DoD INSTRUCTION 5200.44

PROTECTION OF MISSION CRITICAL FUNCTIONS TO ACHIEVE TRUSTED SYSTEMS AND NETWORKS

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering Office of the DoD Chief Information Officer
Effective:	February 16, 2024
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012, as amended
Incorporates:	Deputy Secretary of Defense Memorandum, "Procedures for Supply Chain Risk Management in Support of DoD Trusted Systems and Networks," August 20, 2021
Approved by: **Approved by:**	Heidi Shyu, Under Secretary of Defense for Research and Engineering John Sherman, DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directives 5137.02 and 5144.02, this issuance:

- Establishes policy and assigns responsibilities to:
  - Minimize information and communications technology (ICT) supply chain and engineering risks to the DoD's warfighting capabilities, business, and enterprise information systems to maintain a technological advantage.
  - Implement ICT supply chain risk management (SCRM) requirements.
- Implements the DoD's trusted systems and networks (TSN) strategy, described in the December 22, 2009 Report on Trusted Defense Systems, through program protection and cybersecurity implementation to provide uncompromised weapon and information systems.

- Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive-54/Homeland Security Presidential Directive-23; Section 807 of Public Law 115-91; and Committee on National Security Systems Directive No. 505.
- Implements August 20, 2021 Deputy Secretary of Defense Memorandum, and provides guidance for implementation of the authorities set forth in Section 3252 of Title 10, United States Code (U.S.C.).

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to:

(1) 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 Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

(2) The United States Coast Guard. The United States Coast Guard will adhere to DoD cybersecurity requirements, standards, and policies in this issuance in accordance with the direction in Paragraphs 4.(a) through 4.(d) of the January 19, 2017 Memorandum of Agreement between the DoD and the Department of Homeland Security.

(3) All DoD information systems, networks, and weapon systems that are or include the following systems that are referred to collectively in this issuance as "applicable systems:"

(a) National security systems.

(b) Any DoD system with a high impact level for any of the three security objectives—confidentiality, integrity, and availability—in accordance with the system categorization procedures in DoD Instruction (DoDI) 8510.01.

(c) Other DoD systems that the DoD Component's acquisition executive, chief information officer, or designee determines are critical to directly fulfilling military or intelligence missions, which may include some connections to or enclaves of the Non-classified Internet Protocol Router Network, control systems, and business systems.

(d) Other DoD systems supporting national leadership command capabilities; nuclear weapons; nuclear command, control, and communications; continuity of U.S. Government operations; ballistic missile defense; protected satellite communications; and overhead persistent infrared systems as prioritized by the DoD Component heads.

(4) All mission critical functions and critical components in applicable systems identified through a criticality analysis, including spare or replacement parts.

(5) Acquisition of critical programs and technology, high-interest commodity ICT, critical components, or their integration within applicable systems, whether acquired through a commodity purchase, acquisition pathway in the Adaptive Acquisition Framework described in DoDI 5000.02, or sustainment process.

b. This issuance does not alter existing authorities and responsibilities of the heads of DoD elements of the Intelligence Community (IC).

1.2. POLICY.

a. Mission critical functions will be protected through the application of TSN and ICT SCRM practices.

b. Critical components within applicable systems will have a level of assurance consistent with system criticality and their function in the system.

c. All-source intelligence analysis of suppliers of critical components will be used with supply chain illumination capabilities as part of supplier due diligence to inform risk management decisions.

d. Risk to the assurance of applicable systems will be considered as part of the risk management process used throughout the entire system life cycle. Risk management will include TSN processes, tools, and techniques to:

(1) Reduce vulnerabilities in mission critical functions through use of TSN practices and system security engineering.

(2) Assess risk, and plan and implement mitigations to ensure the confidentiality, integrity, availability, quality, configuration, software patch management, and security of software, hardware, and systems throughout their life cycles, including components or subcomponents provided in sources throughout the supply chain.

(3) Detect the occurrence, reduce the likelihood, and mitigate the consequences of unknowingly using products containing counterfeit components or malicious functions in accordance with DoDI 4140.67.

(4) Assess vulnerabilities in custom and commodity hardware and software through thorough use of 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 consideration of use of the authority to take the covered procurement actions in Section 3252 of Title 10, U.S.C.

