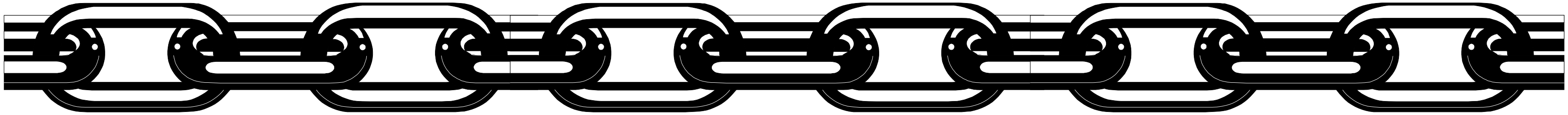
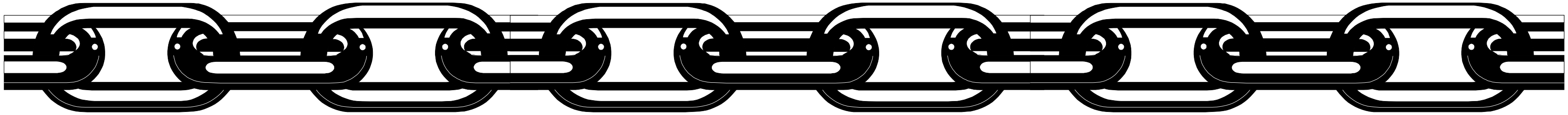


Piloting Supply Chain Risk Management Practices for Federal Information Systems

2 March 2011

Jon Boyens
Computer Security Division
Information Technology Laboratory

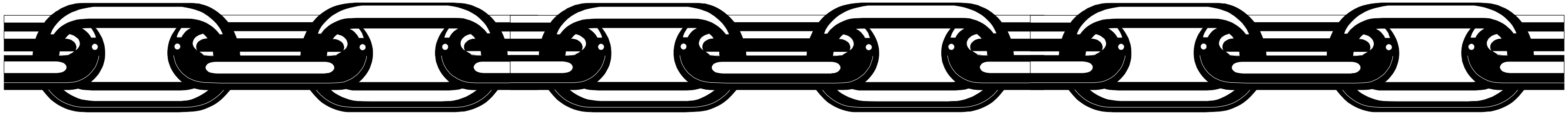
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY



What is NISTIR 7622 ?

NIST Interagency or Internal Reports (NISTIRs):

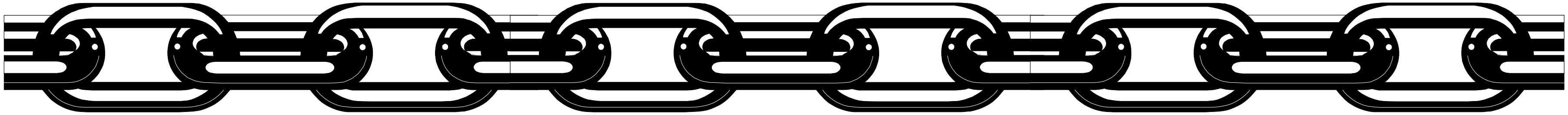
- Describes research of a technical nature of interest to a specialized audience.
- Includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment).
- May also report results of NIST projects of transitory or limited interest, including those that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



What is NISTIR 7622 ? (con't)

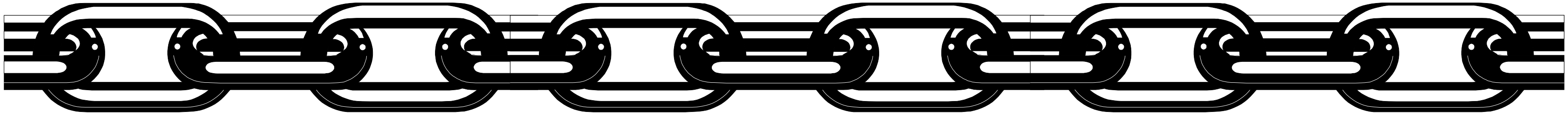
- Guidance and recommended risk mitigating strategies for the acquiring federal agency only.
  - NISTIR 7622 is not meant to be comprehensive.

