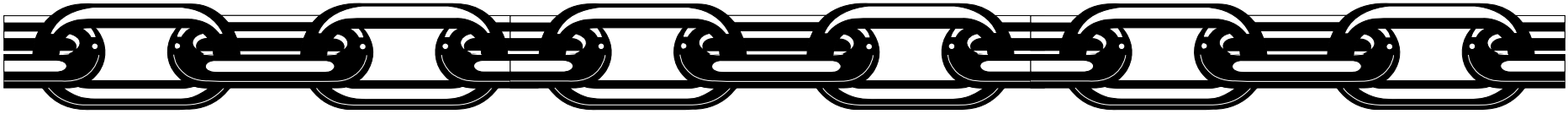


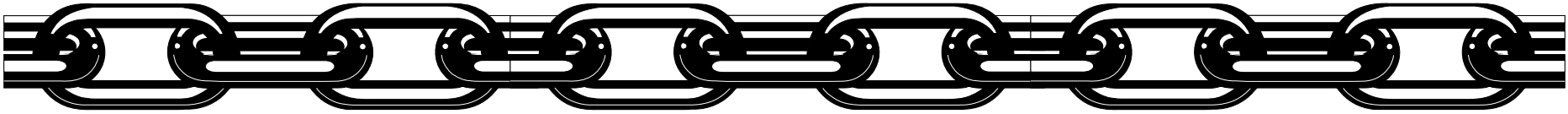
Piloting Supply Chain Risk Management Practices for Federal Information Systems

Marianne Swanson
Computer Security Division
Information Technology Laboratory



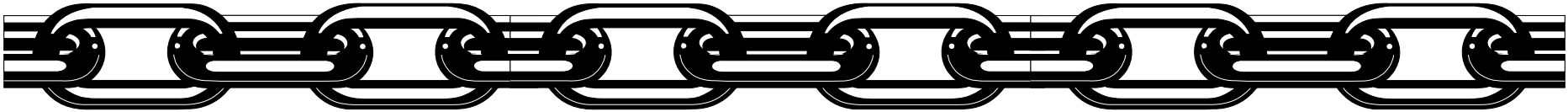
Agenda

- Terms and Background
- Implementing Supply Chain Risk Management
- Supply Chain Risk Management Practices
- Contact Information



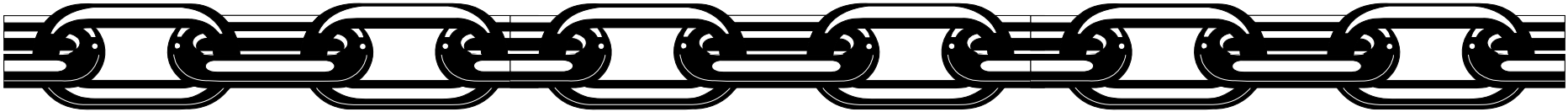
Terms

- *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.*



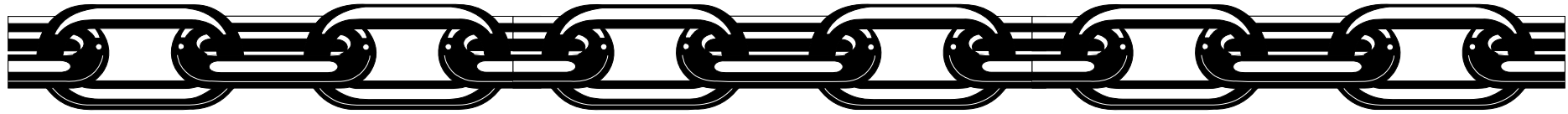
Terms (continued)

- *Supplier – An organization that produces elements and provides them to a customer or 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.)*



Background

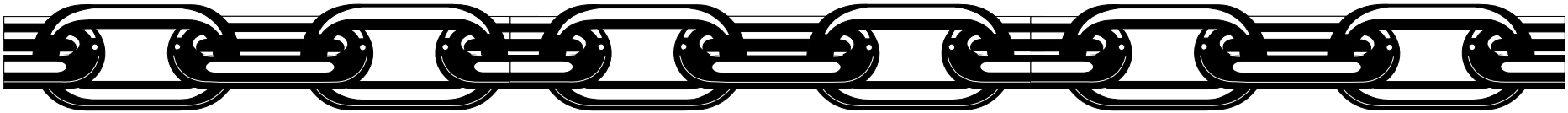
- Comprehensive National Cybersecurity Initiative11: Develop Multi-Pronged Approach for Global Supply Chain Risk Management (SCRM)
- Provide US Government with robust toolset of supply chain methods and techniques
- Multi-tiered Approach:
 - Cost effective procurement related strategies
 - Industry input into supply chain practices and development of international standards
 - Ability to share supply chain threat information