(6) Review intelligence and counterintelligence assessments of known supplier threats; determine associated risks affecting DoD information systems, networks, weapon systems, and defense critical infrastructure; identify ICT supply chain risks that may be common across the enterprise; and direct or recommend specific mitigation actions, as appropriate and authorized.

e. Procurement of custom designed, custom manufactured integrated circuit-related products and services for applicable systems and such products and services tailored for a specific DoD military end use must be accomplished as follows:

(1) Unless approved pursuant to Paragraph 1.2.e.(2), procurement of custom designed, custom manufactured integrated circuit-related products and services for applicable systems and

such products and services tailored for a specific DoD military end use must be from a trusted supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA).

(2) When a trusted supplier is not available, procurement of custom designed, custom manufactured integrated circuit-related products and services for applicable systems and such products and services tailored for a specific DoD military end use must be approved by the DoD Component head after consideration of the factors in Paragraph 1.2.d.

f. Mission critical functions, critical components, and risk planning and management activities, including criticality analyses and risk acceptance, as appropriate, will be identified and documented in the program protection plan in accordance with DoDI 5000.83 and in relevant cybersecurity plans and documentation in accordance with DoDI 8500.01.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (USD(R&E)).

The USD(R&E):

a. In coordination with the DoD Chief Information Officer (DoD CIO), oversees and provides guidance on implementing this issuance.

b. In coordination with the DoD CIO, the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), the Under Secretary of Defense for Intelligence and Security (USD(I&S)), and the DoD Component heads:

(1) Establishes policy and provides guidance, mitigations, education, and training for the science and technology manager and engineering workforce on the protection of mission critical functions and critical components and the application of software and hardware assurance mechanisms relating to systems engineering, acquisition, logistics, and materiel readiness policies. Ensures that assurance concepts are implemented in policies relating to technology demonstration or other research projects, defense acquisition programs, commodity purchases, operations and maintenance activities, and disposal procedures.

(2) Develops budget recommendations for the life cycle of the TSN's capability and aligns DoD TSN enterprise resources to advance the state of the art in assurance tools, techniques, and methods across the system life cycle.

(3) Develops a strategy for managing TSN risk in the supply chain for products and services identifiable to the supplier as specifically procured, created, or modified for the DoD.

(4) Establishes, if demand for threat assessments exceeds resources, threat assessment prioritization and IC support prioritization.

c. Conducts risk assessment activities to support implementation of Section 3252 of Title 10, U.S.C..

d. In coordination with the DoD CIO; the USD(A&S); the USD(I&S); the Secretaries of the Military Departments; and the Commander, United States Cyber Command (USCYBERCOM), reviews intelligence and counterintelligence assessments of known ICT supplier threats and identifies associated risks affecting DoD information systems, networks, weapon systems, and defense critical infrastructure. Identifies ICT supply chain risks and indicates whether the risk applies to an individual procurement transaction only or to a class of procurement. Directs or recommends specific mitigation actions, as appropriate.

e. In coordination with the USD(A&S), establishes processes and procedures to ensure assured access to trusted microelectronics pursuant to Section 231 of Public Law 114-328, also

known and referred to in this issuance as the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2017.

f. Manages and oversees the Joint Federated Assurance Center (JFAC) in accordance with DoDI 5000.83.

2.2. DOD CIO.

The DoD CIO:

a. Coordinates with the USD(R&E), the USD(A&S), and the DoD Component heads as a subject matter expert on ICT SCRM activities in assured systems and networks, implementation of supply chain assurance practices across the DoD, and development of ICT SCRM training, requirements, best practices, and mitigations.

b. In coordination with the USD(R&E), the USD(A&S), the USD(I&S), and the DoD Component heads, integrates multilayered ICT SCRM concepts into security controls and other policies and processes.

c. In coordination with the USD(R&E), the USD(I&S), and the USD(A&S), issues information systems security engineering and ICT SCRM guidance and develops budget recommendations for the capability's life cycle.

d. In coordination with the USD(A&S):

(1) Establishes and maintains procedures for the execution of the exclusion authorities in Section 3252 of Title 10, U.S.C. and other relevant exclusion authorities.