- A set of practices to be used for HIGH-IMPACT LEVEL SYSTEMS (FIPS 199) – medium-impact dependent upon risk management approach.



NISTIR 7622 – What It Provides

- Roles and responsibilities.
- Best practices to augment baseline security controls.
- Helps determine which procurements should consider supply chain risk.
- Describes how to work with a supply chain risk management team to mitigate risk through careful security specifications and contract requirement.
- Looks at risks in the full lifecycle of COTS & GOTS.
  - Design, development, acquisition, system integration, system operation, and disposal.
- Serves a broad audience.
  - System owners, acquisition staff, system security personnel, system engineers, etc.

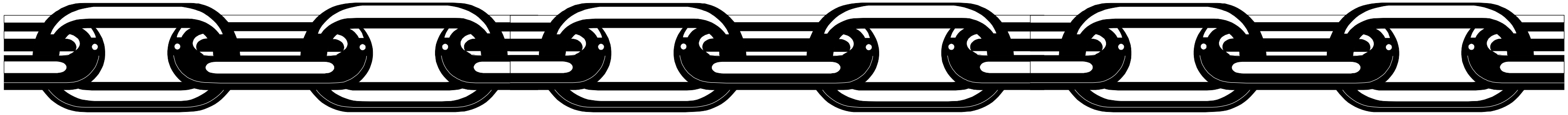


NISTIR 7622 – What It Does NOT Do

- NISTIR 7622 DOES NOT Provide:
  - Specific contract language.
  - Threat assessments.
  - A complete list of supply chain assurance methods and techniques that mitigate supply chain threats.

SCRM Terms

- Supply Chain – The set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization’s customers.
  - *+17 definition based on participants, systems, functions, processes, objectives, etc.*
- Element – Includes: COTS and GOTS (software, hardware and firmware) and synonymous with components, devices, products, systems, and materials. A part of a system. Synonym for component. An element may be implemented by products or services.
- Acquirer - For this document, the acquirer is always a government agency (including those agencies taking on the role of integrator).
- Integrator – A third-party organization that specializes in combining products/elements of several suppliers to produce elements (information systems).
- Supplier – Third-party organization providing individual elements. *Synonymous with vendor and manufacturer; also applies to maintenance/disposal service providers.*



