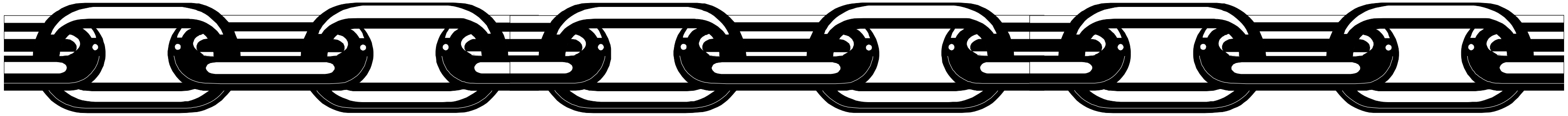
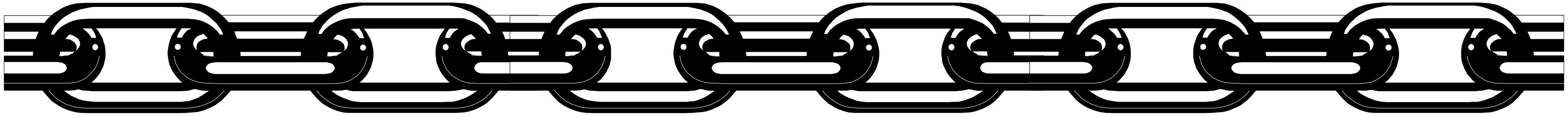


Piloting Supply Chain Risk Management Practices for Federal Information Systems

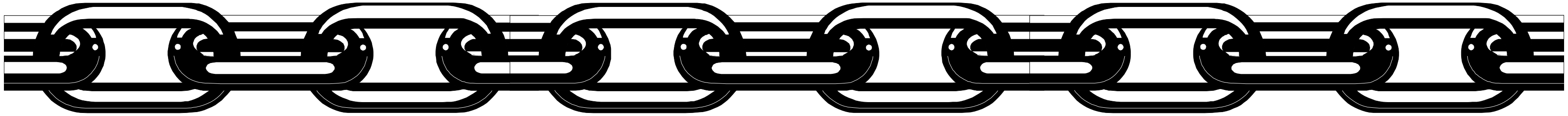
Jon Boyens
Computer Security Division
Information Technology Laboratory



What is NISTIR 7622 ?

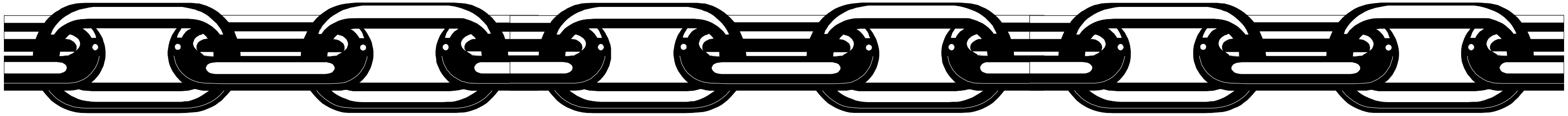
NIST Interagency or Internal Reports (NISTIRs):

- 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.



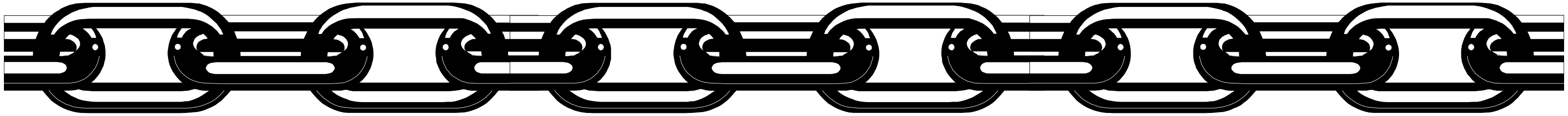
What is NISTIR 7622 ? (con't)

- Guidance and recommended risk mitigating strategies for the acquiring federal agency only.
- Component of greater Comprehensive National Cybersecurity Initiative (CNCI) 11 effort .
  - NISTIR 7622 is not meant to be comprehensive.
  - Organizations to pilot activities and provide feedback on practicality, feasibility, cost, challenges and successes.
- A set of practices to be used for HIGH-IMPACT LEVEL SYSTEMS (FIPS 199) – medium-impact dependent upon risk management approach.



