Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012

DoD CIO/USD(AT&L)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoD Instruction (DoDI) 5200.39 (Reference (g)), DoDD 5000.01 (Reference (h)), DoDI 5000.02 (Reference (i)), DoDD 8500.01E (Reference (j)), and Committee on National Security Systems Directive No. 505 (Reference (k)).

2. APPLICABILITY. This Instruction applies to:

a. 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 DoD (hereinafter referred to collectively as the "DoD Components").

b. All DoD information systems and weapons systems that are or include systems described in subparagraphs 2.b.(1) through 2.b.(3) (hereinafter referred to collectively as "applicable systems"):

(1) National security systems as defined by section 3542 of title 44, United States Code (U.S.C.) (Reference (l));

(2) Mission Assurance Category (MAC) I systems, as defined by Reference (j); or

(3) Other DoD information systems that the DoD Component's acquisition executive or chief information officer determines are critical to the direct fulfillment of military or intelligence missions;

c. All mission critical functions and critical components within applicable systems identified through a criticality analysis. For the purposes of this Instruction, only information and communications technology (ICT) components in applicable systems shall be considered for the processes described herein until this Applicability section is modified in accordance with Enclosure 2, paragraph 1.f.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. Mission critical functions and critical components within applicable systems shall be provided with assurance consistent with the criticality of the system and with their role within the system.

b. All-source intelligence analysis of suppliers of critical components shall be used to inform risk management decisions.

c. Risk to the trust in applicable systems shall be managed throughout the entire system lifecycle. The application of risk management practices shall begin during the design of applicable systems and prior to the acquisition of critical components or their integration within applicable systems, whether acquired through a commodity purchase, system acquisition, or sustainment process. Risk management shall include TSN process, tools, and techniques to:

(1) Reduce vulnerabilities in the system design through system security engineering.

(2) Control the quality, configuration, and security of software, firmware, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources. Employ protections that manage risk in the supply chain for components or subcomponent products and services (e.g., integrated circuits, field-programmable gate arrays (FPGA), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use.

(3) Detect the occurrence of, reduce the likelihood of, and mitigate the consequences of unknowingly using products containing counterfeit components or malicious functions.

(4) Detect vulnerabilities within custom and commodity hardware and software through rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing.

(5) Implement tailored acquisition strategies, contract tools, and procurement methods for critical components in applicable systems, to include covered procurement actions in accordance with Reference (f).

(6) Implement item unique identification (IUID) for national level traceability of critical components in accordance with DoDI 8320.04 (Reference (m)).

d. The identification of mission critical functions and critical components as well as TSN planning and implementation activities, including risk acceptance as appropriate, shall be documented in the Program Protection Plan (PPP) (Reference (n)) and in relevant IA plans and documentation in accordance with DoDI 8500.2 (Reference (o)).

e. In applicable systems, integrated circuit-related products and services shall be procured from a trusted supplier accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASIC)).

5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This Instruction:

a. Is effective November 5, 2012.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoDI 5025.01 (Reference (p)). If not, it will expire effective November 5, 2022 and be removed from the DoD Issuances Website.

Teresa M. Takai
DoD Chief Information Officer

Frank Kendall
Under Secretary of Defense
for Acquisition, Technology, and Logistics

Enclosures
1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005
(b) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
(c) Report on Trusted Defense Systems in response to the National Defense Authorization Act for Fiscal Year 2009, December 22, 2009[1]
(d) Directive-Type Memorandum 09-016, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems," March 25, 2010 (hereby cancelled)
(e) National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," January 8, 2008[2]
(f) Section 806 of Public Law 111-383, "The National Defense Authorization Act for Fiscal Year 2011," January 7, 2011
(g) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008
(h) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
(i) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008
(j) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(k) Committee on National Security Systems Directive No. 505, "Supply Chain Risk Management (SCRM)," March 7, 2012[3]
(l) Section 3542, title 44, United States Code
(m) DoD Instruction 8320.04, "Item Unique Identification (IUID) Standards for Tangible Personal Property," June 16, 2008
(n) Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Program Protection Plan Outline and Guidance," July 18, 2011[4]
(o) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(p) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012
(q) Defense Federal Acquisition Regulation Supplement, current edition[5]
(r) Defense Acquisition Guidebook, current edition[6]
(s) DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011
(t) Supply Chain Risk Management (SCRM) Program Office, Trusted Mission Systems and Networks Directorate, "Key Practices and Implementation Guide for the DoD

[1] Available to authorized users by request from the Office of the USD(AT&L).
[2] Available to authorized users by request from the National Security Council.
[3] Available to authorized users by request from the Committee on National Security Systems.
[4] Available at www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.docx
[5] Available at http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html
[6] Available at http://akss.dau.mil

