Draft Notional Supply Chain Risk Management Practices for Federal Information Systems NIST IR 7622

Federal Computer Security Program Managers' Forum
13 June 2012

Jon Boyens
Computer Security Division

NIST National Institute of Standards and Technology

NIST Interagency Reports (NIST IRs)

- Describe research of a technical nature of interest to a specialized audience.
- Include interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment).
- May also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in more comprehensive form.

Purpose

- 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.

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;
- **INFO SHARING** - A means to share supplier-related threat information;
- **CONTINUOUSLY MANAGE SUPPY 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)**

NIST

HISTORY

- Initial public draft – June 2010
- Second public draft – March 23 - May 25, 2012

Changes to Second Draft

- Problem

Growing sophistication of today's ICT

+

Speed and scale of globalization

↓

Complex global ICT supply chain with logically long and geographically diverse routes, including multiple tiers of outsourcing

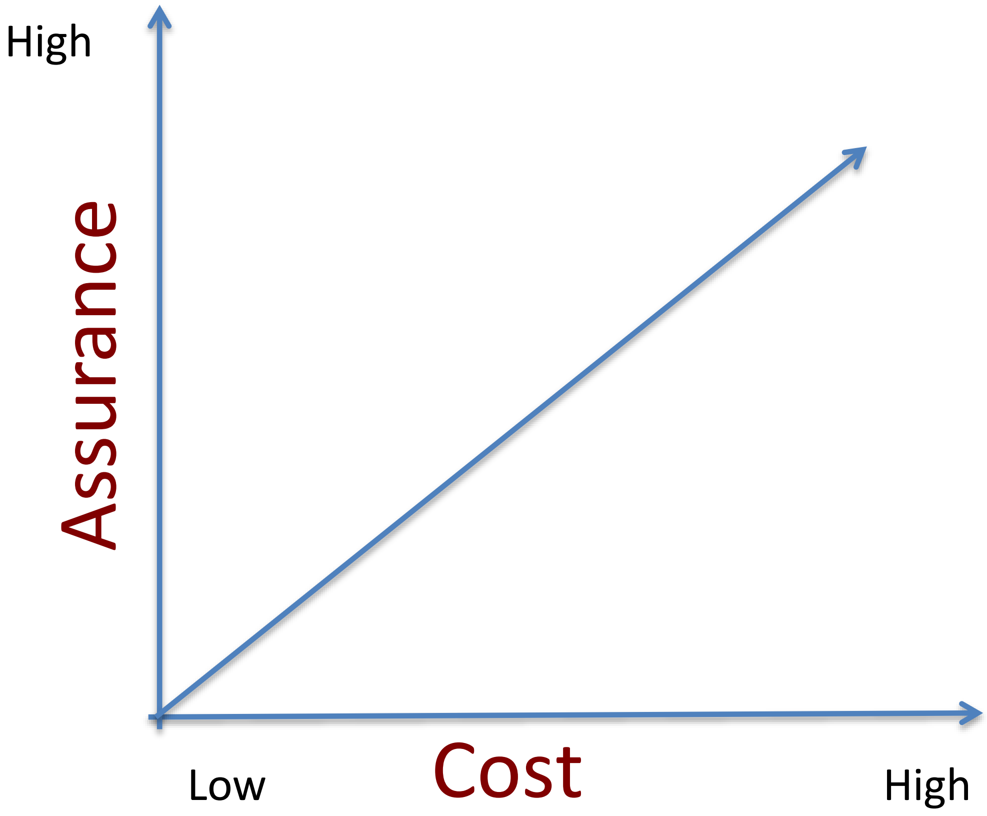
↓

Significant increase in the number of individuals and organizations who "touch" a product