Document Structure

1. Introduction
2. Implementing Supply Chain Risk Management
3. Supply Chain Risk Management Practices

Appendix A – Glossary

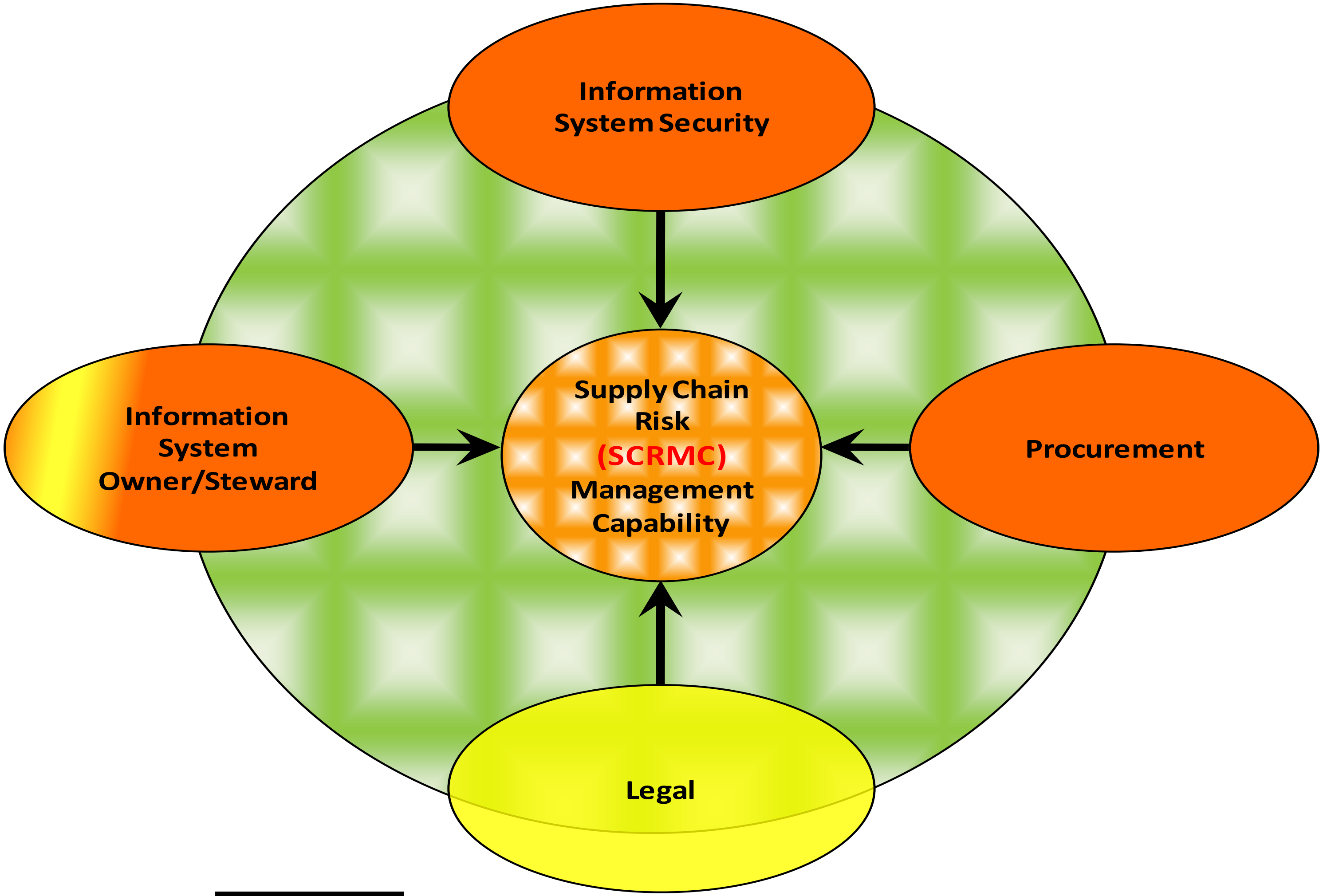
Appendix B – Acronyms

Appendix C – References

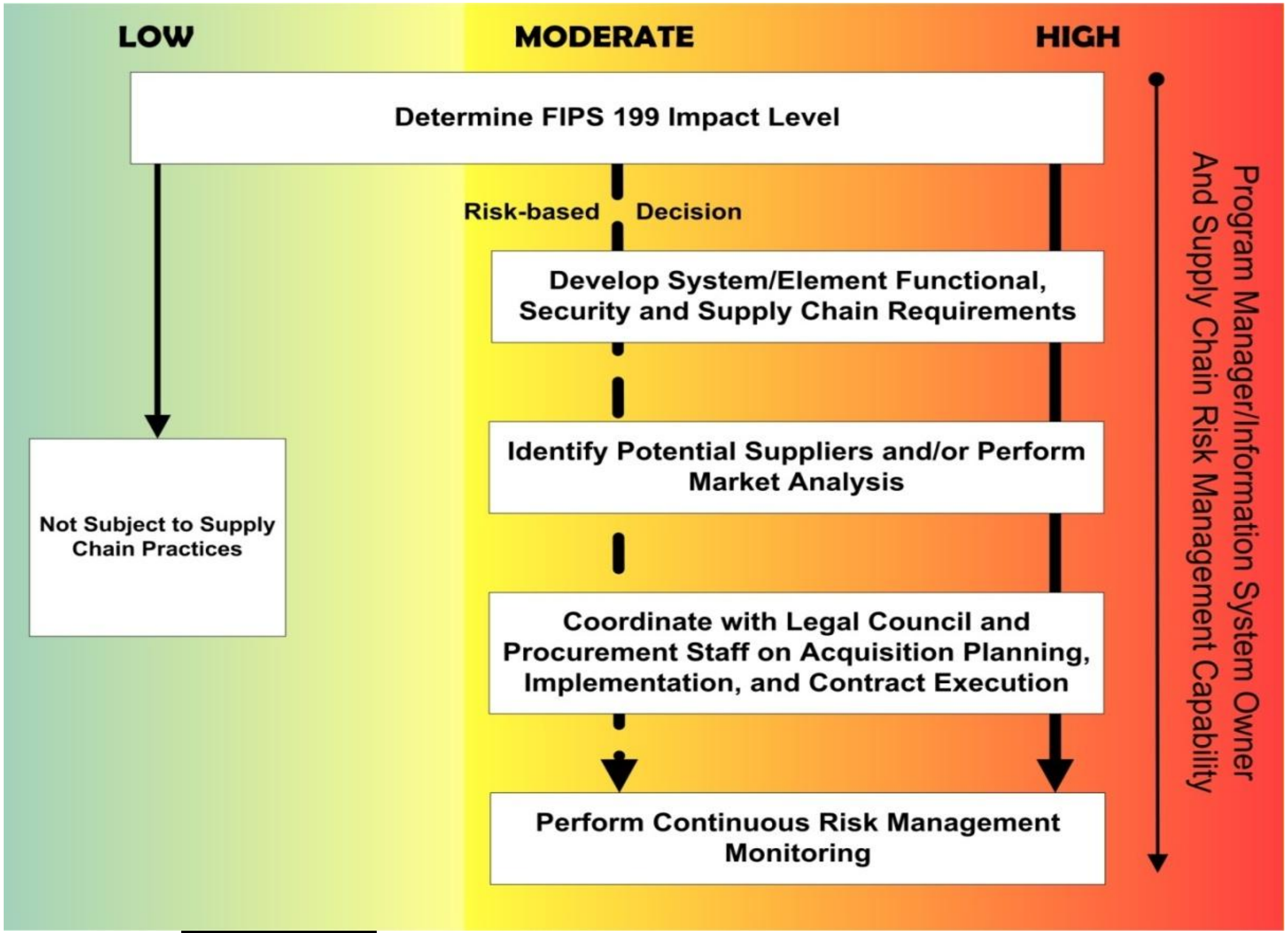
Establish a SCRM Capability

- 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.

Implementation – SCRM Approach

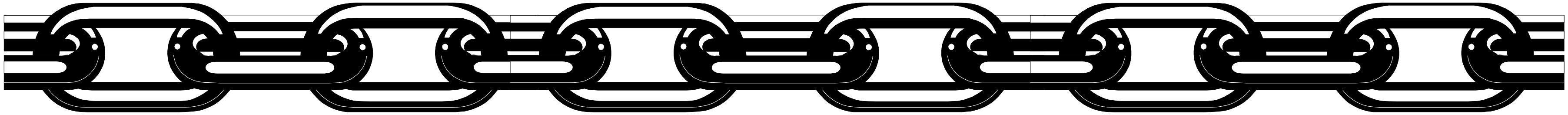

Information System Security
Information System Owner/Steward
Supply Chain Risk (SCRMC) Management Capability
Procurement
Legal

Integrated SCRM Procurement Process


LOW
MODERATE
HIGH
Determine FIPS 199 Impact Level
Risk-based
Decision
Develop System/Element Functional, Security and Supply Chain Requirements
Identify Potential Suppliers and/or Perform Market Analysis
Coordinate with Legal Council and Procurement Staff on Acquisition Planning, Implementation, and Contract Execution
Perform Continuous Risk Management Monitoring
Not Subject to Supply Chain Practices
Program Manager/Information System Owner
And Supply Chain Risk Management Capability

Supply Chain Practices

- Topic areas include:
  - Procurement
  - Design/Development
  - Testing
  - Operational
  - Personnel
- 21 varying practices:
  - Acquirer: Programmatic and validation activities
  - Supplier or integrator: General, technical and validation requirements.
  - Assumes the organization has a developed and implemented robust information security program.
  - Cover complete system development life cycle.

