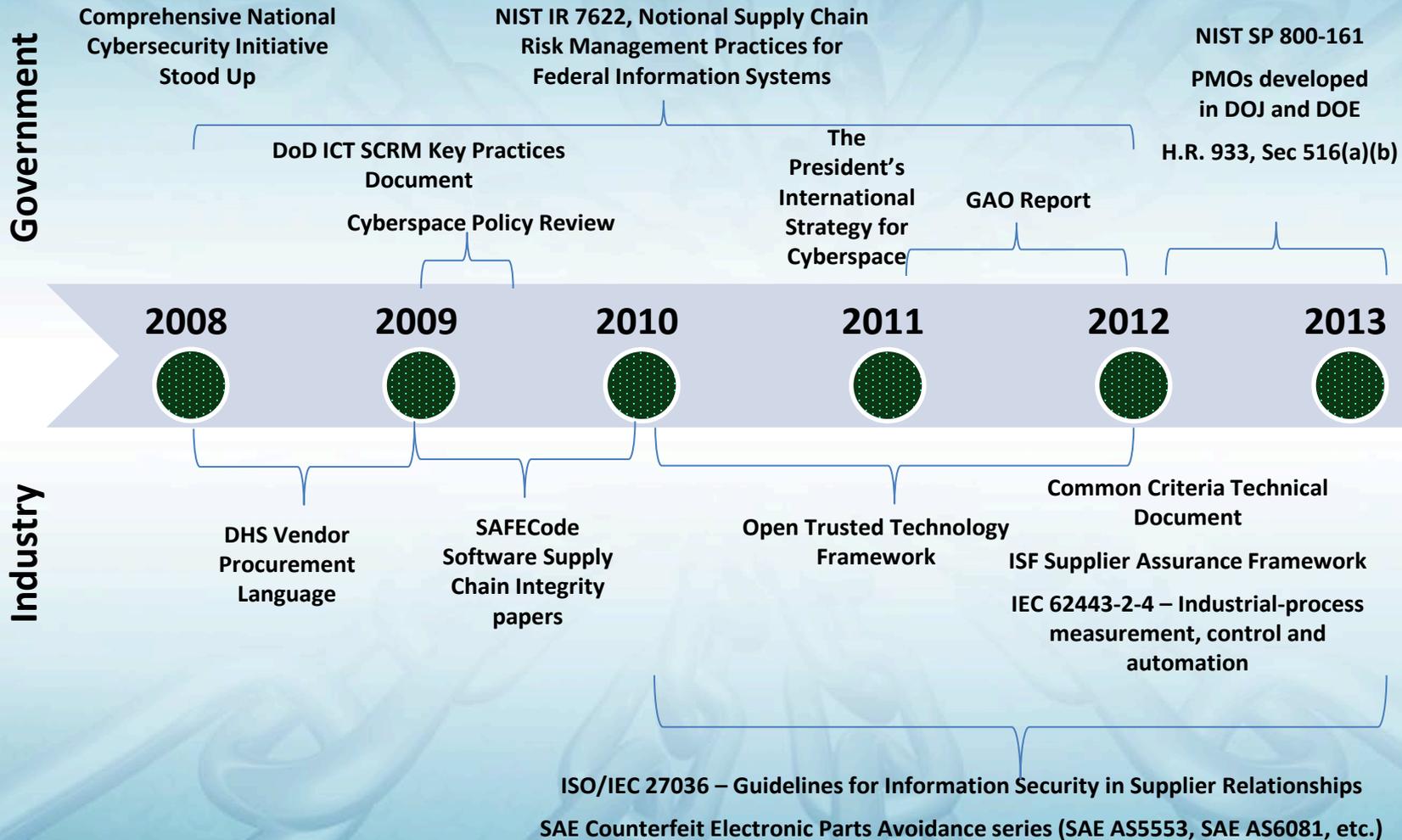
➤ Risk can be managed, but not eliminated.

➤ Holistic approach, involving all stakeholders in an enterprise and identifying risk *to* and *through* the supply chain.