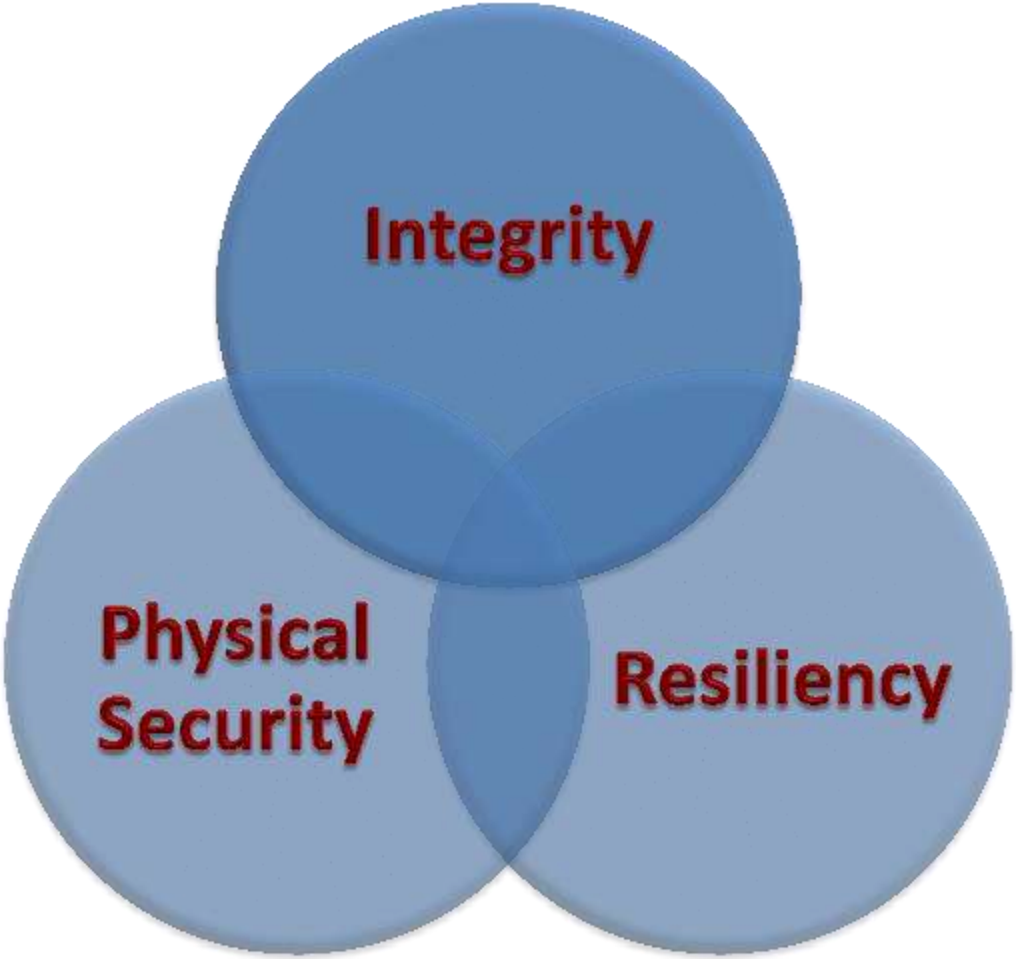
=

Lack of visibility, understanding and control to enable risk management.

COTS vs. Custom



ICT Supply Chain Assurance



Changes to Second Draft

- Resources – What are we asking actors to do?
  - Many activities already practiced that address various disciplines, including logistics, security, reliability, safety, quality control, etc.

- Description vs. Prescription
  - What vs. How

Document Structure

- Introduction: Purpose, scope and background
- Overview: Provides a high-level discussion of ICT supply chain challenges, success factors and foundational practices.
- Implementing ICT SCRM: Implementing SCRM provides information on how ICT SCRM considerations can be integrated into the Federal acquisition lifecycle.
- ICT SCRM Practices: 10 key practices for acquires integrators, and suppliers: Programmatic Activities, General Requirements, Technical Implementation Requirements and Validation and Verification Activities.
- Appendix A: Glossary
- Appendix B: Acronyms
- Appendix C: References
- Appendix D: UMD ICT Supply Chain Study: "Assessing SCRM Capabilities and Perspectives of the IT Vendor Community"