(2) Issues guidance on using automated supply chain illumination capabilities to provide SCRM decision support and real-time monitoring of sub-tier suppliers to identify risks related to foreign influence, cybersecurity, financial stability, and other factors.

e. For risks requiring action under Section 3252 of Title10, U.S.C., in coordination with the USD(A&S) and the USD(I&S), prepares and executes an action package that contains a joint recommendation of the DoD CIO and USD(A&S) on the basis of a risk assessment by the USD(I&S), regarding the assessment of a significant supply chain risk, the scope of applicability, and required or recommended mitigations. The Joint Recommendation package may also contain:

(1) The advance concurrence of the USD(A&S), including any conditions or limitations thereon, for any subsequent determination by an Authorized Official in a Military Department (see Defense Federal Acquisition Regulation Supplement (DFARS) Part 239.7303) to exercise the authority in Section 3252 of Title10, U.S.C. for a procurement that is within scope of the joint recommendation, pursuant to DFARS Part 239.7304(b).

(2) The determination by the USD(A&S), including any conditions or limitations thereon, to exercise the authority in Section 3252 of Title 10, U.S.C. for procurements by any DoD Component (including the MILDEPS and the DoD Fourth Estate) that are within the scope of the joint recommendation, pursuant to DFARS Part 239.7304(b).

f. Issues guidance on the DoD operational usage of suppliers and components on DoD systems that are excluded from procurement or otherwise restricted from use due to a significant ICT supply chain risk.

g. In coordination with the USD(R&E); the USD(A&S); the USD(I&S); the Secretaries of the Military Departments; and the Commander, USCYBERCOM, reviews intelligence and counterintelligence assessments of known ICT supplier threats and determines associated risks affecting DoD information systems, networks, weapon systems, and defense critical infrastructure. Identifies ICT supply chain risks and directs or recommends specific mitigation actions, as appropriate.

h. Oversees the establishment of a DoD enterprise ICT SCRM capability to provide risk decision support for due diligence of high-interest commodity ICT items.

i. Retains all signed joint recommendation, concurrence, and determination packages developed in connection with DoD's exercise of the authority set forth in Section 3252 of Title 10, U.S.C. and DFARS Part 239.73, in accordance with applicable recordkeeping guidelines.

j. Issues guidance and provides recommendations to DoD Component heads for ICT supply chain due diligence, risk and mitigation trade-offs, and residual risk management.

k. Develops 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.

2.3. USD(A&S).

The USD(A&S):

a. In coordination with the USD(R&E) and the DoD CIO, evaluates the supply chain risk and integrates ICT SCRM into the acquisition process.

b. Establishes policy and develops implementing guidance for acquisition and materiel management, including source selection guidance in support of TSN capabilities, to include ICT SCRM.

c. In coordination with the USD(R&E), the DoD CIO, the USD(I&S), and the DoD Component heads, establishes TSN and ICT SCRM policy, guidance, education, and training for the program managers and the acquisition and sustainment workforce to include cybersecurity for acquisition decision authorities and program managers in accordance with DoDI 5000.90. Develops budget recommendations for the lifecycle of the TSN capability.

d. In coordination with the USD(R&E), the DoD CIO, and the DoD Component heads, integrates identifying and protecting mission critical functions and critical components into acquisition, logistics, and materiel readiness policies to ensure that assurance concepts are implemented in defense acquisition programs.

e. Through the Director, DMEA, and in coordination with the DoD CIO and the DoD Component heads, performs the accreditations of trusted suppliers, reviews those accreditations on an annual basis, issues follow-on guidance for the use of trusted suppliers, establishes criteria for accrediting trusted suppliers of integrated circuit-related products and services, and executes efforts to ensure assured access to trusted microelectronics pursuant to Section 231 of the NDAA for FY 2017.

f. In coordination with the DoD CIO, establishes and maintains procedures to implement the authorities in Section 3252 of Title 10, U.S.C..

g. For risks requiring action under Section 3252 of Title 10, U.S.C., coordinates on an action package prepared by DoD CIO that contains a joint recommendation of the DoD CIO and USD(A&S), on the basis of a risk assessment by the USD(I&S), regarding the assessment of a significant supply chain risk, the scope of applicability, and required or recommended mitigations.

h. Coordinates on any determination by an Authorized Official in a Military Department to exercise the authority in Section 3252 of Title 10, U.S.C. for a procurement that is within scope of a joint recommendation, pursuant to DFARS Part 239.7304(b).

i. As the Defense Acquisition Executive, makes determinations pursuant to DFARS Part 239.7304(b) for the DoD Components on behalf of the Secretary of Defense, when necessary, to protect national security by reducing ICT supply chain risk. This authority cannot be further delegated.

j. Provides congressional notifications, as required, of exclusion determinations that are made by the USD(A&S) in accordance with Section 3252 of Title 10, U.S.C..

k. Fulfills congressional reporting requirements regarding covered procurement actions taken pursuant to DFARS Part 239.73 during the annual reporting period.

l. In coordination with the USD(R&E); the DoD CIO; the USD(I&S); the Secretaries of the Military Departments; and the Commander, USCYBERCOM, reviews intelligence and counterintelligence assessments of known ICT supplier threats and determines associated risks affecting DoD information systems, networks, weapon systems, and defense critical infrastructure.

m. Identifies ICT supply chain risks and indicates whether the risk applies to an individual procurement transaction only or to a class of procurements. Directs or recommends specific mitigation actions, as appropriate.

n. In coordination with the USD(R&E), the DoD CIO, and the USD(I&S), provides mitigations for printed circuit boards and interconnect technology in accordance with DoD Directive 5101.18E.

o. Develops and implements guidance to resolve or mitigate potential consequences of foreign adversary influence through ownership or business relationships within the DoD's ICT supply chain, including products and services received through simplified acquisition procedures and purchase card orders.

2.4. USD(I&S).

The USD(I&S):

a. Guides collection of foreign intelligence and counterintelligence information, directs all-source analyses of ICT supply chain threats, and integrates TSN concepts into USD(I&S)-managed policies and processes.

b. Develops procedures for:

(1) Responding to suspected or actual ICT supply chain exploits that the DoD Component heads identify.

(2) Sharing findings such as vulnerability assessments, best practices, and educational materials.

c. Develops policy and establishes processes for DoD Components to share intelligence, counterintelligence, and ICT supply chain threat information within the DoD and defense industrial base, within defense critical infrastructure, and among Federal agencies.

d. Oversees security support to protect mission critical functions and critical components in accordance with DoDI O-5240.24.

e. In coordination with the Director of National Intelligence, directs and oversees DoD IC elements to share actionable ICT supply chain threat intelligence information at multiple classification levels.

f. In coordination with the USD(R&E); the DoD CIO; the USD(A&S); and the Commander, USCYBERCOM, reviews intelligence and counterintelligence assessments of known ICT supplier threats and determines associated risks affecting DoD information systems, networks, weapon systems and defense critical infrastructure. Identifies ICT supply chain risks, indicates whether risk applies to an individual procurement transaction only or to a class of procurements, and directs or recommends specific mitigation actions, as appropriate.

g. In coordination with the DoD CIO, the USD(A&S), the USD(R&E), and the DoD Component heads, establishes policy, guidance, mitigations, education, and training for protecting mission critical functions and critical components.

h. Develops the risk assessments that serve as the basis for a joint recommendation under Section 3252(b)(1) of Title 10, U.S.C.

2.5. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS).

Under the authority, direction, and control of the USD(I&S), and in addition to the responsibilities in Paragraph 2.9., the DIRNSA/CHCSS:

a. In coordination with the DoD CIO, the USD(I&S), and the DoD Component heads, supports the development and application of TSN requirements, best practices, and processes. If demand for support exceeds resources, establishes prioritization for support to achieve TSN.

b. Advises and guides the DoD Component heads in applying processes, tools, techniques, and methods to minimize vulnerabilities and risk of malicious intent in procured and developed software and hardware for applicable systems.

c. Defines processes, tools, techniques, and standards to effectively test newly developed and acquired DoD software and hardware for applicable systems.

d. Supports DoD Components with assessment of software analysis tools and practices and provides guidance on software and hardware vulnerability reduction and malicious intent identification to enable acquisition programs to manage risk effectively.

2.6. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA).

Under the authority, direction, and control of the USD(I&S), and in addition to the responsibilities in Paragraph 2.9., the Director, DIA:

a. Produces intelligence and counterintelligence threat assessments to support the DoD's mission and provides them to requesting parties in a timely manner relative to acquisition life cycles.

b. In coordination with the USD(R&E), the DoD CIO, the USD(A&S), the USD(I&S), and the DoD Component heads, operates and prioritizes support to conduct threat analysis of suppliers of critical ICT components when demand for support exceeds resources.

c. Notifies the DoD CIO; the USD(R&E); the USD(A&S); the USD(I&S); the Secretaries of the Military Departments; the Commander, USCYBERCOM; and the Director, Defense Counterintelligence and Security Agency of critical, high, and select medium threats on ICT supplier threat ratings.

d. Assesses significant ICT supply chain threats to national security systems.