Effective SCRM = Many Disciplines



Existing and Emerging Activity

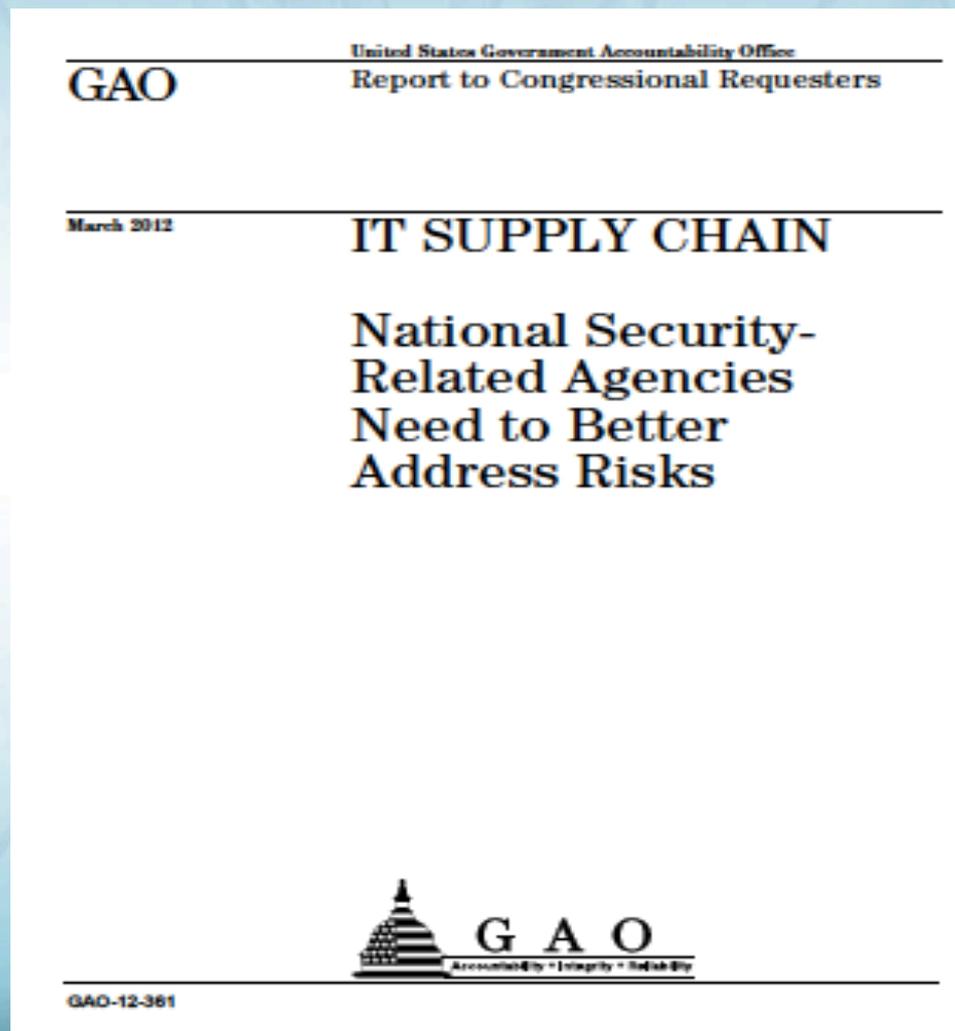


Federal Government Drivers

CNCI 11 – Develop a multi-pronged approach for global supply chain risk management (January 2008)

- **FAR** - Federal Acquisition Regulations (FAR) that require supply chain practices; **(NIST SUPPORT)**
- **INFO SHARING** - A means to share supplier-related threat information;
- **CONTINUOUSLY MANAGE SUPPLY CHAIN RISK** - Increased ability of Federal agencies to manage supply chain risks once an information system is in place;
- **STANDARDS** - Standards (preferably widely-used and/or international) on supply chain practices for integrators and suppliers; and, **(NIST ROLE)**
- **TOOLS AND TECHNOLOGIES** - Current and new technologies and tools incorporated into supply chain practices. **(NIST ROLE)**

