DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1010

March 25, 2010
Incorporating Change 3, March 23, 2012

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-Type Memorandum (DTM) 09-016 – Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems

References: See Attachment 1

Purpose. This DTM:

- Reissues DTM 08-048 (Reference (a)), updating policy and responsibilities.

- Establishes policy and a defense-in-breadth strategy for managing supply chain risk to information and communications technology (ICT) within DoD critical information systems and weapons systems in accordance with National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (b)).

- Directs actions in accordance with DoD Instruction 5200.39 (Reference (c)) to mitigate and manage supply chain risk, as defined in the Glossary, using a multi-disciplinary approach for SCRM pursuant to Reference (b).

- Is effective immediately. It shall be converted to a new DoD issuance. This DTM shall expire effective ~~*March 1, 2012*~~ *August 1, 2012.*

Applicability. This DTM applies to:

- OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

- All DoD critical information systems and weapons systems, which includes all major systems as defined by section 2302(5) of title 10, United States Code (U.S.C.) (Reference (d)); national security systems (NSS) as defined by section 3542 of title 44, U.S.C. (Reference (e)); and all DoD information systems, categorized as Mission Assurance Category (MAC) I, and select DoD information systems, categorized as MAC II, in accordance with DoD Directive 8500.01E (Reference (f)) (hereafter referred to collectively as "covered systems").

Definitions. See Glossary.

Policy. It is DoD policy that:

- Supply chain risk shall be addressed early and across the entire system lifecycle through a defense-in-breadth approach to managing the risks to the integrity of ICT within covered systems.

- SCRM capability shall be incrementally instituted using the pilot process described in this DTM that shall include:

    - Incorporation of all-source intelligence analysis into assessments of the supply chain for covered systems.

- Controls to ensure that such all-source intelligence assessments are conducted in accordance with all applicable laws, Executive orders (E.O.s), policies, and regulations governing intelligence activities and the safeguarding of classified information (e.g., E.O.s 12333, 12958, and 12968 (References (g), (h), and (i)) and DoD 5240.1-R (Reference (j))).

- Processes to assess threats from potential suppliers providing critical ICT components to covered systems.

- Processes to control the quality, configuration, and security of software, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources.

- Processes to detect the occurrence, reduce the likelihood of occurrence, and mitigate the consequences of products containing counterfeit components or malicious functions.

- Processes to ensure that the fabrication of integrated circuits that are custom-designed and/or custom-manufactured (generally referred to as "application-specific integrated circuits") for a specific DoD end use within covered systems are, as appropriate to the risk, performed by suppliers of integrated circuit-related services accredited through an authority designated by the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), unless expressly waived by the Milestone Decision Authority (MDA) established pursuant to DoD Directive 5000.01 (Reference (k)).

- Enhanced developmental and operational test and evaluation capabilities, including software vulnerability detection methods and automated tools that are compliant with the security content automation protocol and enhanced information assurance certification established by DoD Instruction 8510.01 (Reference (l)).

Responsibilities. See Attachment 2.

Procedures. See Attachment 3.

Releasability. UNLIMITED. This DTM is approved for public release and is available on the DoD Issuances Website at http://www.dtic.mil/whs/directives.

Attachments:
As stated

ATTACHMENT 1

REFERENCES

(a) Directive-Type Memorandum 08-048, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems," February 19, 2009 (hereby cancelled)
(b) National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," January 8, 2008[1]
(c) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008
(d) Section 2302(5) of title 10, United States Code
(e) Section 3542 of title 44, United States Code
(f) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(g) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(h) Executive Order 12958, "Classified National Security Information," April 17, 1995, as amended
(i) Executive Order 12968, "Access to Classified Information," August 2, 1995, as amended
(j) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1, 1982
(k) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
(l) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
(m) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990
(n) Director of Central Intelligence Directive 7/6, "Community Acquisition Risk Center," April 20, 2001[2]

[1] Available to authorized users by request from the National Security Council.
[2] Available to authorized users on the Joint Worldwide Intelligence Communications System at http://www.dni.ic.gov/ddnicustomer/dnipag.nsf.

