Committee on National Security Systems

CNSSD No. 505
7 March 2012

(U) SUPPLY CHAIN RISK MANAGEMENT (SCRM)

THIS DOCUMENT PROVIDES MINIMUM REQUIREMENTS FOR NATIONAL SECURITY SYSTEMS. IT ALSO MAY OFFER GUIDELINES FOR THOSE PERFORMING THE SAME FUNCTIONS FOR UNCLASSIFIED SYSTEMS. YOUR DEPARTMENT OR AGENCY MAY IMPLEMENT MORE STRINGENT REQUIREMENTS IF APPROPRIATE.

CNSSD No. 505

CHAIR

FOREWORD

1. (U) In order to achieve cost efficiencies and innovations, the U.S. Government relies on the commercial information and communications technology (ICT) sector for components and services that support mission-critical networks, systems, and weapons. This reliance forces the U.S. Government to depend on the trustworthiness of the commercial ICT supply chain. However, trustworthiness in commercial ICT has become uncertain due to increasing globalization and the participation of unfamiliar, unknown, and changing actors in the supply chain. The U.S. Government must address the reality that the global marketplace provides increased opportunities for adversaries to penetrate ICT supply chains to subvert the components bound for U.S. Government critical systems to gain unauthorized access to data, alter data, interrupt communications, or disrupt critical infrastructures. The marketplace threat analysis process is well known, but the practices to mitigate ICT supply chain risks are still evolving. This Directive provides policy for the U.S. Government to develop an initial capability for supply chain risk management (SCRM) for National Security Systems (NSS).

2. (U) The U.S. Government must utilize enhanced government practices and, where possible, drive improved commercial practices through market incentives and the competitive process to achieve security objectives in NSS, new technologies and products, and managed services to counter the dynamic threats our adversaries use against us.

3. (U//FOUO) National Security Presidential Directive-54, in conjunction with Homeland Security Directive-23 (NSPD-54/HSPD-23) (Reference b), established “United States policy, strategy, guidelines, and implementation actions to secure cyberspace.” It also directed a Comprehensive National Cybersecurity Initiative (CNCI) to better protect United States (U.S.) interests within cyberspace. CNCI initiative 11 requires the “development of a multi-pronged approach for global supply chain risk management.”

4. (U) This Directive requires supply chain risk management (SCRM) to protect the confidentiality, integrity, and availability of NSS, and to mitigate and manage the risks posed by the threats described above.

5. (U) Additional copies of this Directive may be obtained from the Secretariat or at the CNSS website: www.cnss.gov.

/s/
TERESA M. TAKAI

(U) Supply Chain Risk Management (SCRM)

(U) SECTION I – PURPOSE

1. (U//FOUO) In accordance with CNSSP No. 22, "Information Assurance Risk Management Policy for National Security Systems" and the strategy established by the Comprehensive National Cybersecurity Initiative (CNCI), this Directive assigns responsibilities, and establishes the minimum criteria for the development and deployment of capabilities for the protection of National Security Systems (NSS), as defined in Reference d, from supply chain risk.

(U) SECTION II – AUTHORITY

2. (U) This Directive derives its authority from National Security Directive (NSD)-42, (Reference A) which outlines the roles and responsibilities for securing NSS, as affirmed by E.O. 12333 (Reference E).

3. (U) Nothing in this Directive shall alter or supersede the authorities of the Director of National Intelligence.

(U) SECTION III – SCOPE

4. (U) This directive applies to all departments, agencies, bureaus, and offices of the U.S. Government; their employees; and supporting contractors and agents that own, operate, use, maintain, procure, secure, develop, or manage NSS, as defined in Reference D.

5. (U) Organizations may implement more stringent requirements than those included in this Directive as necessary to support their mission(s).

(U//FOUO) SECTION IV – POLICY

6. (U//FOUO) U.S. Government departments and agencies shall establish an organizational supply chain risk management (SCRM) capability to identify and manage supply chain risk to NSS early and throughout their entire system lifecycle through the use of acquisition and engineering mitigations informed by all-source supply chain threat information.