Federal Government Drivers

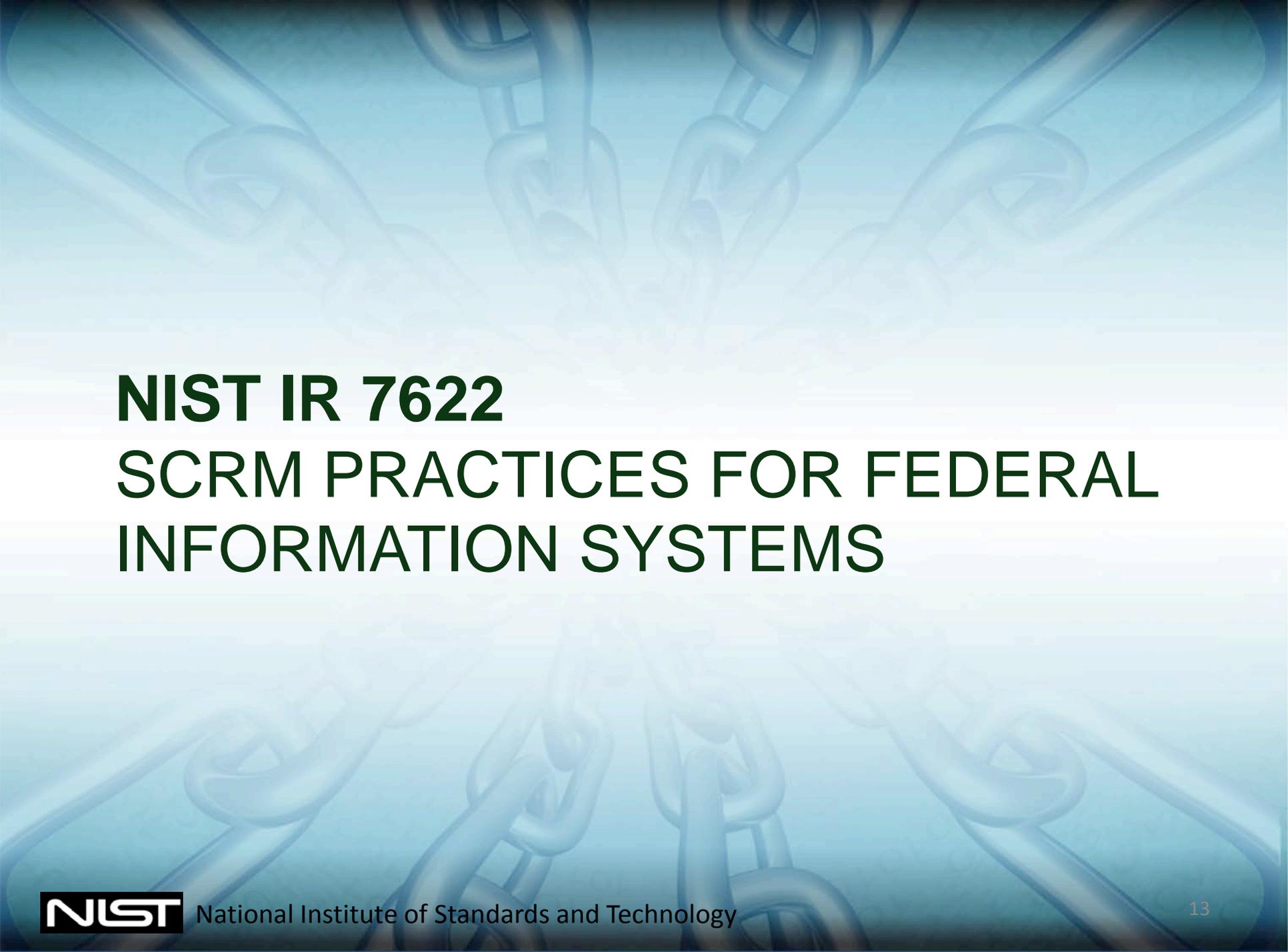


H.R. 933 Sec. 516 (a)(b)

- Sec. 516(a) - None of the funds appropriated or otherwise made available under this Act may be used by the Departments of Commerce and Justice, the National Aeronautics and Space Administration, or the National Science Foundation to acquire an information technology system unless the head of the entity involved, in consultation with the Federal Bureau of Investigation or other appropriate Federal entity, has made an assessment of any associated risk of cyber-espionage or sabotage associated with the acquisition of such system, including any risk associated with such system being produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China.

EO Cybersecurity Framework

- “Supply chain” one of the most mentioned phrases found in responses to NIST’s public *request for information* (RFI).
- Supply chain called out as the Common Point *Understanding Your Threat Environment*, during the RFI analysis.
- Supply chain identified as a Gap (insufficient information) under Dependencies.



NIST IR 7622

SCRM PRACTICES FOR FEDERAL INFORMATION SYSTEMS

NIST IR 7622

- **Guidance** and recommended practices to manage supply chain risk to a level commensurate with the criticality of information systems or networks for the acquiring federal agency only
- **High-Impact Level Systems (FIPS 199)** medium-impact dependent upon risk management approach
- **System Development Life Cycle (SDLC)**
(COTS & GOTS.)
 - Design, development, acquisition, integration, operation, and disposal
- **Broad Audience**
 - System owners, acquisition staff, system security personnel, system engineers, etc.