ATTACHMENT 2

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO, in addition to the responsibilities in section 7 of this attachment, shall:

a. Integrate SCRM in policies and processes as appropriate.

b. Coordinate with the Heads of the DoD Components and the USD(AT&L) to identify and support SCRM pilot systems as described in Attachment 3.

c. Identify, in coordination with the Heads of the OSD and DoD Components, appropriate lead organizations and supporting elements for the development and governance of an integrated strategy for SCRM for ICT.

d. Establish and manage pilot teams and their activities in coordination with the USD(AT&L) and the Heads of the DoD Components.

e. Develop programming recommendations for full operating capability.

f. Oversee implementation of this DTM.

g. Coordinate with the USD(AT&L), the Under Secretary of Defense for Intelligence (USD(I)), and affected DoD Component Heads to develop processes and procedures to identify mission dependence upon critical systems in order to prioritize implementation of SCRM, identify MAC II systems for inclusion as covered systems, develop guidance for identification of critical components, and develop SCRM training for relevant DoD Component and contractor personnel.

2. USD(AT&L). The USD(AT&L), in addition to the responsibilities in section 7 of this attachment, shall:

a. Provide direction and management for acquisition program SCRM in accordance with Reference (c).

b. Provide acquisition and procurement guidance in implementing this DTM.

c. Coordinate with the Heads of the DoD Components and the ASD(NII)/DoD CIO to identify and support SCRM pilot systems as described in Attachment 3.

d. Ensure appropriate research and development support for SCRM.

e. In coordination with the ASD(NII)/DoD CIO, the USD(I), and the Heads of the DoD Components, evaluate the feasibility and usefulness of applying the processes that are piloted for ICT components for covered systems in accordance with this DTM to non-ICT components that are critical to covered systems. In the event that demand for threat assessments exceeds resources, establish, in coordination with the ASD(NII)/DoD CIO, the USD(I), and the Heads of the DoD Components, the prioritization for threat assessment support.

f. Coordinate with the ASD(NII)/DoD CIO, the USD(I), and the affected DoD Component Heads to develop processes and procedures to identify mission dependence upon critical systems in order to prioritize implementation of SCRM, identify MAC II systems for inclusion as covered systems, develop guidance for identification of critical components, and develop SCRM training for relevant DoD Component and contractor personnel.

g. Designate and oversee an accreditation authority to establish criteria for accrediting trusted suppliers, to perform the accreditations of suppliers, and to review those accreditations on an annual basis.

3. USD(I). The USD(I), in addition to the responsibilities in section 7 of this attachment, shall:

a. Integrate SCRM into USD(I)-managed policies and processes as appropriate.

b. Support SCRM pilot systems as described in Attachment 3.

4. DIRECTOR, NATIONAL SECURITY AGENCY (NSA). The Director, NSA, under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 7 of this enclosure and pursuant to National Security Directive 42 (Reference (m)), shall support the SCRM pilot program in the development and application of supply chain risk prevention, detection, and mitigation methods and capabilities. The level of support will be mutually agreed upon by the Director, NSA, and the Head of the DoD Component conducting the SCRM pilot program and will be provided as available.

5. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 7 of this attachment, shall:

a. In coordination with the Intelligence Community and the Defense Intelligence and Defense Counterintelligence Components, manage production of all-source supply chain threat assessments and associated collection requirements on behalf of the Department of Defense in the implementation of this DTM as required by Reference (c), subject to the availability of funds.

b. Modify or establish collection requirements to support SCRM as appropriate.

6. GENERAL COUNSEL, DEPARTMENT OF DEFENSE (GC, DoD). The GC, DoD, in addition to the responsibilities in section 7 of this attachment, shall provide advice and support regarding all legal matters pertaining to the implementation of this DTM, including providing appropriate representation on the ASD(NII)/DoD CIO-designated governance structure for SCRM activities.

