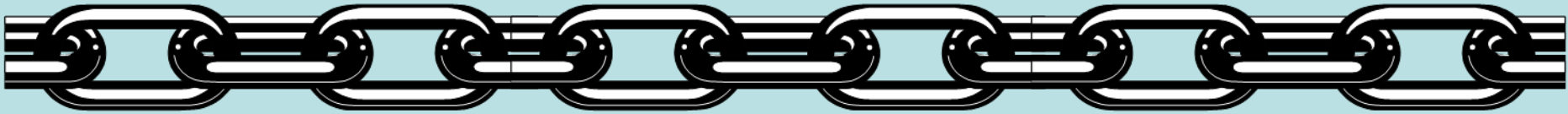




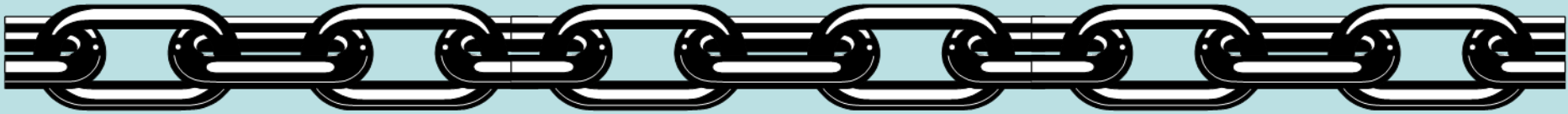
# Supply Chain Risk Management Practices for Unclassified Federal Information Systems

Marianne Swanson  
*Computer Security Division*  
*Information Technology Laboratory*



# *Agenda*

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



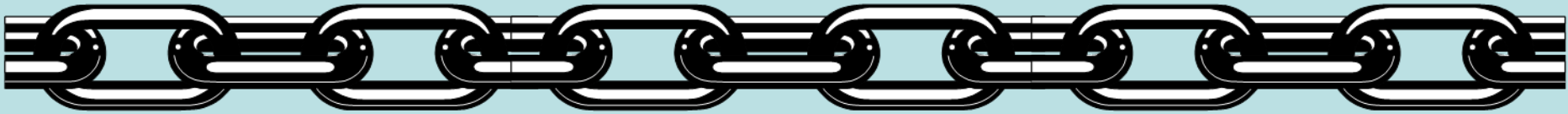
## *Background*

- 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 incident information



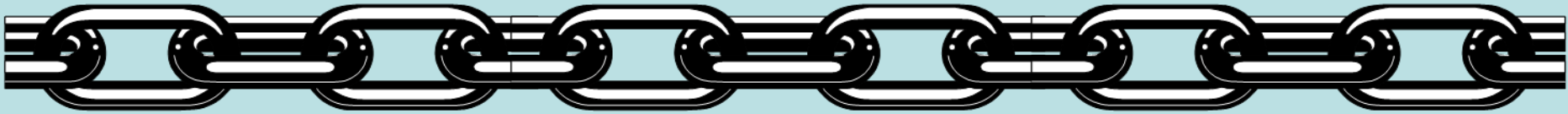
## ***Lifecycle Processes and Standards Working Group***

- 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



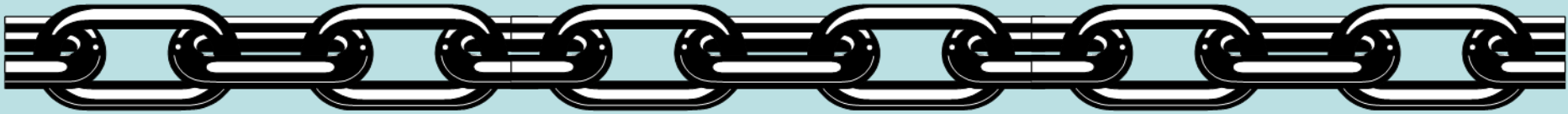
## *Guidance*

- Draft NIST Inter-Agency Report (NISTIR) 7622  
*Supply Chain Risk Management Practices for Federal Information Systems*
  - First Public Draft – October, 2009
- Future NIST Special Publication
  - First Public Draft – October, 2010