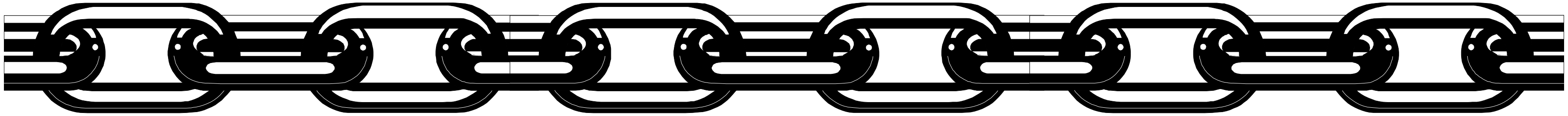
NISTIR 7622 – What It Does

- Provides roles and responsibilities.
- Provides a list of best practices to augment baseline security controls.
- Describes how to 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.



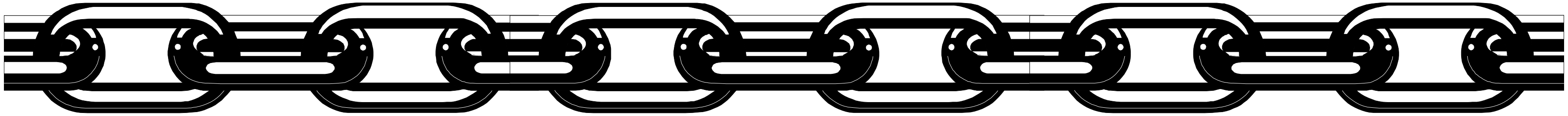
NISTIR 7622 – What It Does NOT Do

- 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.



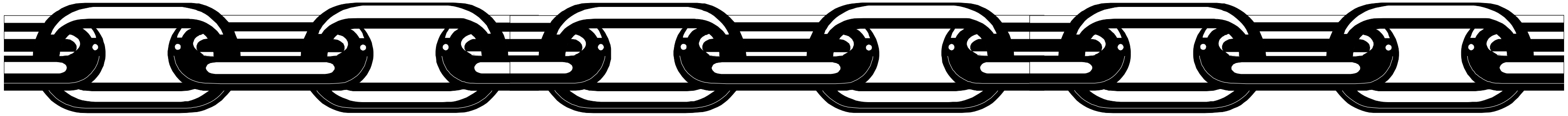
Background

- CNCI 11: Develop Multi-Pronged Approach for Global Supply Chain Risk Management (SCRM)
  - Lifecycle Processes and Standards Working Group
    - Provide US Government with robust toolset of supply chain methods and techniques.
    - Develop guidance for civilian agencies on implementing supply chain risk mitigation strategies.
    - Test existing and proposed guidance through pilots in FY10 and FY11.
    - Collaborate with organizations and industry on developing supply chain standards and practices.



Collaboration

- INCITS/CS1 TAG ICT SCRM Ad Hoc.
- IT and Telecom Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs).
- Federal CIO Council: Information Security and Identity Management Committee.
- University of Maryland Robert H. Smith School of Business.
- Needs to grow.