7. (U//FOUO) Elements acquired for use within NSS shall be commensurately assured based on:

a. (U//FOUO) The criticality of the system to the mission, and

b. (U//FOUO) The role of the element in achieving, protecting, or impacting the mission critical functions of the system.

(U//FOUO) SECTION V – RESPONSIBILITIES

8. (U//FOUO) Heads of U.S. Government departments and agencies shall develop and document a strategy for the planned evolution of the department or agency-specific SCRM capability that shall include:

a. (U//FOUO) Integrating SCRM practices and risk mitigations, including threat support to acquisition, into department or agency-specific system and acquisition life cycle processes, security capabilities, and an enterprise-wide risk management policy consistent with National Institute of Standards and Technology (NIST) Special Publication 800-39 and the CNCI 11 SCRM Strategy and Implementation Plan.

b. (U//FOUO) Initiating SCRM capability within one year of this directive’s issue date to begin incremental implementation and to gain the experience necessary to identify and develop the plans, tools, and skills necessary to achieve a full-scale SCRM capability. Initial SCRM capabilities shall include:

1) (U//FOUO) Establishing processes and policy for using all-source threat information, in coordination with the Office of the Director of National Intelligence (ODNI), Office of the National Counterintelligence Executive (ONCIX).

2) (U//FOUO) Developing and implementing minimum standards for threat assessments to inform risk management decisions for mission-critical elements of NSS.

3) (U//FOUO) Identifying and prioritizing NSS for initial implementation of SCRM best practices (See ANNEX C).

c. (U//FOUO) Resourcing plans, to include major milestones to implement a full-scale SCRM capability to protect NSS within six years of the date of issue of this directive.

d. (U//FOUO) Processes which prioritize mission-critical elements of NSS for SCRM and which apply SCRM across the lifecycle of NSS, including systems acquisitions and commodity purchases.

e. (U//FOUO) Identifying the appropriate lead organization for the governance and support of the full-scale SCRM capability. The lead organization shall:

1) (U//FOUO) Establish agency-specific policies and procedures for SCRM.

2) (U//FOUO) Coordinate with internal and external organizational stakeholders for the implementation and governance of the enterprise SCRM capability.

3) (U//FOUO) Establish a mechanism and procedures for addressing threat that current engineering and acquisition mitigations and countermeasures cannot address.

4) (U//FOUO) Develop awareness, education, and training for personnel on supply chain risks and mitigations.

5) (U//FOUO) Establish a process for documenting how supply chain risks have been addressed and using this information for future risk mitigation and SCRM activities.

6) (U//FOUO) Provide regular reporting, as directed by the National Security Staff, on implementation progress and effectiveness of SCRM capabilities as part of the CNCI, through the appropriate CNCI leadership, including the SCRM Senior Steering Group.

9. (U//FOUO) The Office of the Director of National Intelligence (ODNI), Office of the National Counterintelligence Executive (ONCIX), shall develop standards, methodologies, and tools to assist departments and agencies in implementing threat assessments to inform risk management decisions for mission-critical elements of NSS.

(U) SECTION VI – GUIDANCE

10. (U//FOUO) SCRM Capability

a. (U//FOUO) Threat support to acquisition - Organizations shall use all-source intelligence assessments on potential suppliers (e.g., re-sellers, component manufacturers, product manufacturers, system integrators) to inform acquisition and risk management decisions for critical elements, subsystems, and systems used within NSS, in accordance with applicable laws, regulations, Executive Orders, and policies. Departments and agencies shall work with ONCIX to develop and implement all-source intelligence threat assessments in acquisition decision making, in accordance with the CNCI 11 SCRM Strategy and Implementation Plan. The ONCIX provides the minimum standards, along with methodologies, tools, and best practices to conduct counterintelligence analysis on supply chain threats. Agencies will follow ONCIX's guidelines when developing threat assessments. ONCIX supports the U. S. Government by serving as the national clearing house for threat information affecting the supply chain, enabling these organizations to develop and implement effective mitigation strategies.

b. (U//FOUO) SCRM processes, tools, and techniques - ANNEX C identifies numerous SCRM processes, tools, and techniques to facilitate the implementation of SCRM USG-wide. Departments and agencies shall adopt and tailor these recommended SCRM processes, tools, and techniques, and apply them to the procurement and operation of mission critical elements within NSS, to include those which:

1) (U//FOUO) Control the quality, configuration, and security of software, hardware, and systems throughout their lifecycles, including commercial elements or sub-elements.