Implementing ICT SCRM: Roles & Responsibilities

Plan Procurement	Oversee	Oversee	Oversee	Lead	Approve	Lead
Define/Develop Requirements	Oversee	Oversee	Oversee	Advise	Advise	Lead
Identify Potential Suppliers and/or Perform Market Analysis	Oversee	Oversee	Oversee	Advise	Advise	Lead
Complete Procurement	Oversee	Oversee	Approve	Lead	Approve	Lead
Operations and Maintenance	Oversee	Oversee	Oversee	Advise	Advise	Lead

Risk Executive (Function)	Chief Information Officer (CIO)	Senior Information Security Officer (SISO)	Contracting Officer(CO)	Legal	Mission Business Owner
---------------------------	---------------------------------	--	-------------------------	-------	------------------------



PROCESS →

NISTIR 7622 ICT SCRM Practices Format

Practices formatted by role, activities, and requirements.

Practice
Format

Role	Type of Action	Description of Action
Acquirer	Programmatic Activities	Practices that an acquirer will undertake within their programs, including requirements to be included in contractual documents, as well as internal policies and procedures.
Integrator	General Requirements	General practices that an integrator will implement within programs that are either in response to contractual requirements or to document existence of programmatic activities that reduce supply chain risk.
Supplier	General Requirements	General practices that a supplier will implement within programs to document existence of programmatic activities that reduce supply chain risk.
Integrator	Technical Implementation Requirements	Detailed technical practices that an integrator will implement within programs to document technical capabilities to manage supply chain risk.
Supplier	Technical Implementation Requirements	Detailed technical practices that a supplier will implement within programs to document technical capabilities to manage supply chain risk.
Acquirer	Validation and Verification Activities	Suggestions for how an acquirer can ascertain that integrators or suppliers have implemented ICT SCRM.
Integrator	Validation and Verification Requirements	Suggestions on how an integrator can demonstrate that they have implemented ICT SCRM.
Supplier	Validation and Verification Requirements	Suggestions on how a supplier can demonstrate that they have implemented ICT SCRM.

NISTIR 7622 ICT SCRM Practices

Uniquely Identify Supply Chain Elements, Processes, and Actors

Limit Access and Exposure within the Supply Chain

Create and Maintain the Provenance of Elements, Processes, Tools and Data

Share Information within Strict Limits

Perform SCRM Awareness and Training

Use Defensive Design for Systems, Elements, and Processes

Perform Continuous Integrator Review

Strengthen Delivery Mechanisms

Assure Sustainment Activities and Processes

Manage Disposal and Final Disposition Activities Throughout the System or Element Lifecycle



Special Publication 800-53 R4

Security and Privacy Controls for Federal Information Systems and Organizations

SA-12: Supply Chain Protection

- Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.
- Supplemental Guidance: Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control enhancement also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