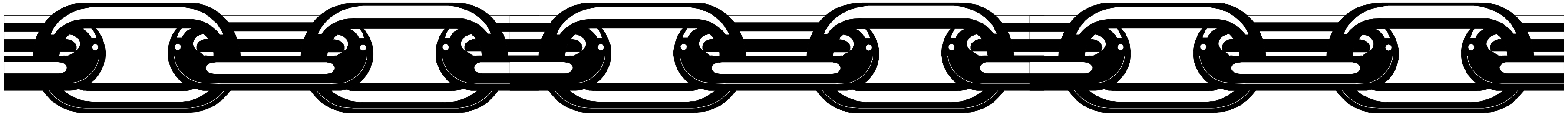
Document Structure

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

Appendix A – Glossary

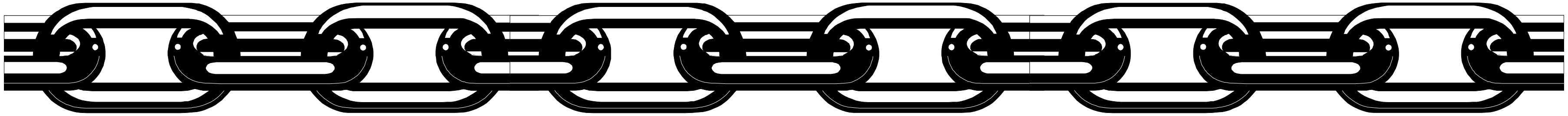
Appendix B – Acronyms

Appendix C – References



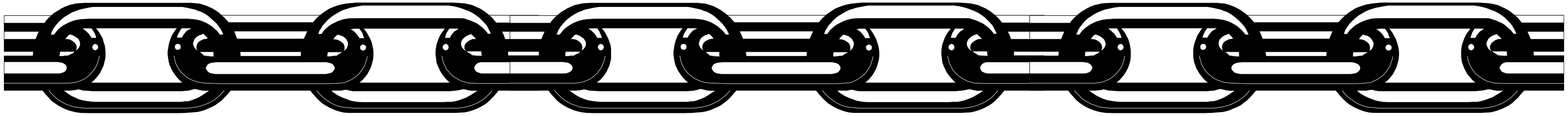
SCRM Terms

- 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.
- 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.*



Section 2: Implementing Supply Chain Risk Management

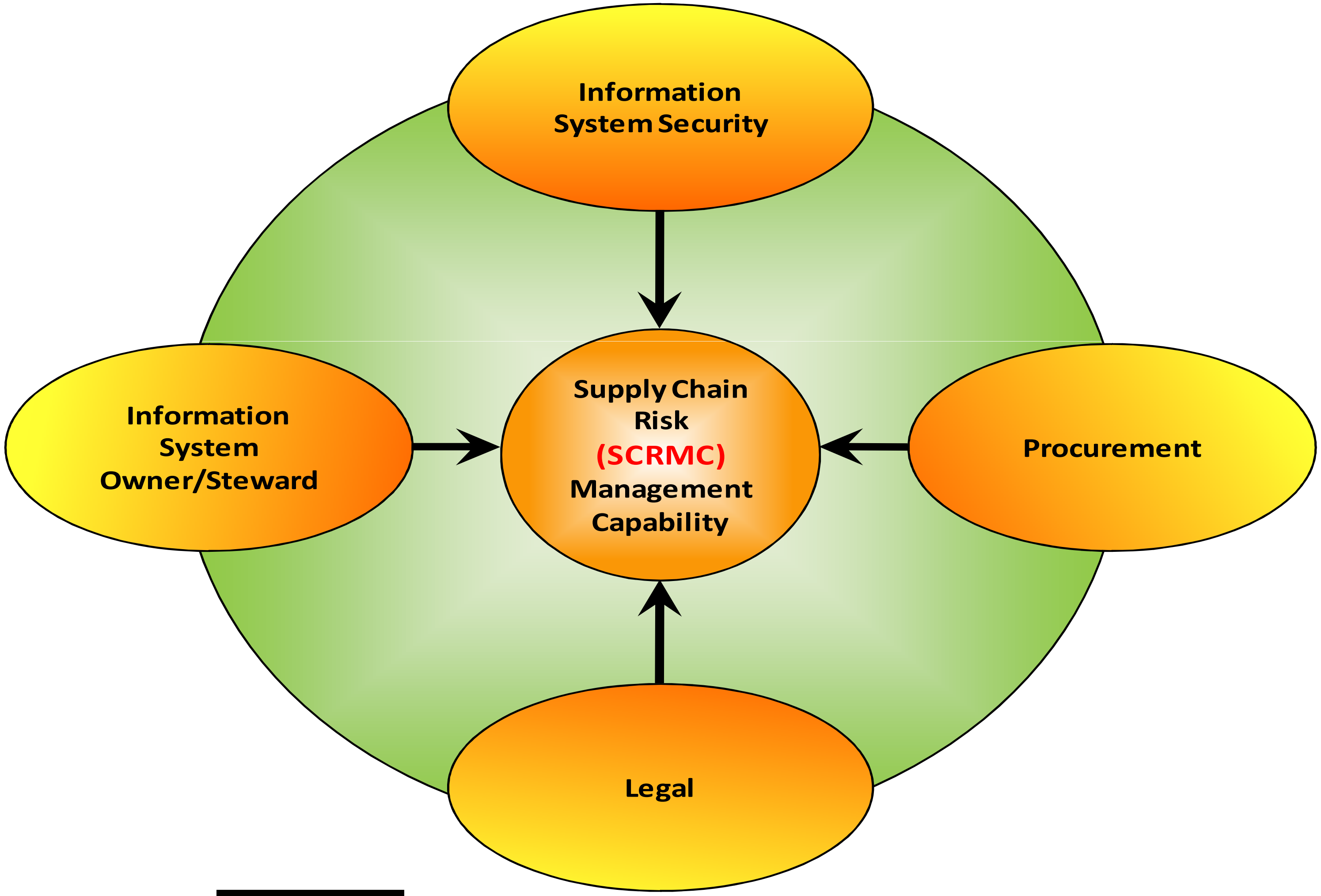
- Establish a Supply Chain Risk Management Capability (SCRMC)
- Assign Roles and Responsibilities
- Integrate SCRM Procurement Processes