2) (U//FOUO) Detect the occurrence, reduce the likelihood of occurrence, and mitigate the consequences of products containing counterfeit elements or malicious functions.

3) (U//FOUO) Develop requirements or capabilities to detect the occurrence of vulnerabilities within custom and commodity hardware and software through enhanced test and evaluation.

4) (U//FOUO) Enhance security through the implementation of system security engineering throughout the system life cycle.

5) (U//FOUO) Optimize acquisition and contracting to define requirements and source selection criteria that reduce supply chain risk, give preference to vendors that minimize supply chain risk in verifiable ways, and evaluate security with other desirable factors, such as low cost, rapid deployment, or new features.

6) (U//FOUO) Implement acquisition processes to document and monitor risk mitigation methods and requirements and provide for the update of documentation throughout the system lifecycle.

11. (U//FOUO) Supply Chain for Application-Specific Integrated Circuits (ASICS)

(U//FOUO) The Department of Defense instituted the Microelectronics Trusted Integrated Circuit Supplier Accreditation Program assigning authority for the program to the Trusted Access Program Office (TAPO) in the National Security Agency. TAPO developed and implemented the program and assigned responsibility for daily operation and accreditation authority to the Defense Microelectronic Activity (DMEA). DMEA accredits integrated circuit service providers for Design, Aggregator/Broker, Mask and Wafer Fabrication, Packaging, and Test services across a broad technology range for specialized governmental applications, both classified and unclassified. When a need for trusted microelectronics services exists, an accredited supplier shall be used.

Enclosures:

ANNEX A – Definitions
ANNEX B – References
ANNEX C – Best Practices, Tools, and Resources

ANNEX A

(U) ANNEX A – DEFINITIONS

(U) Definitions in CNSS Instruction No. 4009, “National Information Assurance Glossary,” apply to this Directive. Additional terms specific to this Directive that are not defined in CNSSI No. 4009 can be found below. These definitions provide clarification required for purposes of supply chain risk management and are not included in the CNSSI No. 4009. They are to be used exclusively in the context of this Directive.

a. (U) All-source intelligence - Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data in the production of finished intelligence.

b. (U) Application-Specific Integrated Circuits (ASICs) - Custom-designed and/or custom-manufactured integrated circuits.

c. (U) Mission-critical element - A system component or subsystem that delivers mission critical functionality to a system or that may, by virtue of system design, introduce vulnerability to mission critical functions.

d. (U) Mission-critical functionality - Any system function, the compromise of which would degrade the effectiveness of that system in achieving the core mission for which it was designed.

e. (U) Supply chain risk - The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system (Ref: The Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Section 806).

f. (U) Supply Chain Risk Management (SCRM) - A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

(U) ANNEX B – REFERENCES

(U) The following references provide amplifying or supplementary information. Future updates to referenced documents shall be considered applicable to this policy.

a. (U) National Security Directive No. 42, National Policy for the Security of National Security Telecommunications and Information Systems, July 5, 1990

b. (U) National Security Presidential Directive 54/Homeland Security Presidential Directive 23, Cybersecurity Policy, January 8, 2009.

c. (U) Public Law 107-347 [H.R. 2458], codified at 44 U.S.C. § et seq., The E-Government Act of 2002, Title III, the Federal Information Security Management Act of 2002, December 17, 2002.

d. (U) Committee for National Security Systems Instruction Number 4009, National Information Assurance (IA) Glossary, 26 April 2010.