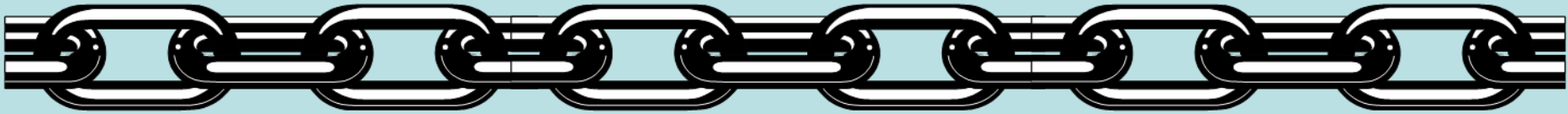
# *Collaboration*

- 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



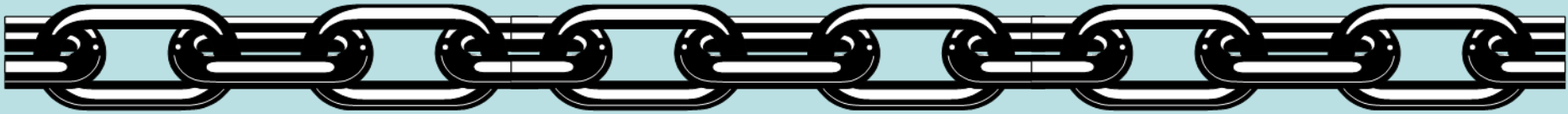
# *Implementing Supply Chain Risk Management*

- Implement Good Design and Development Practices
- Establish a Supply Chain Risk Management Capability (SCRMC)
- Roles and Responsibilities
- SCRMC Procurement Process



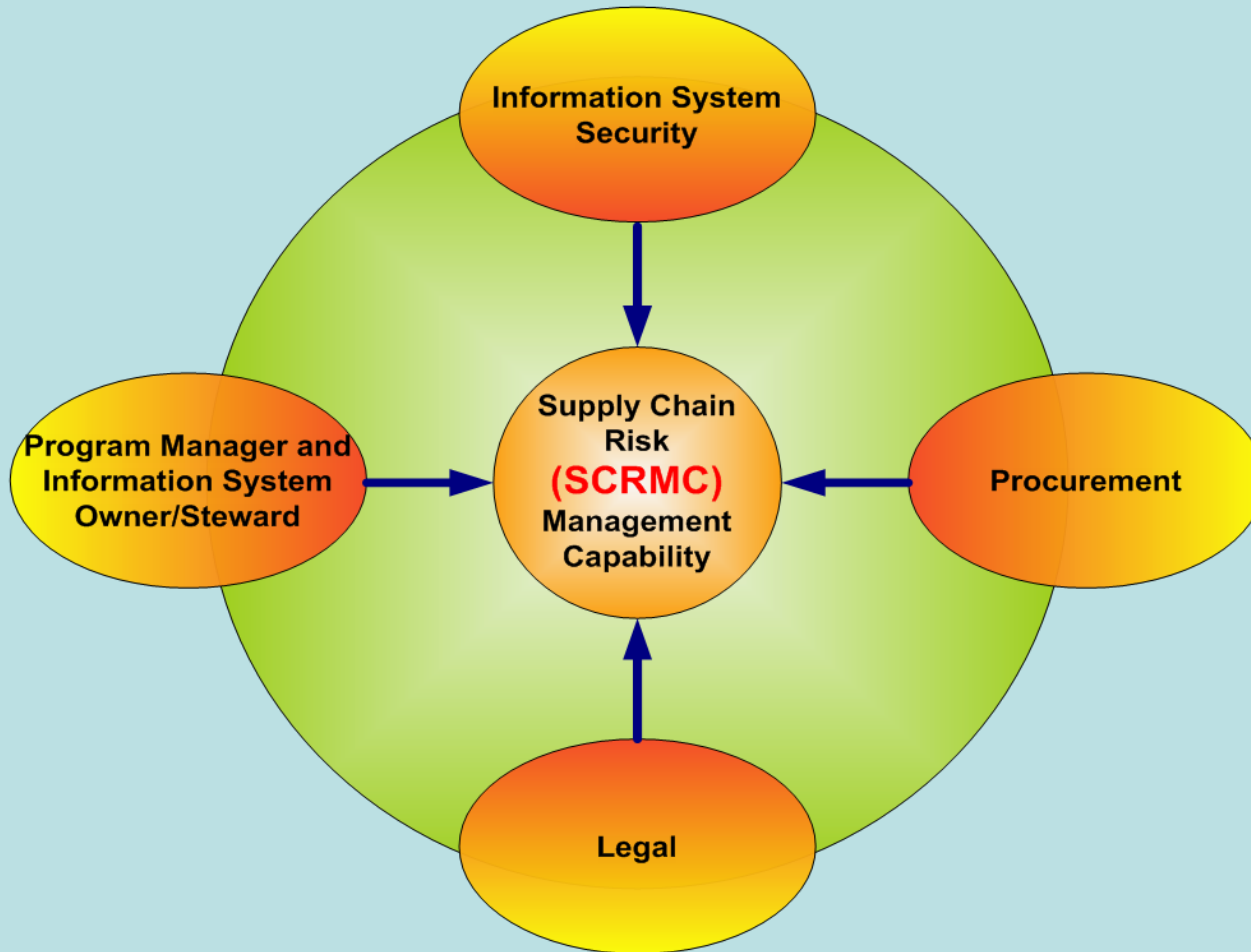
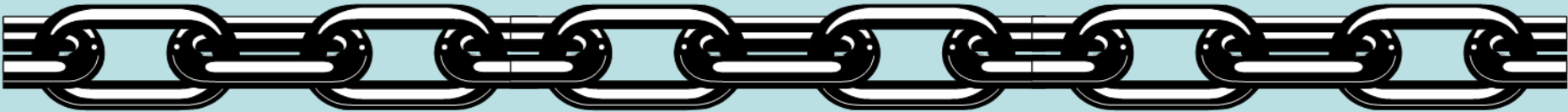
# ***Good System Design and Development Practices***