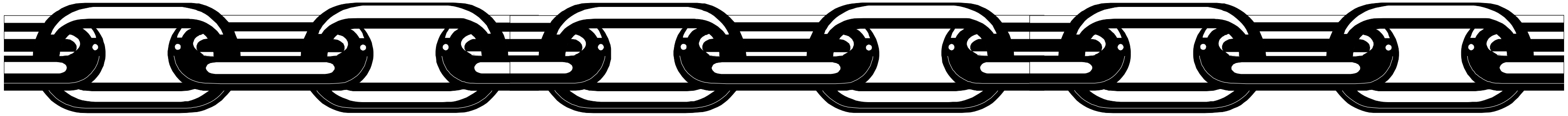


Establish a SCRM Capability

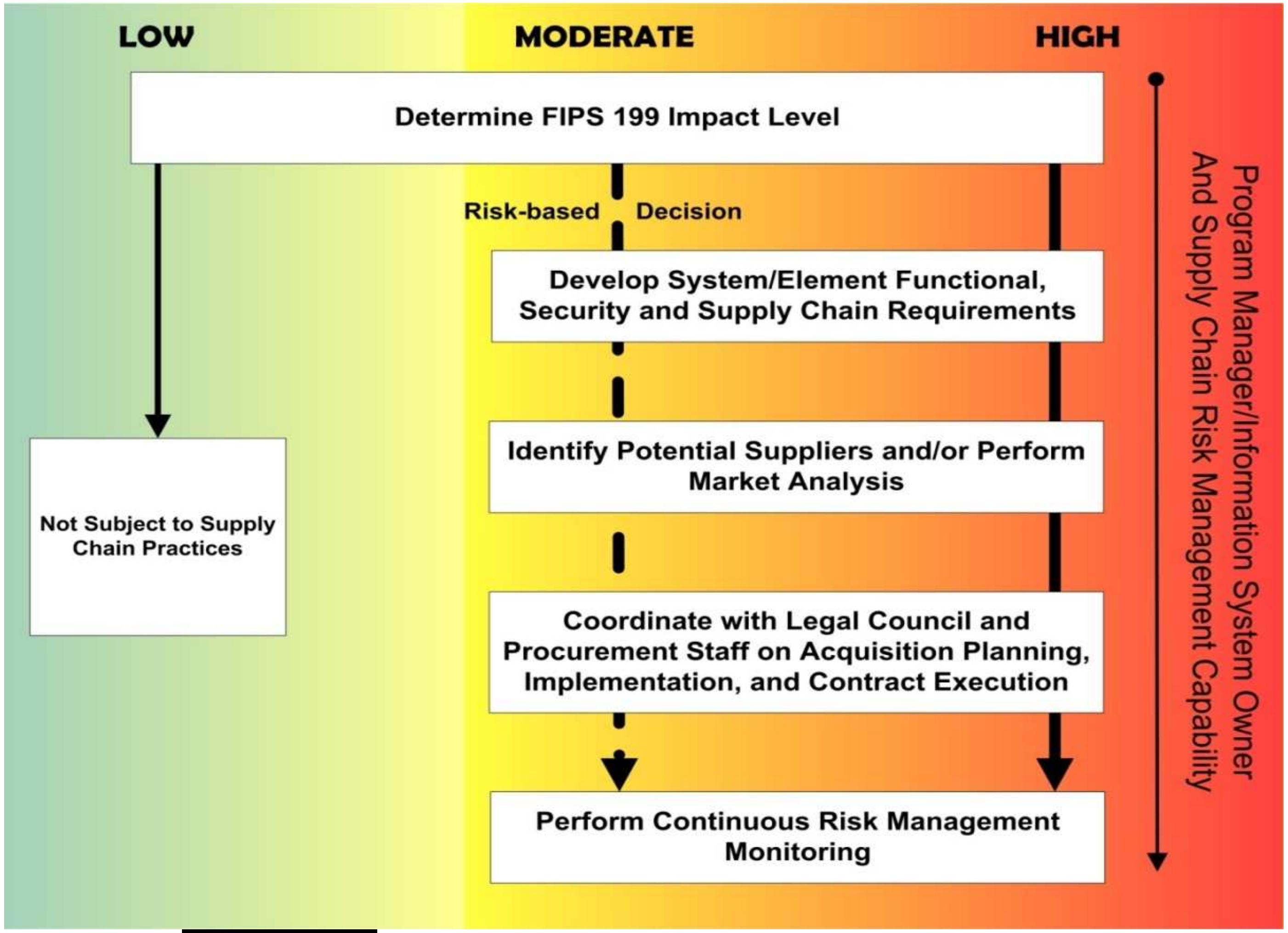
- Ad-hoc or formal team.
- Develop policy and procedures.
  - Determine who performs requirement analysis, makes risk decisions, prepares procurement related documents, and specifies any specific training requirements.

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