e. (U) Executive Order 12333, United States Intelligence Activities, December 4, 1981, as amended.

f. (U) Executive Order 13526, Classified National Security Information, December 29, 2009, as amended.

g. (U) Executive Order 12968, Access to Classified Information, August 2, 1995, as amended.

h. (U) Committee on National Security Systems Instruction Number 1253, Security Categorization and Control Selection for National Security Systems, October 2009.

i. (U) Director of Central Intelligence Directive 7/6, Community Acquisition Risk Center, March 02, 2005.1

j. (U) Supply Chain Risk Management (SCRM) Program Management Office, Globalization Task Force(GTF), Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Program, February 25, 2010.

k. (U) Committee for National Security Systems Policy Number 22, Information Assurance Risk Management Policy for National Security Systems, February, 2009.

l. (U) Comprehensive National Cybersecurity Initiative (CNCI) 11 Supply Chain Risk Management Strategy and Implementation Plan, October, 2008. Classified: SECRET NOFORN

m. (U) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011.

n. (U) OMB Policy Letter 91-3, Reporting Nonconforming Products, April 9, 1991.

o. (U) NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010.

p. (U) Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011.

ANNEX C – BEST PRACTICES, TOOLS, AND RESOURCES

1. (U) The following resources provide SCRM, systems security engineering, and detailed risk management guidance and best practices for use in government systems.

a. (U) Draft NISTIR 7622, *Piloting Supply Chain Risk Management for Federal Information Systems*, June 2010. This document provides a set of practices that can be used for those information systems categorized at the FIPS (Federal Information Processing Standards) 199 high-impact level. These practices are intended to promote the acquisition, development, and operation of information systems or system-of-systems to meet cost, schedule, and performance requirements in today's environment with globalized suppliers and active adversaries. Integrated within the information systems development life cycle (SDLC), these practices provide risk mitigating strategies for the acquiring federal agency to implement.

b. (U) National Defense Industrial Association (NDIA) System Assurance Committee, 2008. *Engineering for System Assurance*, Arlington, VA. This document provides guidance on how to build assurance into a system throughout its life cycle. It identifies and discusses system engineering activities, process, tools and considerations to address system assurance. Assurance guidance used by the DoD and its contractors is also included in the document.

c. (U) The US-CERT maintains the Software Assurance (SwA) Pocket Guide Series on software assurance in acquisition and outsourcing, system development, system life-cycle, and measurement. SwA Pocket Guides are developed collaboratively by the SwA Forum and Working Groups which function as a stakeholder community that welcomes additional participation in advancing and refining software security. The SwA Pocket Guide Series can be found on https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html.

2. (U) The DoD SCRM best practices for NSS provide guidance on the successful implementation of SCRM pilots that incorporate all-source threat information, summarize the DoD pilot experience, and identify trusted suppliers of integrated circuits as accredited by the Defense Microelectronic Agency. They include:

a. (U) Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11: Supply Chain Risk Management Pilot Program. February 25, 2010. (https://diacap.iaportal.navy.mil/ks/pages/scrm.aspx)

b. (U) Concept of Operations for the DoD Comprehensive National Cybersecurity Initiative 11: Supply Chain Risk Management Pilot Program. August 25, 2009.

c. (U) Comprehensive National Cybersecurity Initiative (CNCI) DoD Supply Chain Risk Management (SCRM) Pilot Program Report, April 26, 2011.

3. (U) SCRM assistance and references from the Department of Homeland Security, Global Cyber Security Office can be found by contacting DHS_SCRM@dhs.gov. Agencies may contact Software.Assurance@dhs.gov for assistance in the development of a software assurance capability.

4. (U) Selected SCRM industry standards listed below pertain to quality assurance for electronic components.

a. (U) EIA-4899 - Standard for Preparing an Electronic Component Management Plan

b. (U) IDEA-STD-1010 – Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook

c. (U) SAE-AS9120 – Quality Management Systems for Aerospace Product Distributors

d. (U) SAE-AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition