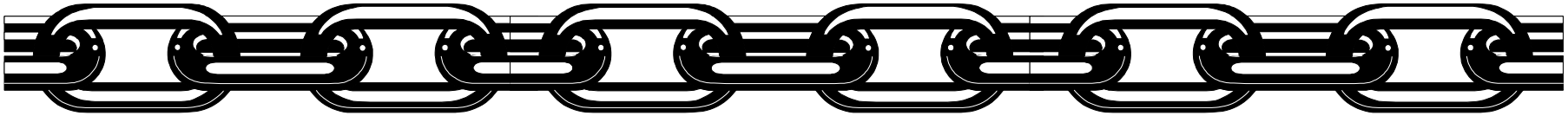
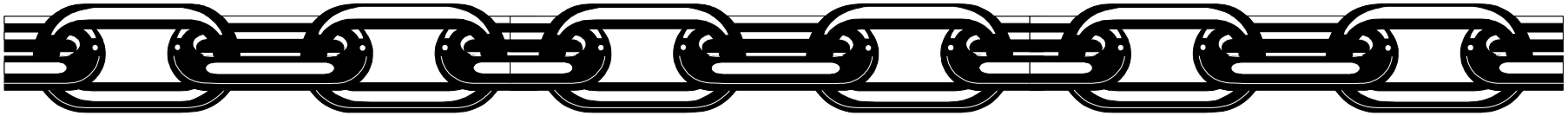


Piloting Supply Chain Risk Management Practices for Federal Information Systems

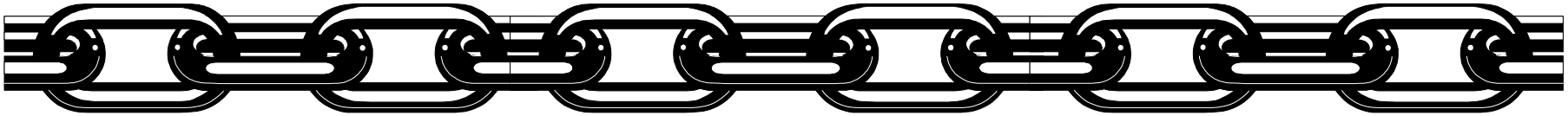
Rama S. Moorthy
In support of
Marianne Swanson
National Institute of Standards and Technology (NIST)



Lifecycle Processes and Standards Working Group

- 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

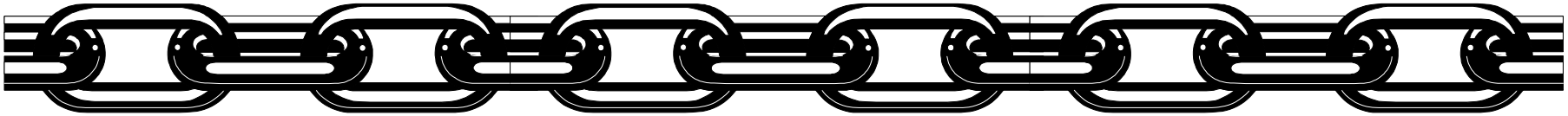
NIST



Guidance

- Draft NIST Inter-Agency Report (NISTIR) 7622 *Piloting Supply Chain Risk Management Practices for Federal Information Systems*
- Future NIST Special Publication

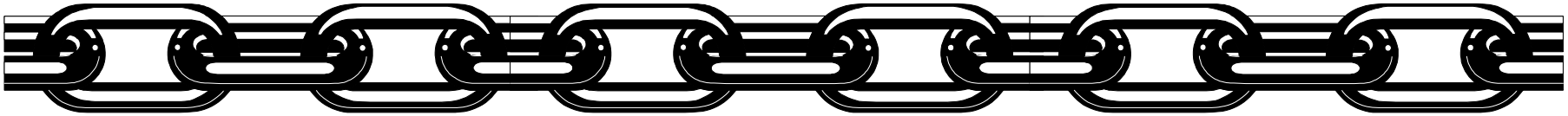
NIST



Collaboration

- ISO CS-1 Global Supply Chain Risk Management Ad Hoc Meetings
- IT and Telecom Sector Coordinating Councils (SCCs) and Government Coordinating Councils GCCs)
- Federal CIO Council: Information Security and Identity Management Committee