Not Subject to Supply Chain Practices

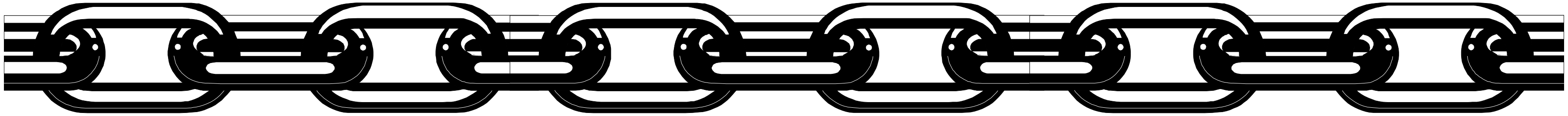
Develop System/Element Functional, Security and Supply Chain Requirements

Identify Potential Suppliers and/or Perform Market Analysis

Coordinate with Legal Council and Procurement Staff on Acquisition Planning, Implementation, and Contract Execution

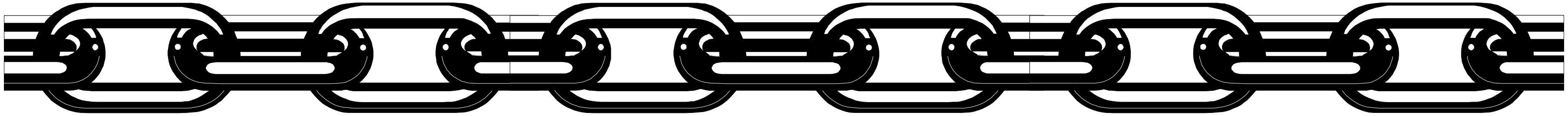
Perform Continuous Risk Management Monitoring

