NIST Participation in the Comprehensive National Cybersecurity Initiative11: Supply Chain Risk Management (SCRM)

Marianne Swanson

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

April 2, 2009

Introduction

- Globalization of IT hardware and software products being built, delivered, maintained, and upgraded increases risk of supply chain attacks.
  - Global commercial supply chain provides adversaries with greater opportunities to manipulate IT products over the IT product lifecycle
  - Provides adversaries with greater access to United States Government (USG) networks when product or service is delivered
  - Increases opportunities for adversaries to exploit USG networks

Comprehensive National Cybersecurity Initiative11: Supply Chain Risk Management (SCRM)

- Tasked under National Security Presidential Directive-54/Homeland Security Presidential Directive-23
- Provide US Government with robust toolset of SCRM methods and techniques
- Multi-tiered Approach:
  - Cost effective procurement related strategies
  - Industry input into SCRM key practices and development of international standards
  - Ability to report and share supply chain incident and threat information

Initiative 11: Working Groups

Working Group	***Mission***
Senior Steering Group (SSG)	Coordinate the analysis and recommendations of all three supply chain working groups into a comprehensive supply chain risk management program and integrate into the larger Comprehensive National Cybersecurity Initiative
Threat Information Sharing	Recommend processes for sharing vendor threat analyses across the federal government
Acquisition Policy and Legal Analysis	Recommend a strategy to enhance federal government acquisition policy to address supply chain risk based on a legal and policy evaluation of the potential application of Intelligence Community (IC) processes for supply chain risk management to non-IC departments/agencies, including the use of vendor threat information in acquisition
Lifecycle Processes and Standards	Recommend criteria for identifying federal government systems and networks requiring enhanced efforts to ensure supply chain risk management. Recommend an approach for enhancing federal government technical expertise, guidance, and standards to manage supply chain risk.

Lifecycle Processes and Standards Working Group

- Provide highest investment in SCRM for high priority systems
  - Define as high availability/confidentiality impact levels in accordance with IC, NIST/Committee on National Security Systems (CNSS), and DoD standards
  - Issue guidance on selection criteria for identifying high priority systems
- Develop a robust body of acquisition and engineering guidance enabling SCRM
  - Complete gap analysis of current technical guidance (OMB, CNSS, NIST, etc.)
  - Develop and influence new policy to address gaps

Lifecycle Processes and Standards Working Group

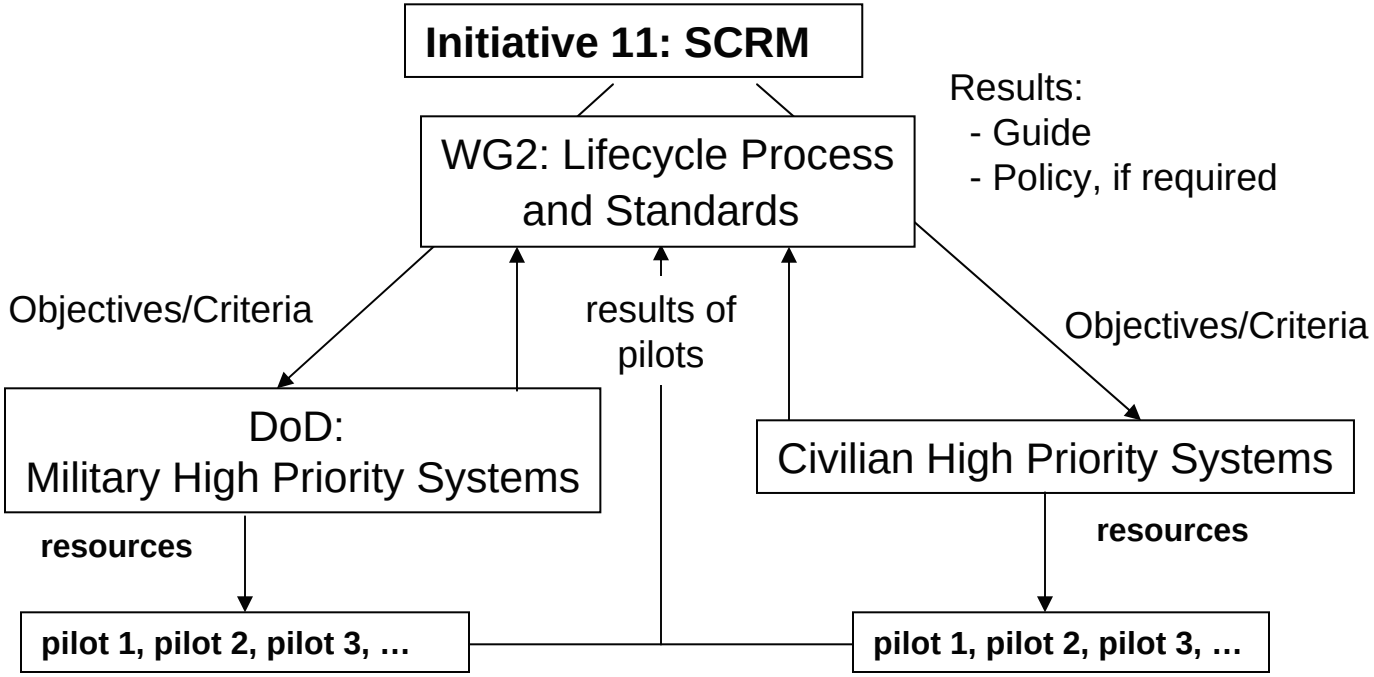
- Test existing and proposed guidance and incrementally implement SCRM approaches and techniques during pilots in FY09 and FY10
- Collaborate with organizations and industry on developing SCRM standards and best practices

Identification of High Priority Systems

	DCID		DOD		NIST/CNSS[1]
SCRM Thresholds	**Availability/ Integrity Level of Concern (LOC)**	**Minimum Protection Level (PL)**	**Minimum Mission Assurance Category (MAC) Level[2]**	**Minimum Confidentiality Level[3]**	**Availability/Integrity/Confidentiality Impact Level**
High Assurance	***High***	***PL1***	***MAC 1***	***Sensitive***	***High***
Medium Assurance	**Medium**	**PL1**	**MAC 2**	**Sensitive**	**Moderate**
Low Assurance	**Basic**	**PL1**	**MAC 3**	**Public**	**Low**

[1] CNSSI 1199 is in draft format and addresses the security categorization for NSS.
[2] Mission assurance categories are primarily used to determine the requirements for availability and integrity.
[3] The SCRM Threshold for High Assurance includes the confidentiality level of classified for all MAC levels.

Pilot Program Organization



- DHS will provide budgeted resources to support civilian agency pilots
- DoD will provide budgeted resources to support DoD pilots
- Core talent established within pilot organizations

SCRM Pilot Overview

- DoD and civilian agency pilots serve multiple purposes:
  - Incremental rollout of SCRM capabilities
  - Exercise threat informed technical mitigations
  - Exercise lifecycle SCRM techniques
  - Identify policy gaps
- DoD pilots are established
- Initial civilian pilot – Testing of SCRM procurement language in Networx contract revision for the Managed Trusted Internet Protocol Service
- Additional civilian pilots are being planned

Lifecycle Risk Mitigation Approach

Life Cycle Stages	Design	Manufacturing	Integration	Distribution	Operations	Services/ Maintenance	Retirement
Sample Protective Measures	• Use vetted providers and industry best practices	• Employ service level agreements related to quality and security	• Limit online SW installations •Thoroughly vet updates	• Use secure distribution channels	• Implement and enforce traditional information assurance policies	• Confirm the integrity of network mapping	•Secure destruction of media and computers

To meet tomorrow's threat we must develop protection measures across product lifecycle *and* reinforce these measures through acquisition processes and effective implementation of agency security practices

Proposed Next Steps for Pilot Program - 1

- Finalize Action Plan and Concept of Operations Plan for DoD and civilian pilots
- Select potential high priority systems/networks for civilian pilots
  - Selected in coordination with federal agencies
  - Reflect the diversity of federal government acquisitions
  - Approve and fund civilian pilot agencies
  - Implement civilian pilots

Proposed Next Steps for Pilot Program - 2

- Continue implementation of the DoD pilots
- Test key practices and modify based on lessons learned
- Research supply chain incident reporting and sharing

Pilot Program Key Practices Guide

- Using DoD's draft SCRM Pilot Program Key Practices and Implementation Guide as the base document:
  - Modify for civilian pilots
  - Work closely with DoD to continue to enhance guide as input is received from public review
- After pilots, anticipate that guide will evolve into a NIST Special Publication and a CNSS guide.

Interested Organizations

- Financial Sector Information Sharing and Analysis Center (FS-ISAC)
- SAIC and University of Maryland
- Bureau of Industry and Security, DOC
- Internet Security Alliance
- ICSA Labs
- IT and Telecom Sector Coordinating Councils (SCCs) and Government Coordinating Councils GCCs)
- Aerospace Industries Association (AIA) Counterfeit Part Group
- Federal CIO Council: Information Security and Identity Management Committee
- US Cybersecurity and System and Software Technical Advisory Groups under ISO

Contact Information

Marianne Swanson

marianne.swanson@nist.gov

301-975-3293

Annabelle Lee

annabelle.lee@nist.gov

301-975-8897

NIST
National Institute of Standards and Technology