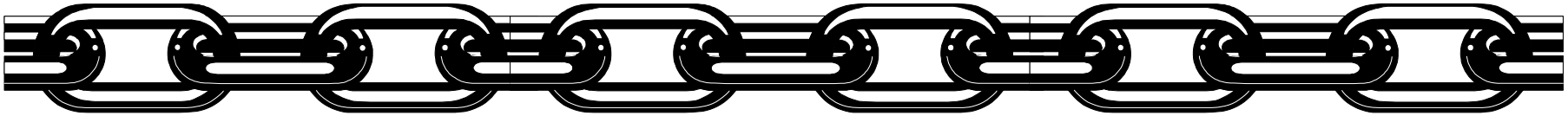
NIST



Implementing Supply Chain Risk Management

- Establish a Supply Chain Risk Management Capability (SCRMC)
- Roles and Responsibilities
- Integrated SCRM lifecycle Procurement Process

NIST

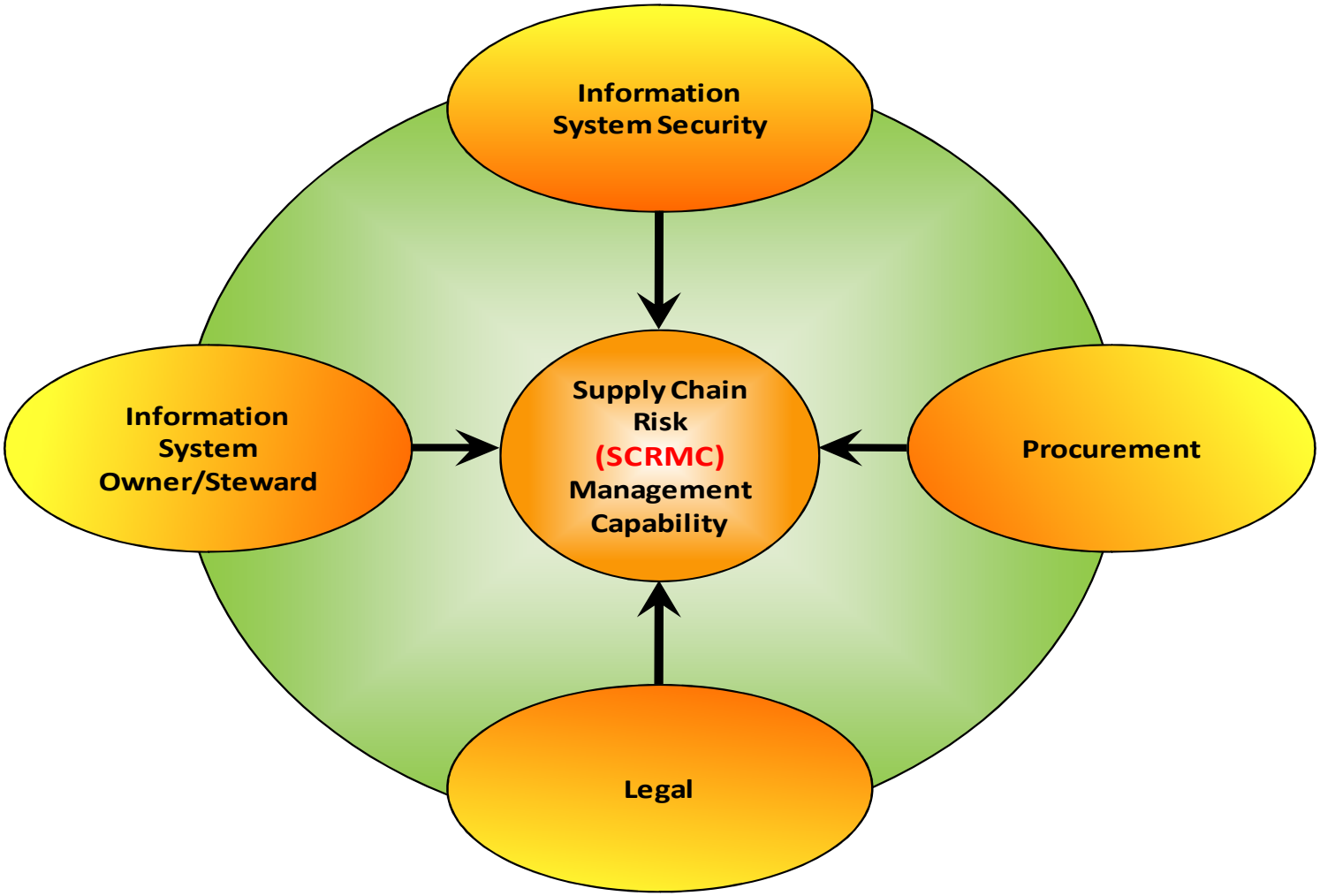


SCRM Terms

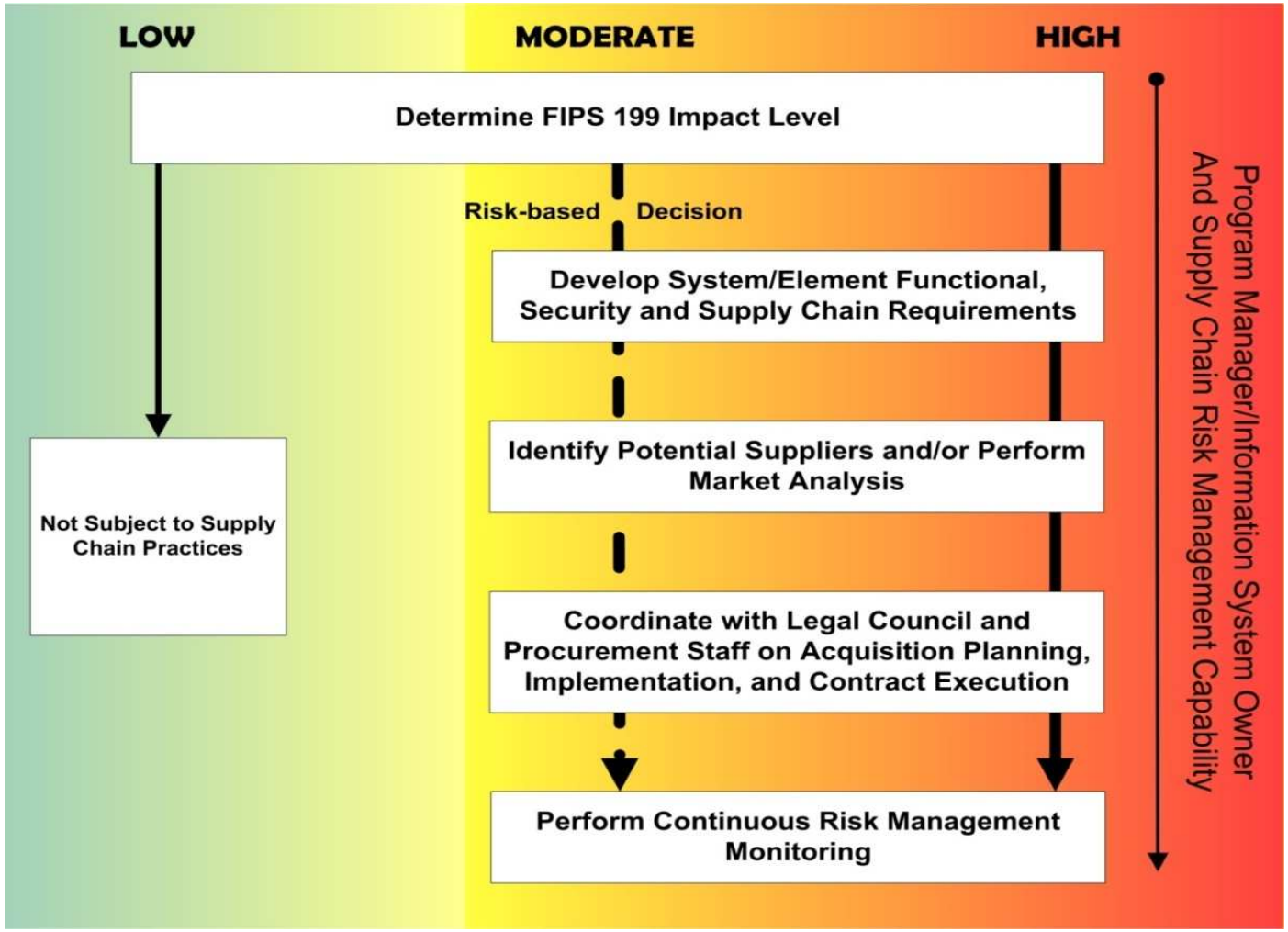
- Supply Chain – *Set of organizations, people, activities, information, and resources for creating and moving a product/elements or service (including sub-elements) from suppliers through to an organization's customers.*
- Element – *COTS or GOTS software, hardware and firmware and is synonymous with components, devices, products, systems, and materials.*
- Supplier – *An organization that produces elements and provides them to an integrator to be integrated into the overall system; it is synonymous with vendor and manufacturer. It also applies to maintenance/disposal service providers.*
- Integrator – *A third party organization that specializes in combining products/elements of several suppliers to produce elements (information systems.)*
- *Acquirer -*