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



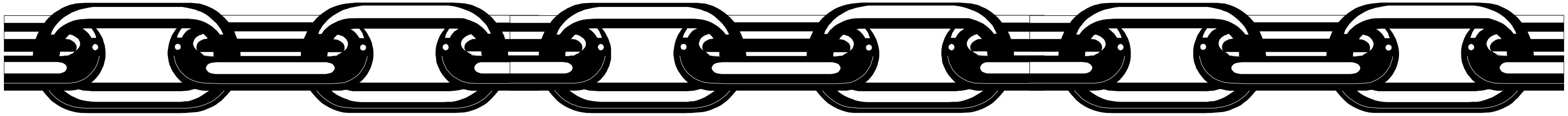
Step 1: Determine Supply Chain Risk Threshold

- FIPS 199 High Impact System
- NIST Special Publication 800-53 Rev. 3 Security Control: SA-12 Supply Chain Protection
  - Control: The organization protects against supply chain threats by employing: [Assignment: organization-defined list of measures to protect against supply chain threats] as part of a comprehensive, defense-in-breadth information security strategy.
  - Supplemental Guidance: A defense-in-breadth approach helps to protect information systems (including the information technology elements that compose those systems) throughout the system development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk.



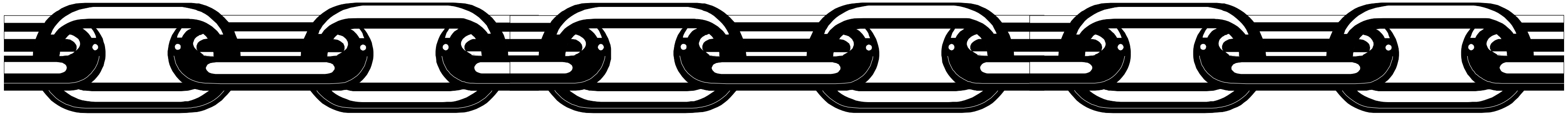
Step 2: Develop Requirements

- Identify critical elements, processes, systems, and information across the program.
- Determine appropriate level of risk.
- Review all data gathered during the pre-solicitation.
- Obtain any additional information.
- Consider a procurement strategy.
- Develop a Statement of Work (SOW).



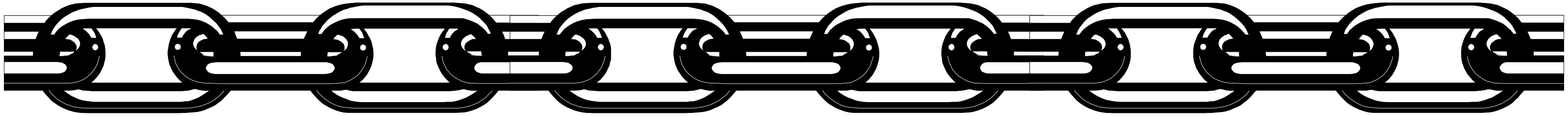
Step 3: Identify Potential Suppliers

- Post a RFI and/or “sources sought” notification.
- Due Diligence
  - Gather information from open-sources.
  - Conduct research and analysis.



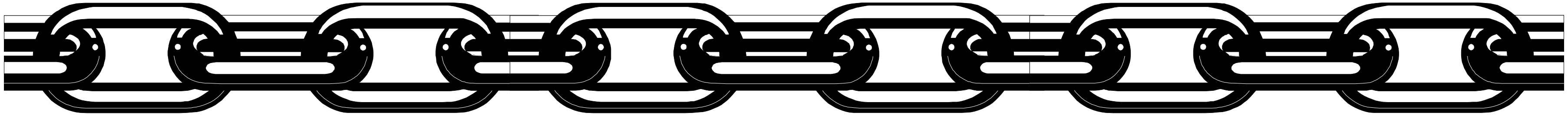
Step 4: Coordinate Acquisition Plan and Contract Execution

- Develop an Acquisition Plan
  - List of potential sources of suppliers.
  - Description of how competition will be sought.
  - Description of various contacting considerations.
  - Strategies for mitigating supply chain risk.
- Disclose any legal issues.
- Perform technical review.
- Select supplier.