- Integrate information system security requirements from inception
- Follow consistent, well documented, repeatable processes for system engineering and acquisition
- Perform quality assurance and quality control
- Actively manage suppliers through Service Level Agreements/contracts.



## ***Establish a SCRMC***

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





# ***SCRMC Procurement Process***



## ***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



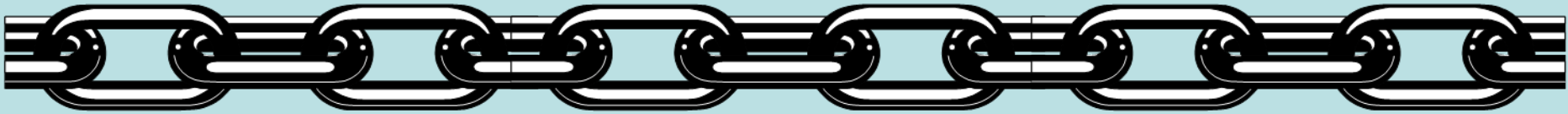
## ***Step 2 - Identify Potential Suppliers***

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



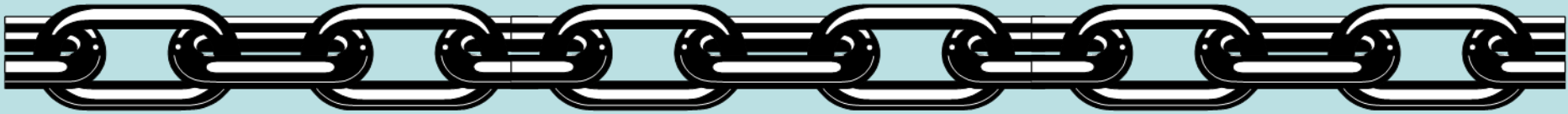
## *Open Sources*

- Central Contractor Registry (CCR)
- Online Representation & Certifications Applications (ORCA)
- Excluded Parties List System (EPLS)
- US Security & Exchange Commission
- Commercial & Government Entity (CAGE)
- Lexis/Nexis
- Past Performance Information Retrieval System (PPIRS)
- Dunn & Bradstreet
- Business Identification Number Cross-reference (BINCS)