SA-12: Supply Chain Protection

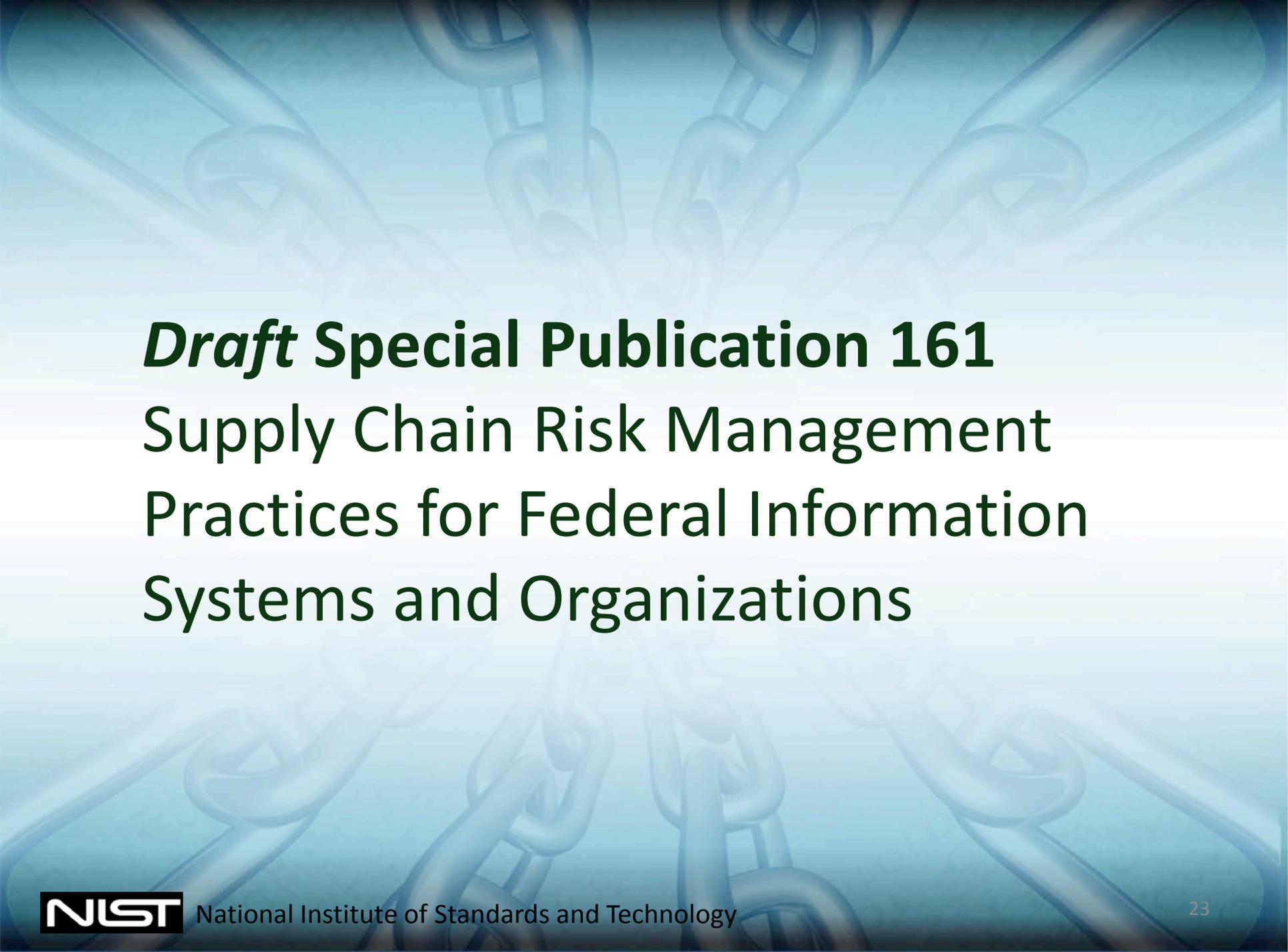
1. Acquisition Strategies / Tools / Methods
2. Supplier Reviews
3. Limitation Of Harm
4. Assessments Prior To Selection / Acceptance / Update
5. Use Of All-source Intelligence
6. Operations Security
7. Validate As Genuine And Not Altered
8. Penetration Testing / Analysis Of Supply Chain Elements, Processes and Actors
9. Inter-organizational Agreements
10. Critical Information System Components
11. Identity And Traceability
12. Processes To Address Weaknesses Or Deficiencies

Related SA Controls

- SA-3 System Development Life Cycle
- SA-4 Acquisition Process
- SA-8 Security Engineering Principles
- SA-9 External Information System Services
- SA-10 Developer Configuration Management
- SA-11 Developer Security Testing and Evaluation
- SA-14 Criticality Analysis
- SA-15 Development Process, Standards and Testing
- SA-18 Tamper Resistance and Detection
- SA-19 Component Authenticity
- SA-20 Customized Development of Critical Components

Supply Chain-related Controls (non-SA)

- AT-3 Security Training
- CM-8 Information System Component Inventory
- IR-4 Incident Handling
- PE-16 Delivery and Removal
- PL-8 Information Security Architecture
- SC-29 Heterogeneity
- SC-30 Concealment and Misdirection
- SC-38 Operations Security
- SI-7 Software, Firmware and Information Integrity



Draft Special Publication 161
**Supply Chain Risk Management
Practices for Federal Information
Systems and Organizations**