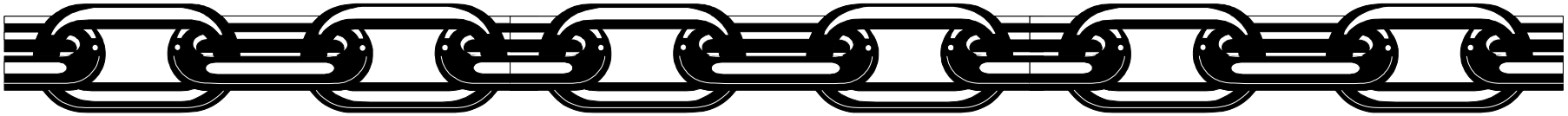
NIST

SCRM Approach



Integrated SCRM Procurement Process

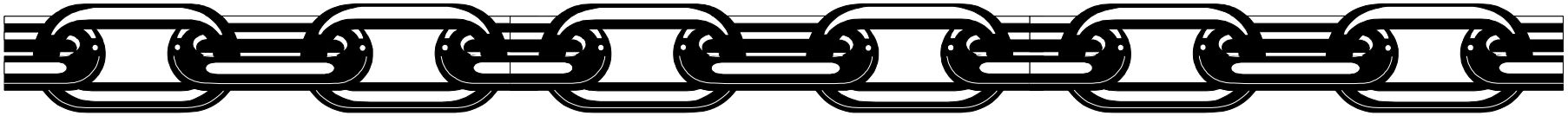




Supply Chain Risk Management Practices

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 Testing

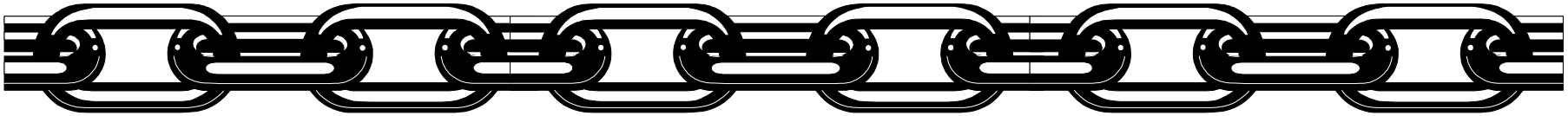
NIST



Supply Chain Risk Management Practices (cont'd)

- 3.12 Configuration Management
- 3.13: Personnel Considerations 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 SC Risks during Software Updates and Patches
- 3.20: Supply Chain Incident Response
- 3.21: Reduce Supply Chain Risks During Disposal

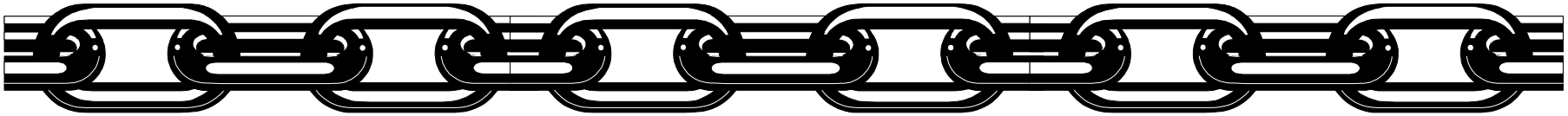
NIST



Schedule of Deliverables

- Draft NIST Inter-Agency Report (NIST IR) 7622 *Piloting Supply Chain Risk Management Practices for Federal Information Systems*
  - First Public Draft – June, 2010
- Future NIST Special Publication
  - First Public Draft – June, 2011

NIST



Thank you

Contacts:

Marianne Swanson - marianne.swanson@nist.gov

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

Nadya Bartol – bartol_nadya@bah.com