Establish a SCRM Capability

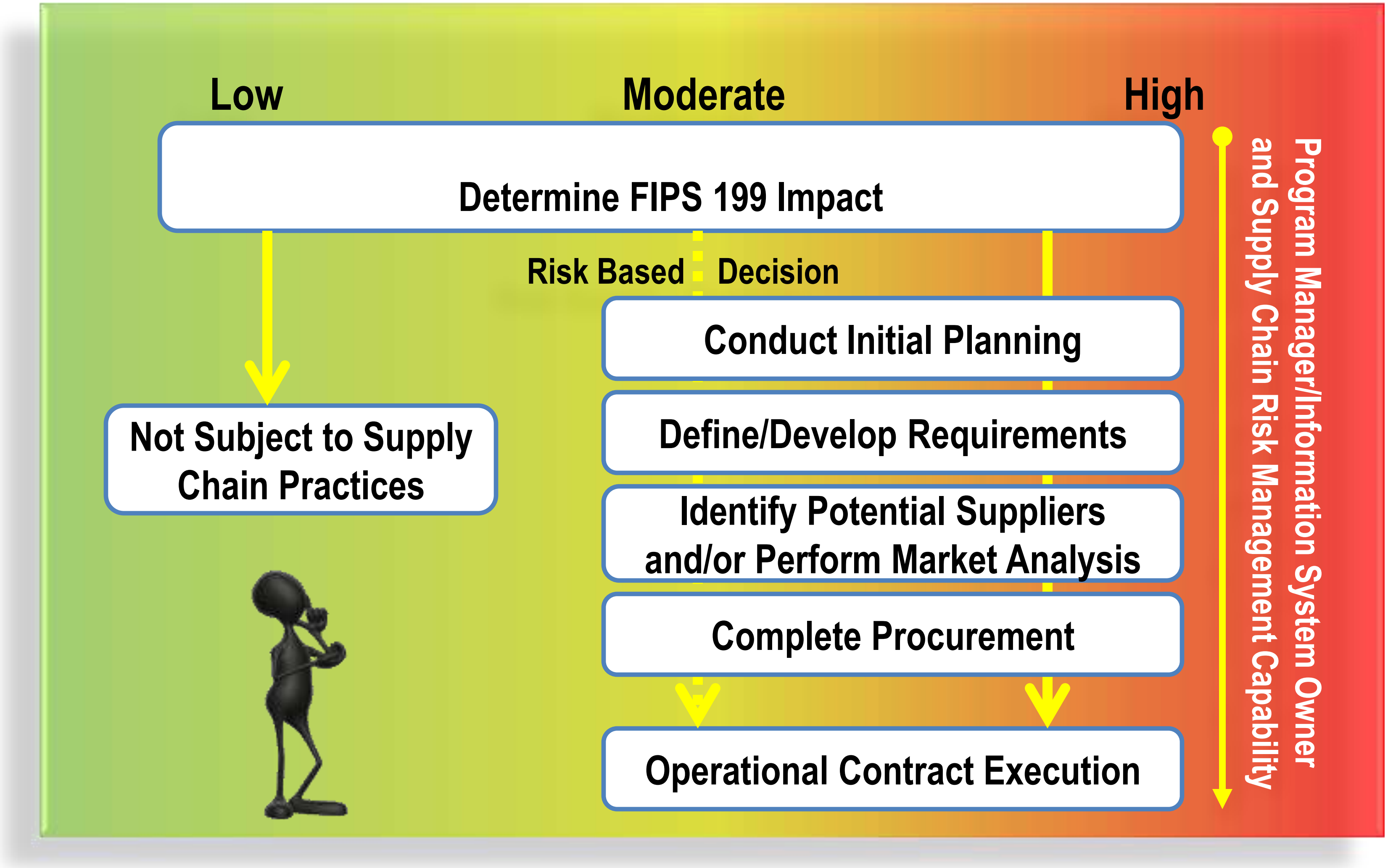
- Ad-hoc or formal team

- Develop policy and procedures
  - Determine who performs requirement analysis, makes risk decisions, prepares procurement related documents, and specifies any specific training requirements.

Implementing ICT SCRM: Roles & Responsibilities

Plan Procurement	Oversee	Oversee	Oversee	Lead	Advise	Lead
Define/Develop Requirements	Oversee	Oversee	Oversee	Lead	Advise	Lead
Identify Potential Suppliers and/or Perform Market Analysis	Oversee	Oversee	Oversee	Advise	Advise	Lead
Complete Procurement	Oversee	Oversee	Lead	Lead	Advise	Lead
Operations and Maintenance	Oversee	Oversee	Oversee	Advise	Advise	Lead
PROCESS→	**Risk Executive (Function)**	**Chief Information Officer (CIO)**	**Chief Information Security Officer (CISO)**	**Contracting Officer(CO)**	**Legal**	**Mission Business Owner**

Integrated SCRM Procurement Process



Low

Moderate

High

Determine FIPS 199 Impact

Risk Based Decision

Not Subject to Supply Chain Practices

Conduct Initial Planning

Define/Develop Requirements

Identify Potential Suppliers and/or Perform Market Analysis

Complete Procurement

Operational Contract Execution

Program Manager/Information System Owner and Supply Chain Risk Management Capability

SCRM Practices (Notional)

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.

ICT SCRM Practices (Notional)

- 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

Information Needed

- The practicality, feasibility, cost, challenges, and successes
- How to differentiate more and less critical components in addition to the information described in Draft NIST SP 800-53 Revision 4 SA-14 and SA-15
- Threat models or other relevant information for use in developing an ICT supply chain risk assessment matrix and threat scenarios
- The information described in this document that is already collected in response to other legislation, regulations, and standards.

Activities and Dates

- Risk Assessment Matrix and Threat Scenarios

- Public Workshop: July 11-12, 2012 (possible topics)
  - Foundation (lexicon, scope, etc)
  - Practices (Practicality/feasibility in terms of cost and implementation)
  - Tools and Technology
  - Research (current and needed)

Thank you

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

http://scrm.nist.gov