Draft SP 161, SCRM Practices For Federal Information Systems

➤ Goals and Scope

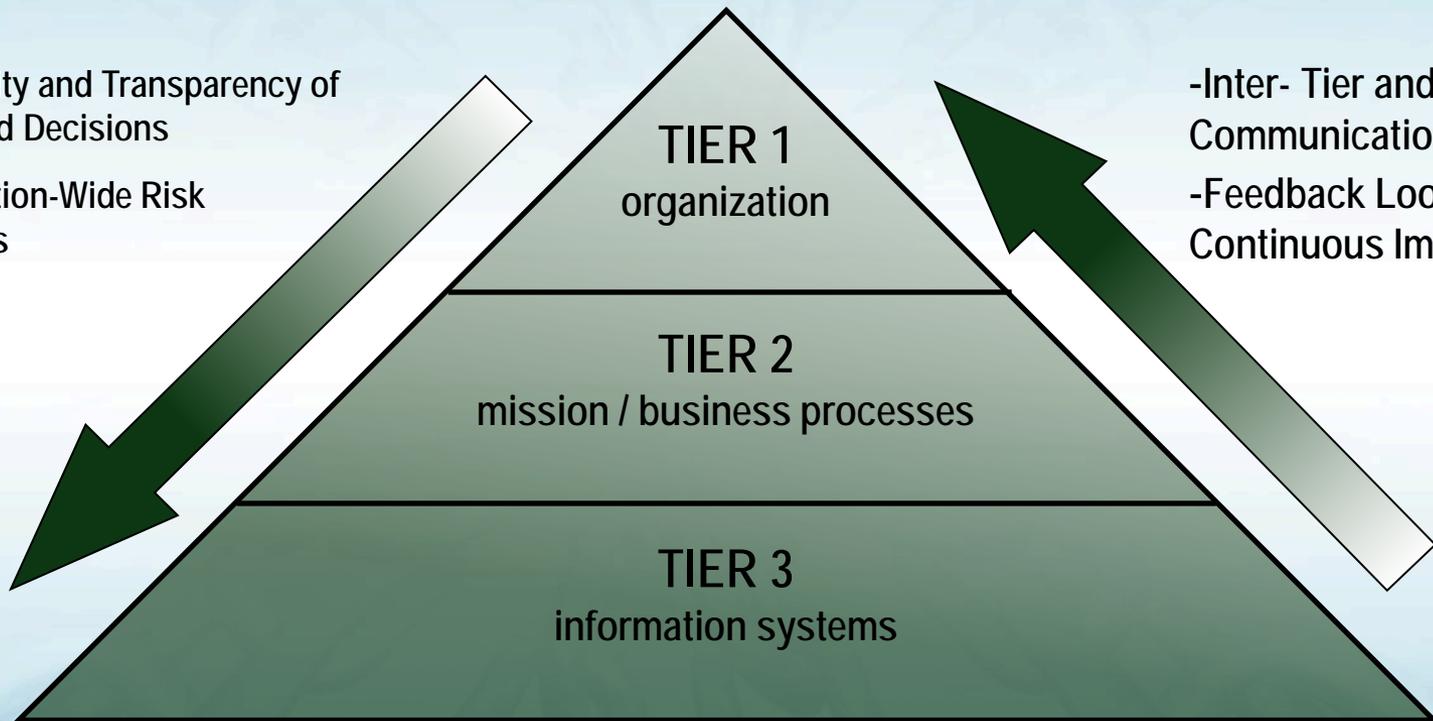
- Ability to implement and assess
- Enterprise Risk Management
- System Development Life Cycle
- Tied to JTF Unified Framework and other publications
 - Enterprise Supply Chain Risk Management Guidance (800-39; Organization, mission/business, operations/system)
 - Supply Chain Risk Assessment Guidance (800-30)
 - Risk Mitigation and Control Selection Guidance 800-53 R4 and 800-53A – Enhanced Overlay