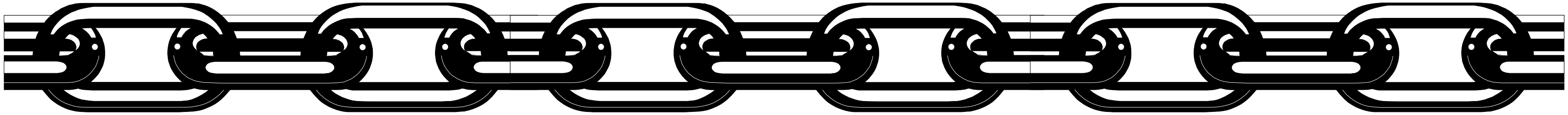


Supply Chain Risk Management Practices

3.1: Maximize Acquirer’s Visibility into Integrators and Suppliers
3.2: Protect Confidentiality of Element Uses
3.3: Incorporate Supply Chain Assurance in Requirements
3.4: Select Trustworthy Elements
3.5: Enable Diversity
3.6: Identify and Protect Critical Processes and Elements
3.7: Use Defensive Design
3.8: Protect the Supply Chain Environment
3.9: Configure Elements to Limit Access and Exposure
3.10: Formalize Service/Maintenance
3.11: Test Throughout the System Development Lifecycle
3.12: Manage Configuration
3.13: Consider Personnel in the Supply Chain
3.14: Promote Awareness, Educate, and Train Personnel on Supply Chain Risk
3.15: Harden Supply Chain Delivery Mechanisms
3.16: Protect/Monitor/Audit Operational System
3.17: Negotiate Requirements Changes
3.18: Manage Supply Chain Vulnerabilities
3.19: Reduce Supply Chain Risks during Software Updates and Patches
3.20: Respond to Supply Chain Incidents
3.21: Reduce Supply Chain Risks During Disposal

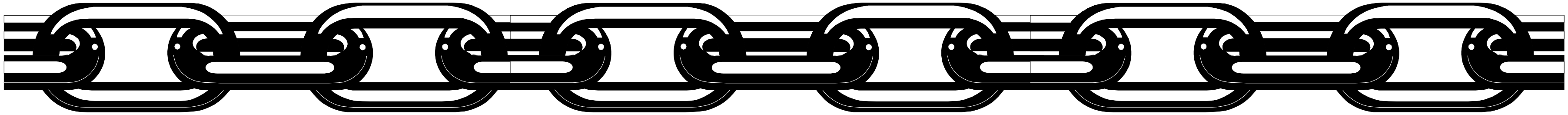
NISTIR 7622: Current Work

- Updating draft based on public comments
  - Define and explain problem better.
    - History, issues, purpose, what IS SCRM?
  - What are we actually asking actors to do?
    - Resources: many activities already practiced that address various disciplines, including logistics, security, reliability, safety, quality control, etc.
    - Roles and responsibilities.
  - Implementation guidance.
    - Due diligence/caveat emptor.
  - Best practices – specify foundational practices.
  - Use cases
  - Reference documentation – NIST 800 53, FIPS 199, etc.



NISTIR 7622: Future Work

- Develop a new Options Plan for future supply chain work.
- Continuing to incorporate public comments in the Draft NIST IR 7622.
- Continue to incorporate feedback from ongoing pilots in the Draft NIST IR 7622.
- Investigate the possibility of utilizing various supply chain tools to help manage relationships.
- Continue to meet with private and public sector stakeholders to obtain additional input into Draft NIST IR 7622.
- Workshop – contingent upon budget and availability of funds.
- Open to suggestions.



Thank you

Contact: Jon Boyens

jon.boyens@nist.gov