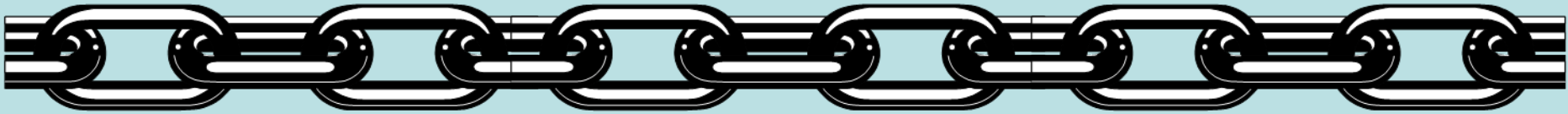
## ***Step 3 - Perform Open Source Analysis***

- Review all data gathered during the pre-solicitation
- Obtain any additional information
- Document findings
- Consider a procurement strategy
- Include applicable practices as requirements in the RFP



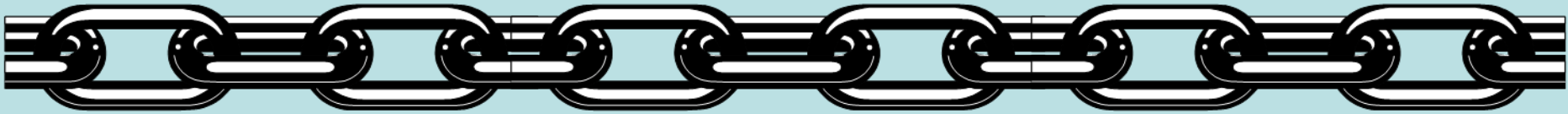
## ***Step 4 – Select Procurement Strategy***

- Identify Pre-solicitation security requirements for capable vendors
  - Qualification requirements
  - Minimum technical requirements in work statements
- Use contract vehicles that include trusted vendors
  - Existing interagency and intra-agency vehicles
  - Small Business programs
  - Avoid risky subcontractors
  - Blind transactions



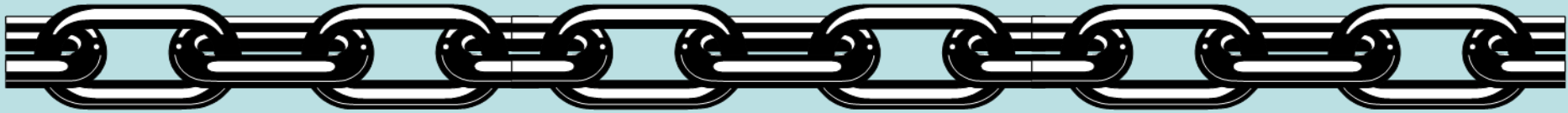
## ***Step 4 – Continued***

- Identify security considerations in solicitation (other than in work statements)
  - “Best Value” Technical and management evaluation factors
- Exclude on the basis of general ineligibility to contract
  - Office of Foreign Assets Control List
  - Excluded Parties List System



## ***Step 4 – Continued***

- Exclude vendors based upon or as part of a responsibility determination
  - Negative responsibility determination
  - Use of special responsibility standards

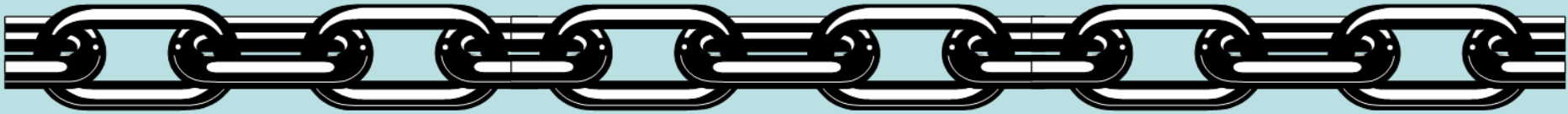


## ***Step 5 - Vendor/Offeror Response***

- Gather information on any new vendors and their sub-suppliers
- Assess vendors risk to the system and mission
- Determine the need for organizations to implement additional security controls
- Make risk based decision on purchasing the product/service