Comprehensive National Cybersecurity Initiative 11 - Supply Chain Risk Management Pilot Program," February 25, 2010[7]
(u) Section 11101 of title 40, United States Code
(v) Committee on National Security Systems Instruction No. 4009, "National Information Assurance (IA) Glossary," April 26, 2010[8]
(w) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982

[7] Available at https://diacap.iaportal.navy.mil/ks/pages/SCRM.aspx
[8] Available at www.cnss.gov/Assets/pdf/cnssi_4009.pdf

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). The USD(AT&L), in accordance with Reference (a), shall:

a. In coordination with the DoD Chief Information Officer (DoD CIO), oversee the implementation of this Instruction and issue supporting guidance as necessary.

b. Coordinate with the DoD CIO and the Heads of the DoD Components to develop TSN requirements, best practices, and mitigations. Develop guidance for identification and protection of mission critical functions and critical components, develop programming recommendations for TSN, align DoD TSN enterprise resources (e.g., test and evaluation, training), and develop TSN training for appropriate DoD Components and contractor personnel.

c. In coordination with the DoD CIO and the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), advance the state of the art in assurance tools, techniques, and methods for creating and identifying non-cryptologic software and hardware that is free from exploitable vulnerabilities and malicious intent.

d. In coordination with the DoD CIO and the Heads of the DoD Components, integrate the identification and protection of mission critical functions and critical components into system engineering, acquisition, logistics, and materiel readiness policies to ensure implementation of TSN concepts in technology demonstration or other research projects, defense acquisition programs, commodity purchases, operations and maintenance activities, and end-of-life disposal procedures.

e. In coordination with the DoD CIO, incorporate TSN concepts and the authorities in Reference (f) into the Defense Federal Acquisition Regulation Supplement (Reference (q)), Defense Acquisition Guidebook (Reference (r)), and solicitation and contract language.

f. In coordination with the DoD CIO, the Under Secretary of Defense for Intelligence (USD(I)), and the Heads of the DoD Components, evaluate the feasibility and usefulness of applying the processes that are described for critical ICT components for applicable systems in accordance with this Instruction to non-ICT components that are critical to DoD weapons and information systems and issue policy as appropriate. In the event that demand for threat assessments exceeds resources, establish, in coordination with the DoD CIO, the USD(I), and the Heads of the DoD Components, the prioritization for threat assessment support.

g. In coordination with the DoD CIO, the Director, Defense Intelligence Agency (DIA), and the Heads of the DoD Components, develop a strategy for managing risk in the supply chain for integrated circuit-related products and services (e.g., FPGAs, printed circuit boards) that are identifiable to the supplier as specifically created or modified for DoD (e.g., military temperature range, radiation hardened).

2. DIRECTOR, DMEA. The Director, DMEA, under the authority, direction, and control of USD(AT&L), shall, in coordination with DoD CIO and the Heads of the DoD Components, perform the accreditations of trusted suppliers, review those accreditations on an annual basis, issue follow-on guidance for the use of trusted suppliers, and establish criteria for accrediting trusted suppliers of integrated circuit-related products and services.

3. DoD CIO. The DoD CIO shall:

a. Coordinate with the USD(AT&L) and the Heads of the DoD Components as a subject matter expert on SCRM activities within TSN, implementation of TSN across the DoD, and development of TSN training, requirements, best practices, and mitigations.

b. Integrate TSN concepts into IA controls and other policies and processes, as appropriate.

c. Issue guidance (e.g., information system security engineering guidance) and develop programming recommendations to ensure the integration of TSN concepts and processes into the acquisition and maintenance of DoD information systems, enclaves, and services, including the purchase and integration of ICT commodities.

4. USD(I). The USD(I) shall:

a. Guide collection of foreign intelligence and direct all-source analysis of supply chain risk.

b. Integrate TSN concepts into USD(I)-managed policies and processes, as appropriate.

c. In coordination with the DIRNSA/CHCSS, develop processes and procedures for responding to suspected or actual supply chain exploits identified by the Heads of the DoD Components, such as vulnerability assessments, best practices, and educational materials.

5. DIRNSA/CHCSS. The DIRNSA/CHCSS, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 8 of this enclosure, shall:

a. Support the development and application of TSN requirements, best practices, and processes. In the event that demand for support exceeds resources, establish, in coordination with the DoD CIO, the USD(I), and the Heads of the DoD Components, prioritization for support to achieve TSN.

b. Advise and guide the Heads of the DoD Components in the application of processes, tools, techniques, and methods to minimize vulnerabilities and risk of malicious intent in procured and developed software and hardware for applicable systems.

c. In coordination with selected software assurance testing centers, define processes, tools, techniques and standards to effectively test newly developed and acquired DoD software and hardware for applicable systems.

d. Assess software analysis tools and practices and disseminate guidance on software and hardware vulnerability reduction and malicious intent identification to enable acquisition programs to manage risk effectively.