Three Tiered Risk Management Approach

STRATEGIC RISK

- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness

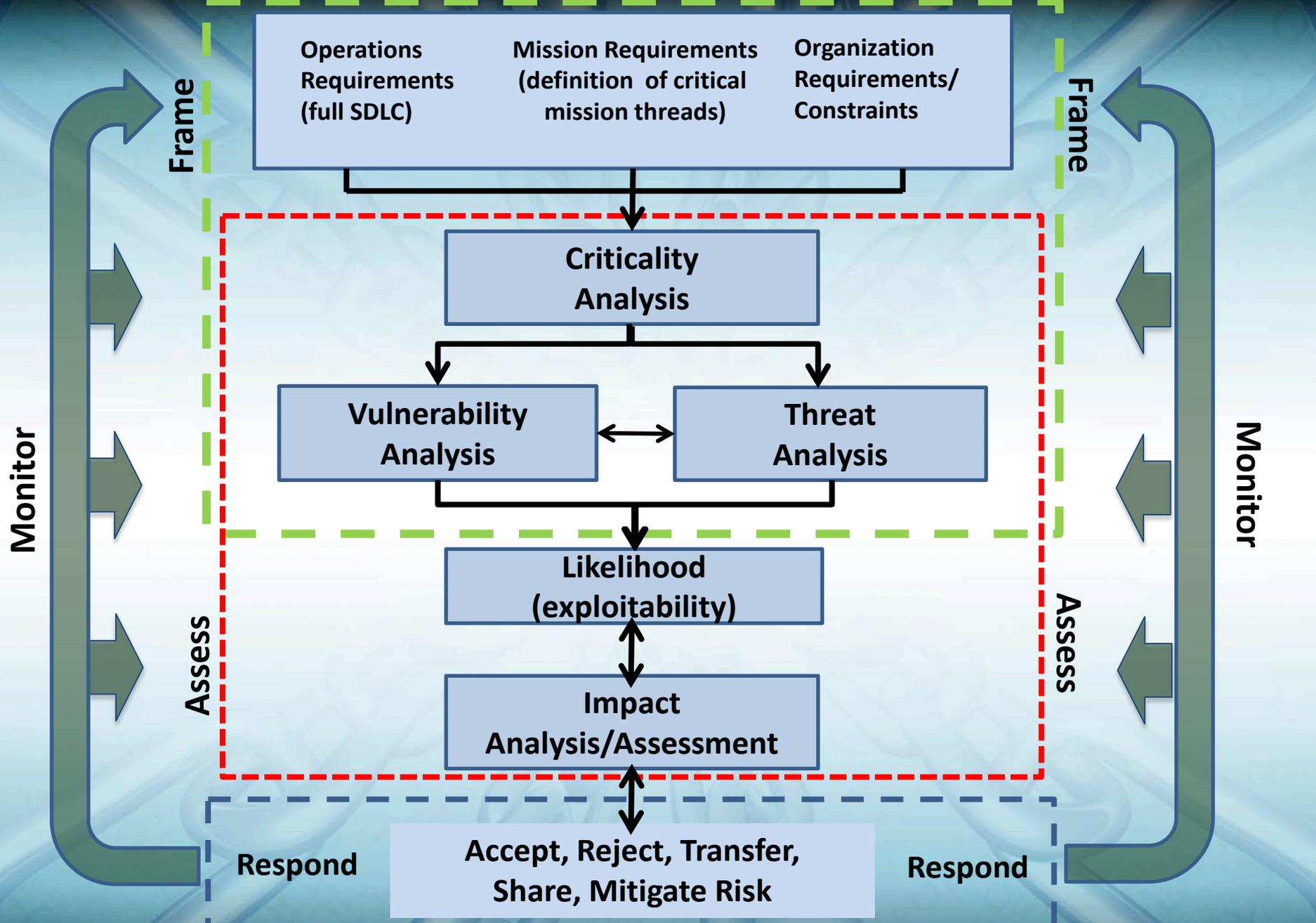
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement



TACTICAL RISK

Organizational Roles and Activities

Tiers	Tier Name	Type of Role	Activities
1	Organization	<ul style="list-style-type: none"> Executive Leadership – CEO, CIO, COO, CFO Risk executive 	<ul style="list-style-type: none"> Corporate Strategy Policy
2	Mission	<ul style="list-style-type: none"> Business Management (includes PM, R&D, and Engineering/SDLC oversight) Procurement Cost Accounting Reliability / safety / quality management 	<ul style="list-style-type: none"> Actionable policies and procedures Guidance Constraints
3	Operation	<ul style="list-style-type: none"> Systems Management – architects, developers, QA/QC, testing Contracting/procurement – approving selection, payment and approach for obtaining, Maintenance Disposal 	<ul style="list-style-type: none"> Policy implementation Requirements Constraints Implementation



Frame

Frame

Monitor

Monitor

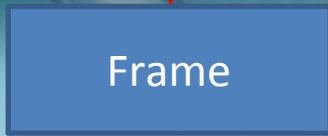
Assess

Assess

Respond

Respond

Enterprise



- Develop ICT SCRM Policy
- Conduct Baseline Criticality Determination
- Integrate ICT SCRM considerations into enterprise risk management

- Integrate ICT SCRM considerations into enterprise risk management

- Make enterprise risk decisions to avoid, mitigate, share, or transfer risk
- Select, tailor, and implement appropriate enterprise ICT SCRM controls
- Document controls in Enterprise ICT SCRM Plan

- Integrate ICT SCRM into agency Continuous Monitoring program
- Monitor and evaluate enterprise-level constraints and risks for change and impact
- Monitor effectiveness of enterprise-level risk response