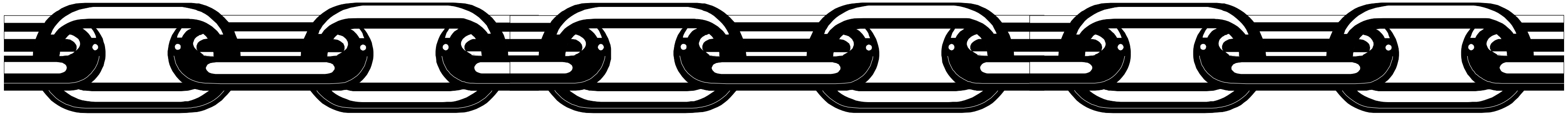
Step 5: Perform Continuous Monitoring

- Record lessons learned.
- Monitor and periodically reevaluate changes in risk, suppliers, operational environment, and usage.
- Replacement components and maintenance should be reviewed for supply chain risk.



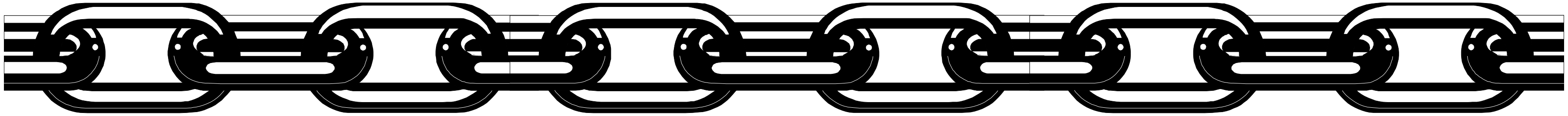
Supply Chain Practices

- 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.



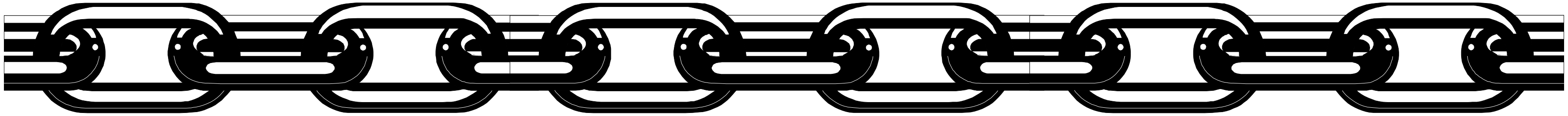
Supply Chain Risk Management Practices

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



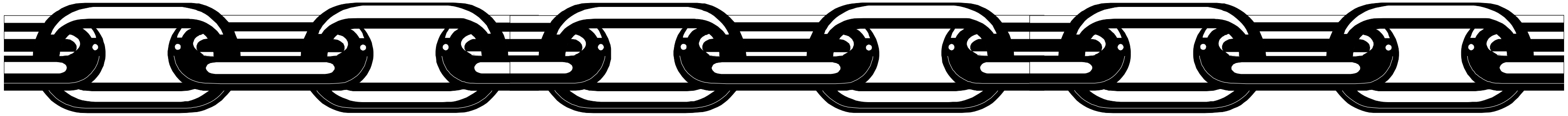
NISTIR 7622: Future Work

- Additional industry and Federal agency input and collaboration.
- Definitions:
  - Many definitions of supply chain based on participants, processes, functions, systems, goals, etc. etc.
- Implementation guidance and tools.
- More specific guidance on pilot feedback.
- Open to suggestions.



NISTIR 7622: Timeline

- Draft NIST Interagency Report (NIST IR) 7622 *Piloting Supply Chain Risk Management Practices for Federal Information Systems:*
  - First Public Draft – June, 2010
  - Second Draft – September 2011
  - Workshop – October 2011
  - Final Release – 2011
- Future NIST Special Publication
  - TBD



Thank you

Contacts:

Jon Boyens - jon.boyens@nist.gov

Nadya Bartol – bartol_nadya@bah.com

Rama S. Moorthy – rama.moorthy@hathasystems.com