6. DIRECTOR, DIA. The Director, DIA, under the authority, direction, and control of the USD(I), and in addition to the responsibilities in section 8 of this enclosure, shall produce an intelligence and counterintelligence assessment of supplier threats to acquisition programs providing critical weapons, information systems, or service capabilities in accordance with DoDI O-5240.24 (Reference (s)). In the event that demand for support exceeds resources, establish, in coordination with USD(AT&L), DoD CIO, and the Heads of the DoD Components, prioritization for support to conduct threat analysis of suppliers of critical components.

7. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) shall, in coordination with the USD(I), establish security policy for foreign national participation in system integration activities.

8. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Designate a TSN focal point or focal points, with access to all DoD Components research, development, and acquisition (RDA) activities for applicable systems, in order to:

(1) Coordinate and prioritize requests for threat analysis of suppliers of critical components in accordance with Reference (s).

(2) Coordinate use of DoD Components and Enterprise TSN resources, including TSN subject matter experts and tools.

(3) Coordinate with the DoD CIO and USD(AT&L) in the development of TSN requirements, best practices, and mitigations.

(4) Assure the identification of mission critical functions and critical components as well as TSN planning and implementation activities are documented in the PPP.

b. Establish processes for managers of RDA activities for applicable systems to manage risk to the trust in the system by:

(1) Conducting a criticality analysis to identify mission critical functions and critical components and reducing the vulnerability of such functions and components through secure system design.

(2) Requesting threat analysis of suppliers of critical components from the pertinent TSN focal point and managing access to and control of threat analysis products containing U.S. person information, in accordance with Reference (s).

(3) Engaging the pertinent TSN focal point for guidance on managing identified risk using DoD Components and Enterprise risk management resources.

(4) Applying TSN best practices, processes, techniques, and procurement tools prior to the acquisition of critical components or their integration into applicable systems, at any point in the system lifecycle. Such tools and practices include contract requirements developed in accordance with USD(AT&L) guidance provided pursuant to paragraph 1.e of this enclosure, SCRM key practices (Reference (t)), and the authorities prescribed in Reference (f), as appropriate.

(5) Documenting TSN plans and implementation activities in PPPs and relevant IA plans and documentation.

c. Assign DoD Components specialists to assist the Director, DIA, to conduct threat analysis of suppliers of critical components.

d. Coordinate with the USD(AT&L) and the DoD CIO regarding TSN training of all appropriate DoD Components and contractor personnel commensurate with their assigned responsibilities.

e. Notify the cognizant Milestone Decision Authority, Designated Accrediting Authority, and the DoD CIO of significant threats that cannot be reasonably addressed through technical mitigation, countermeasures, or risk management procedures.

f. Notify the USD(I) and DIRNSA/CHCSS of discovered or suspected supply chain exploits for the purposes of further analysis and the development of enterprise remediation, as appropriate.

g. Integrate Component-unique TSN concepts into DoD Components policies and processes, as appropriate.

h. Ensure the Component Acquisition Executive or Chief Information Officer designate DoD systems that are not national security systems or MAC I systems as applicable systems in accordance with subparagraph 2.b.(3) of this Instruction.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASIC	application-specific integrated circuits
DIA	Defense Intelligence Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DMEA	Defense Microelectronics Activity
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
FPGA	field-programmable gate arrays
IA	information assurance
ICT	information and communications technology
IT	information technology
IUID	item unique identification
MAC	Mission Assurance Category
PPP	Program Protection Plan
RDA	research, development, and acquisition
SCRM	supply chain risk management
TSN	trusted systems and networks
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
U.S.C.	United States Code

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this Instruction.

critical component. A component which is or contains ICT, including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system.

criticality analysis. An end-to-end functional decomposition performed by systems engineers to identify mission critical functions and components. Includes identification of system missions,

decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system missions(s). Criticality levels are defined in Reference (n).

ICT. Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). ICT is not limited to information technology (IT), as defined in section 11101 of title 40, U.S.C. (Reference (u)). Rather, this term reflects the convergence of IT and communications.

information system. Defined in Committee on National Security Systems Instruction No. 4009 (Reference (v)).

information systems security engineering. Defined in Reference (v).

mission critical functions. Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed.

RDA. Defined in Reference (r).

SCRM. A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD's "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).

software assurance. The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.

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 a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

system security engineering. An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities.

U.S. person. Defined in DoD 5240.1-R (Reference (w)).

weapon system. A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.