Mission/Business Process

- Define ICT SCRM Mission/business requirements
- Incorporate these requirements into mission/ business processes and enterprise architecture
- Establish ICT SCRM Risk Assessment Methodology
- Establish FIPS 199 impact levels
- Conduct Mission Function Baseline Criticality Determination
- Determine ICT SCRM risk assessment methodology

- Conduct Risk Assessment including Criticality Analysis for mission threads
- Determine current risk posture

- Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk
- Select, tailor, and implement appropriate mission/ business-level controls
- Document controls in Mission-level ICT SCRM Plan

- Identify which mission functions need to be monitored for ICT supply chain change and assessed for impact
- Integrate ICT SCRM into Continuous Monitoring processes and systems
- Monitor and evaluate mission-level risks and constraints for change and impact
- Monitor effectiveness of mission-level risk response

System

- Define system-level ICT SCRM requirements

- Conduct ICT SCRM Risk Assessment including Criticality Analysis for individual systems
- Determine current risk posture

- Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk
- Select, tailor, and implement appropriate system-level controls
- Document ICT SCRM controls in System Security Plan

- Monitor and evaluate system-level requirements and risks for change and impact
- Monitor effectiveness of system-level risk response



Contact:

Jon Boyens – jon.boyens@nist.gov

Celia Paulsen – celia.paulsen@nist.gov

<http://scrm.nist.gov>

Components of Risk Assessment

➤ Criticality Analysis

- Purpose: narrow the scope (and resources) issues most important for mission success
- FIPS 199 helps to scope which systems require SCRM
- Criticality analysis narrows the system and its functions to focus on those issues most important for mission success.
- Can contain:
 - Logic-bearing components which can be especially susceptible to malicious alteration throughout the system life cycle
 - Functional breakdown which is an effective method to identify functions, associated critical components, and supporting defensive functions
 - Dependency analysis which is used to identify these functions on which critical functions depend, which themselves become critical functions (e.g., defensive functions such as digital signatures used in software patch acceptance)
 - Identification of all access points and assessment to identify and protect unmediated access to critical function/components (e.g., least privilege implementation)

Components of Risk Assessment

➤ Threat Analysis:

- Specific and timely threat characterization of the identified suppliers, threat adversaries, and any natural disaster possibilities to inform management, acquisition, and engineering activities in an organization
- Includes the capture of data such as:
 - Changes to the systems/components or SDLC environment
 - Observation of attacks while they are occurring
 - Incident data collected post attack
 - Observation of tactics, techniques, and procedures used in specific attacks, whether observed or collected using audit mechanisms
 - Natural disasters in pre, during and post occurrence

Components of Risk Assessment

- Vulnerability: any weakness in system/component design, development, production, or operation that can be exploited by a threat to defeat a system's mission objectives or significantly degrade its performance.
- Vulnerability Analysis
 - Analysis is focused on mission critical functions and systems/components identified by criticality analysis.
 - Iterative process which can lead to adjustment in criticality, and threat analysis as well as informing risk assessment and countermeasure selection.
 - The principal vulnerabilities to watch for in an overall review of SDLC are:
 - Access paths within the supply chain allowing malicious actors to introduce components causing system failure at some later time (“components” here include hardware, software, and firmware).
 - Access paths through which malicious actors can trigger a component malfunction or failure during system operations.
 - Dependencies on supporting or associated components with easy access to subvert components that directly perform critical functions.
 - information gathering opportunities both on the supply chain and component/service (reverse engineering, weaknesses, etc)

Components of Risk Assessment

➤ Likelihood

- Likelihood is the possibility of an exploit occurrence. For Supply chain risk analysis, likelihood is a weighted factor based on a subjective analysis –the probability that a given threat is capable of exploiting a given vulnerability. (CNSS-4009).
- Key knowledge required to evaluate likelihood:
 - Threat assumptions (man-made threats – including natural disasters, cyber threats, etc)
 - Threat modeling of SDLC environment or the supply chain element.
 - Actual supply chain threat information (e.g. adversaries' capabilities, tools, intentions, targets of desire)
 - Empirical data and static analysis to determine probabilities of supply chain threat occurrence
 - Vulnerabilities identified at the system, component, or process weakness.

➤ Impact

- Impact measures the magnitude of harm that can result from the consequences of unauthorized or unpredicted disclosure, modification, or destruction or loss of information or system availability. For supply chain this can mean the access to elements in the supply chain or the supply chain itself requiring organizational, mission/business and operational assessment.