# *Supply Chain Risk Management Practices*



## ***Practices - 1***

1. Manage supply chain risk throughout project processes
2. Use insulated buying strategy
3. Maximize transparency to acquirer
4. Evaluate element trustworthiness
5. Harden supply chain delivery mechanisms
6. Include supply chain assurance/criticality in requirements
7. Manage requirements creep



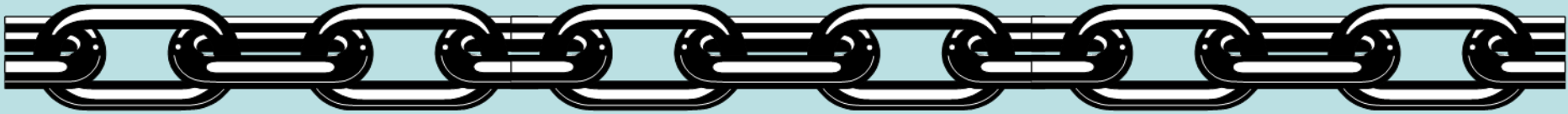
## ***Practices – 2***

8. Identify critical components
9. Use defensive design
10. Use alternatives by using/creating standard interfaces
11. Choose programming languages/subsets/tools that counter weakness
12. Formalize service/maintenance



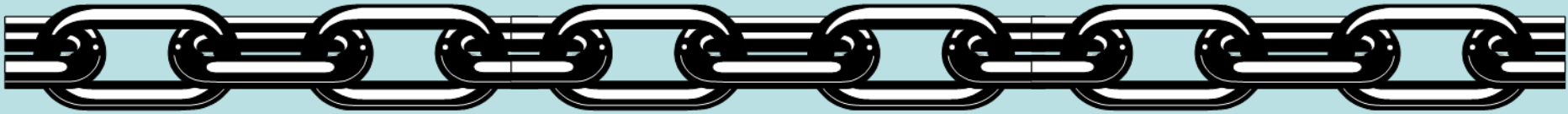
## ***Practices – 3***

- 13. Harden COTS elements
- 14. Collaboratively develop/maintain trustworthy elements
- 15. Diversify
- 16. Manual review
- 17. Static analysis



## *Practices – 4*

18. Dynamic analysis (including fuzz testing)
19. Penetration testing
20. Configuration management
21. Protect the supply chain environment
  - Physical defenses
  - Logical defenses
  - Test the defenses



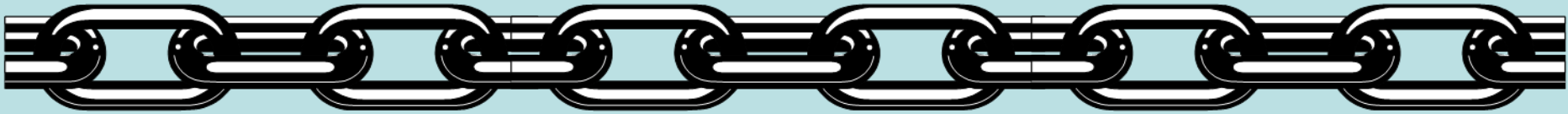
## ***Practices – 5***

- 22. Protect/monitor/audit operational system
- 23. Evaluate people in supply chain
- 24. Separate duties of people through life cycle
- 25. Train/educate/certify personnel on supply chain risks/security
- 26. Software updates and patch management



## *Practices – 6*

27. Disposal
28. Risk assessment for supply chain
29. Supply chain vulnerability management
30. Supply chain incident response
31. Continue supply chain risk management during operations
32. Evaluate supplier/supply chain



## ***Contact Information***

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

Civilian Pilots:                      Ron Ford, Program Manager, DHS  
ronald.m.ford@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