7. HEADS OF THE OSD AND DoD COMPONENTS. The Heads of the OSD and DoD Components shall:

a. Support the ASD(NII)/DoD CIO-designated governance structure and OSD staff in the development of SCRM pilot program concepts and procedures, as appropriate.

b. Support SCRM pilot program execution by assigning Component specialists to participate in the DIA-led intelligence production of all-source supply chain threat assessments, as appropriate.

c. Coordinate with the USD(AT&L) and the ASD(NII)/DoD CIO regarding SCRM training. Apply USD(AT&L) and ASD(NII)/DoD CIO jointly developed SCRM training to all Component and contractor personnel commensurate with their assigned responsibilities.

d. Implement U.S. Government SCRM contract requirements, as applicable according to USD(AT&L) SCRM guidance provided pursuant to section 2 of this attachment.

e. Identify and support SCRM pilot systems as described in Attachment 3.

f. Notify the cognizant MDA and the ASD(NII)/DoD CIO of significant threats that cannot be reasonably addressed through technical mitigation and countermeasures,

and for which procedures have not been established to address or that create significant risk of litigation.

ATTACHMENT 3

SCRM PILOT PROGRAMS

1. GENERAL

a. The Department of Defense depends upon numerous NSS interconnected within the Global Information Grid (GIG) to achieve its mission. The secure and effective performance of the GIG and interconnected systems requires integrity and trustworthiness of components, subsystems, and supporting services. The Department of Defense increasingly relies on ICT for components and services that support its critical information and weapons systems. The complex, transitory, and global nature of the commercial ICT marketplace provides opportunities for adversaries to corrupt ICT as a means to access DoD systems.

b. To manage the risks to integrity and trustworthiness, the Department of Defense is incrementally implementing a SCRM capability that integrates program protection planning, enterprise architecture, counterintelligence, information assurance, systems engineering, procurement, enhanced test and evaluation, and other measures to mitigate supply chain risk. This capability is intended to span the lifecycle of covered systems, beginning with pilot activities in fiscal years (FY) 2009 and 2010 and progressing to full operational capability by FY 2016, as determined by lessons learned from the pilot program.

c. Pilot activities are intended to demonstrate that all-source intelligence assessments are timely and understandable; identified prevention and mitigation methods are effective when broadly employed; and cost, schedule, and performance impacts and gaps in current policy and guidance are identified and evaluated. Selected pilot programs also will be assessed in greater detail as SCRM vulnerability assessments.

2. SUPPLY CHAIN THREAT SUPPORT FOR DoD SYSTEMS

. DoD supply chain all-source intelligence assessment capability builds upon the processes and practices of the Office of the Director of National Intelligence Community Acquisition Risk Section as described in Director of Central Intelligence Directive 7/6 (Reference (n)). DIA manages the DoD effort in coordination with the Defense Intelligence and Defense Counterintelligence Components to provide standardized all-source intelligence assessments of foreign threats and to support acquisition risk management efforts. This support is intended to inform architectural, engineering, and contracting decisions in DoD acquisition, operations, and maintenance, beginning with the SCRM pilot systems and expanding over time to all covered systems.

3. SCRM PILOT CONCEPT AND PROCEDURES. The SCRM pilot concept of operations, criteria and timelines for identifying pilot systems, and procedures for conducting and managing piloting activities will be jointly determined between the OSD staff and the DoD Components.

GLOSSARY

PART I. ACRONYMS AND ABBREVIATIONS

ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
DIA	Defense Intelligence Agency
DTM	Directive-Type Memorandum
E.O.	executive order
FY	fiscal year
GC, DoD	General Counsel, Department of Defense
GIG	Global Information Grid
ICT	information and communications technology
MAC	Mission Assurance Category
MDA	Milestone Decision Authority
NSA	National Security Agency
NSS	national security system
SCRM	supply chain risk management
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this DTM.

SCRM. The management of supply chain risk whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., packaging, handling, storage, and transport).

supply chain risk. The risk that adversaries will insert malicious code into or otherwise subvert the design, manufacturing, production, distribution, installation, or maintenance of ICT components that may be used in DoD systems to gain unauthorized access to data, to alter data, to disrupt operations, or to interrupt communications.