Lifecycle Processes and Standards Working Group

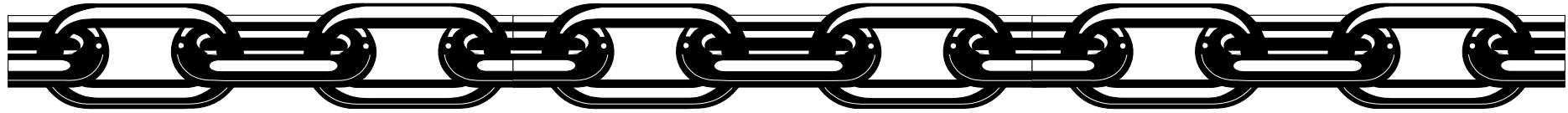
Develop guidance for civilian agencies on implementing supply chain risk mitigation strategies.

- Test existing and proposed guidance during pilots in FY09 and FY10
- Collaborate with organizations and industry on developing supply chain standards and practices



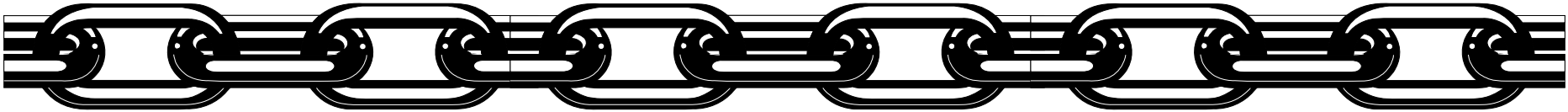
Guidance

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



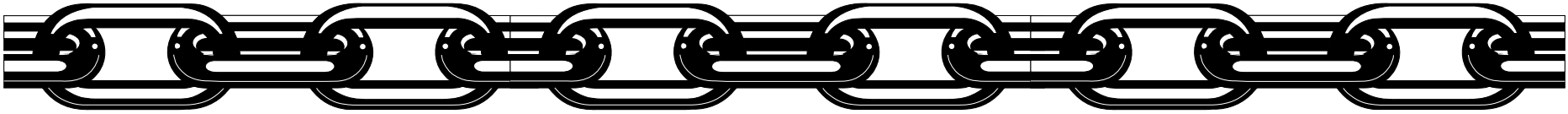
Supply Chain Pilots

- Department of Defense
- Department of Homeland Security
- Piloting of guidance in NISTIR



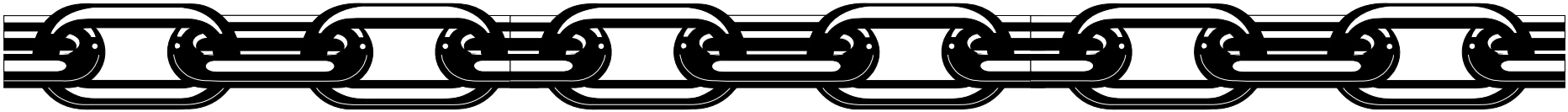
Collaboration

- ISO CS-1 Global Supply Chain Risk Management Ad Hoc Meetings
- IT and Telecom Sector Coordinating Councils (SCCs) and Government Coordinating Councils GCCs)



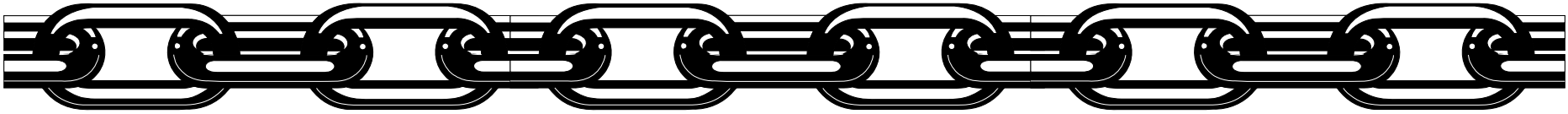
Implementing Supply Chain Risk Management

- Prerequisites for Successful SCRM Implementation
- Establish a Supply Chain Risk Management Capability (SCRMC)
- Roles and Responsibilities
- SCRMC Procurement Process



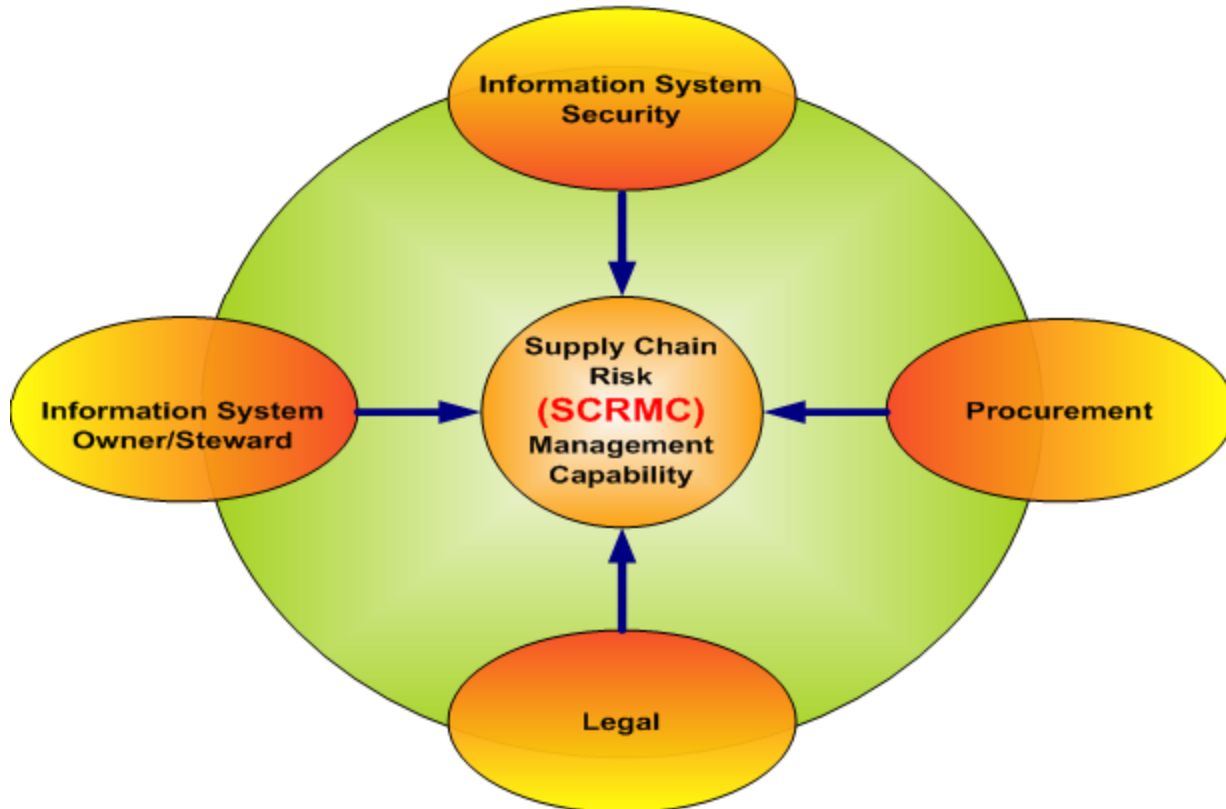
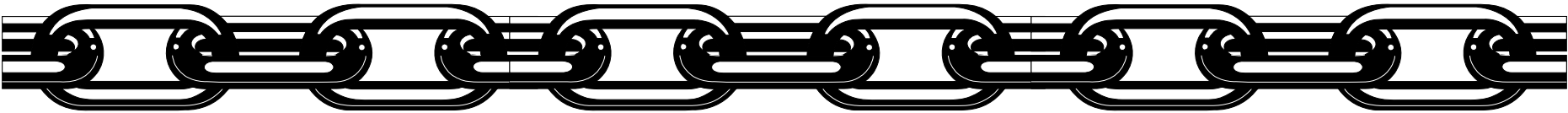
Prerequisites for Successful SCRM Implementation

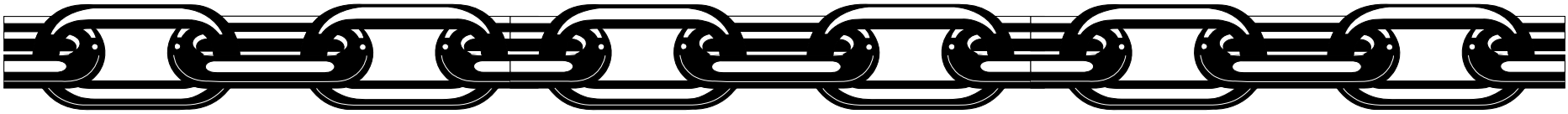
- Integrate information system security requirements from inception
- Ensure funding for information security and SCRM
- Follow consistent, well-documented repeatable system engineering and acquisition processes
- Proper oversight of suppliers
- Actively manage suppliers through Service Level Agreements/contracts
- Fully implement the NIST 800-53 security controls



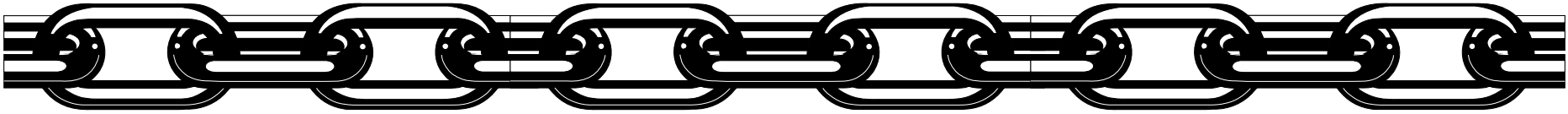
Establish a SCRMC

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



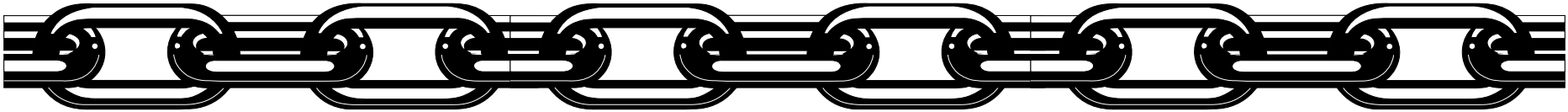


SCRMC Implementation



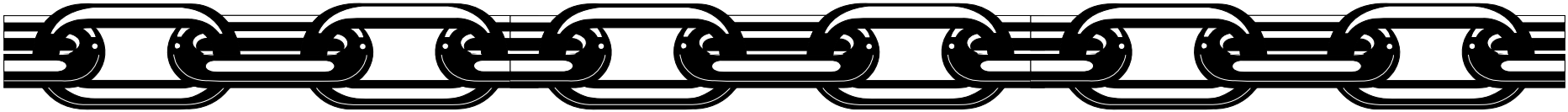
Step 1: Determine Supply Chain Risk Threshold

- FIPS 199 High Impact System
- NIST Special Publication 800-53 Rev. 3 Security Control: SA-12 Supply Chain Protection



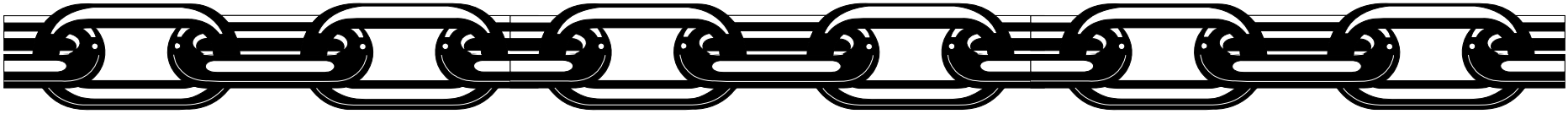
Step 2: Develop Requirements

- 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)



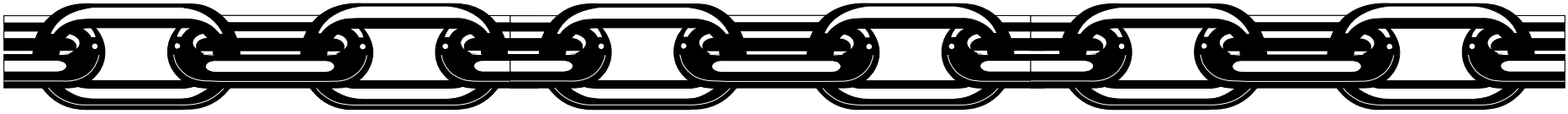
Statement of Work

- Detailed description of the technical, security, and SCRM requirements
- Performance measures
- Evaluation criteria
- Measurement thresholds



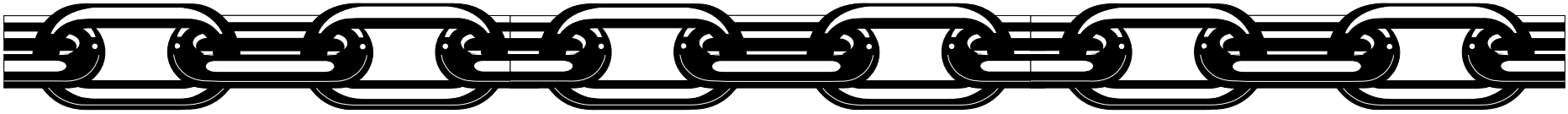
Step 3: Identify Potential Suppliers

- Conduct a market analysis
- Post a “sources sought” notification
- Gather information from open-sources



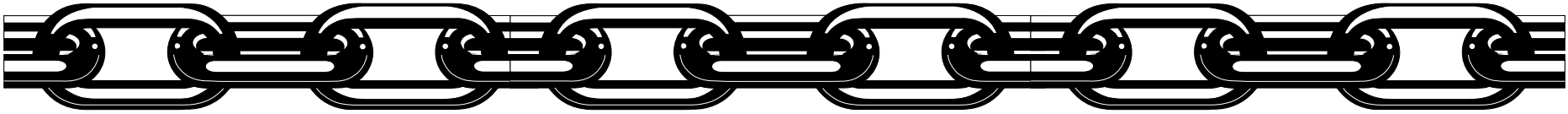
Open Sources

- Central Contractor Registry (CCR)
- Commercial & Government Entity (CAGE)
- Dunn & Bradstreet
- Business Identification Number Cross-reference (BINCS)



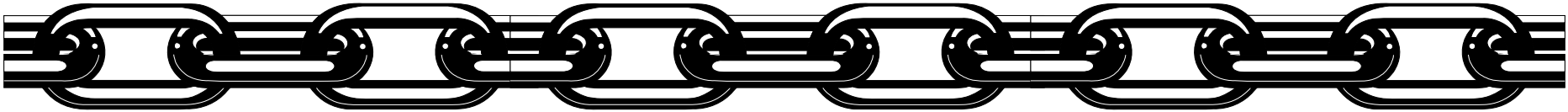
Step 4: Coordinate Acquisition Plan and Contract Execution

- 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



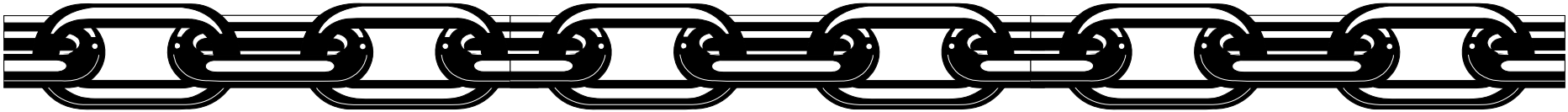
Step 5: Perform Continuous Monitoring

- 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



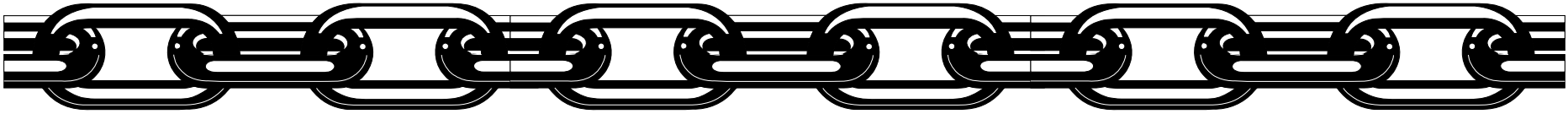
Supply Chain Practices

- 21 varying practices
 - Acquirer: Programmatic and validation activities
 - Supplier or integrator: General, technical and validation requirements
- Topic areas include:
 - Procurement
 - Design/Development
 - Testing
 - Operational
 - Personnel



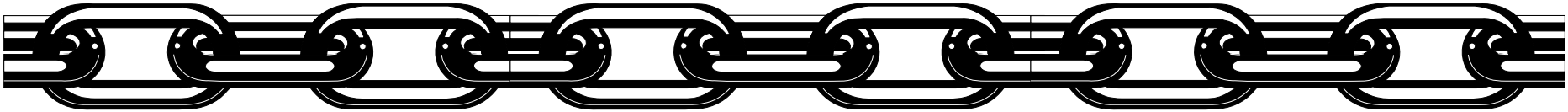
Procurement

- Maximize acquirer's visibility into Integrators and Suppliers
- Protect confidentiality of element uses



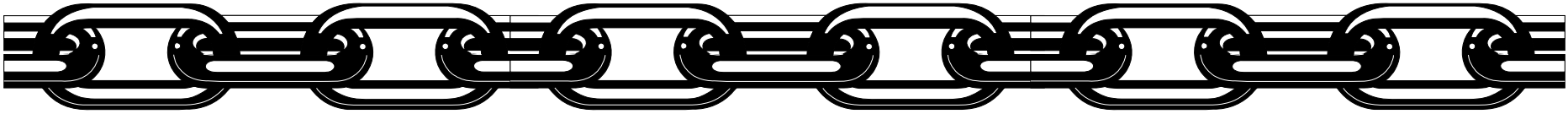
Design/Development

- Incorporate supply chain assurance in requirements
- Select trustworthy elements
- Enable diversity
- Identify and protect critical processes and elements
- Use defensive design



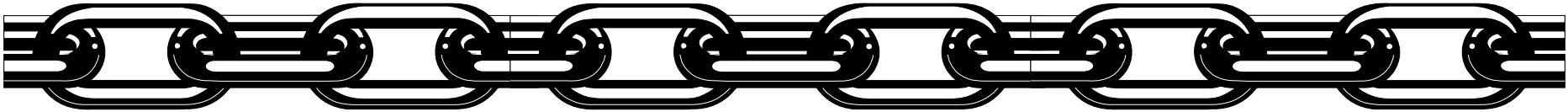
Design/Development (continued)

- Protect the supply chain environment
- Configure elements to limit access and exposure
- Harden supply chain delivery mechanisms



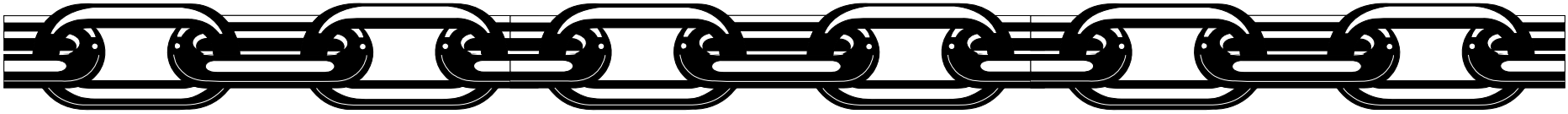
Testing

- Manual review
- Static analysis
- Dynamic analysis
- Penetration testing



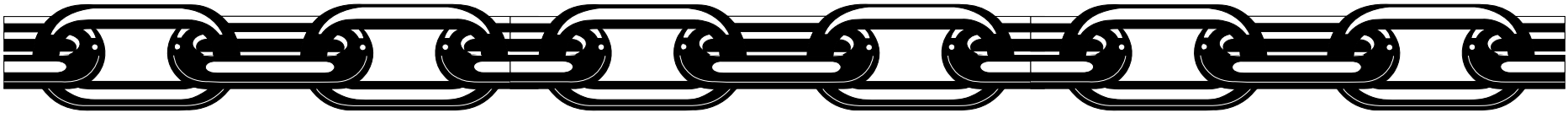
Operational

- Protect/monitor/audit operational systems
- Formalize service/maintenance
- Configuration Management
- Negotiate requirement changes
- Manage supply chain vulnerabilities
- Reduce supply chain risks during software updates and patches
- Supply chain incident response
- Reduce supply chain risks during disposal



Personnel

- Personnel considerations in the supply chain
- Promote awareness, educate and train personnel on supply chain risk



Contact Information

Marianne Swanson, Senior Advisor for Information System Security
marianne.swanson@nist.gov

Civilian Pilots: Kurt Seidling, Program Manager, DHS
kurt.seidling@dhs.gov

DoD Pilots: Annette Mirsky, Pilot Program Manager,
OASD NII CI&IA
annette.mirsky@osd.mil

Standards: Don Davidson, Senior Advisor Standards
OASD NII CI&IA
don.davidson@osd.mil