2.7. DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY.

Under the authority, direction, and control of the USD(I&S), in addition to the responsibilities in Paragraph 2.9., and in accordance with Paragraphs 2.2, 4.1, and 11.2 of Volume 1 of DoD Manual 5220.32, the Director, Defense Counterintelligence and Security Agency:

a. Grants facility and personnel security clearances for contractors who require access to classified information to perform classified contracts and as requested by DMEA for the accreditation of trusted suppliers.

b. Provides counterintelligence reporting and provides counterintelligence awareness and reporting advice and assistance to cleared contractors, in accordance with applicable contracts.

c. Accredits contractor classified information systems at cleared contractor facilities.

2.8. UNDER SECRETARY OF DEFENSE FOR POLICY.

The Under Secretary of Defense for Policy:

a. In coordination with the broader Technology Security and Foreign Disclosure community, the USD(R&E); the DoD CIO; the USD(A&S); the USD(I&S); the DIRNSA/CHCSS; the Director, National Geospatial-Intelligence Agency; the Secretaries of the Military Departments; and others as required, establishes security policy for foreign national participation in system integration activities that support defense exportability and foreign military sales.

b. Oversees policy for DoD activities and efforts related to international technology transfer in accordance with DoDI 2040.02.

2.9. DOD COMPONENT HEADS.

The DoD Component heads:

a. Establish and maintain an operational TSN program to enable risk owners to identify, assess, and manage engineering risks.

b. Establish and maintain an operational ICT SCRM program to enable acquisition risk owners to identify, assess, and manage ICT supply chain risks.

c. Integrate engineering, acquisition, intelligence, counterintelligence, security, and risk management into DoD Component-level TSN and ICT SCRM activities and incorporate enterprise resources as appropriate.

d. Designate a focal point and resources to represent the acquisition executive; risk management executive; and counterintelligence, security, and operational communities with access to the DoD Component's research, development, acquisition, sustainment activities, and ICT supply chain risk analyses for applicable systems to:

(1) Determine and prioritize requests for threat analysis of suppliers of critical components in accordance with DoDI O-5240.24 and share findings.

(2) Determine and prioritize requests for using DoD Component and enterprise ICT supply chain resources, TSN and ICT SCRM subject matter experts, and tools, including using JFAC hardware and software assurance capabilities, as appropriate.

(3) Establish basic ICT supply chain risk due diligence capabilities for decision support and continual monitoring of suppliers for high-interest commodity ICT and critical acquisitions.

e. Establish TSN processes to assess vulnerabilities and manage risk to the assurance in the applicable system by:

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

(2) Requesting threat analysis for critical component suppliers and managing access to and control of threat analysis products, in accordance with DoDI O-5240.24.

(3) Applying guidance on managing identified risk using DoD Component and enterprise risk management resources.

(4) Applying assurance best practices, processes, techniques, and procurement tools as appropriate before procuring or integrating critical components into applicable systems at any point in the system life cycle to include consideration of use of the authority in Section 3252 of Title 10, U.S.C. as implemented in DFARS Part 239.7306.

(5) Using software assurance and hardware assurance tools and practices available through the JFAC, as appropriate.

(6) Documenting risk mitigation activities in program protection plans and relevant cybersecurity plans and documentation in accordance with DoDIs 5000.83 and 8500.01 and the Cybersecurity Strategy Outline and Guidance.

f. Assign analysts to assist the Director, DIA to conduct a threat analysis of suppliers of critical ICT components and share supply chain threat information with other DoD Components and the broader IC.

g. Develop and implement DoD Component-specific TSN and ICT SCRM training.

h. Execute, as applicable, actions taken by an authorized individual pursuant to DFARS Parts 239.7305(a), (b), or (c), and reporting to the USD(A&S) such actions taken during the annual reporting period.

i. Notify the USD(I&S) and the DIRNSA/CHCSS of discovered or suspected ICT supply chain exploits for further analysis and mitigation.

j. Establish DoD Component-level policy, processes, guidance, and mitigations that integrate DoD Component-unique TSN and ICT SCRM concepts in accordance with enterprise-level ICT SCRM and TSN policies.

k. Provide software and hardware assurance capabilities and resources and support the JFAC in accordance with Section 937 of Public Law 113-66, also known as NDAA for FY 2014, and DoD Policy Memorandum 15-001. Share supplier threat information with other DoD Components and other U.S. Government entities with mission interdependencies at appropriate classification levels.

2.10. SECRETARIES OF THE MILITARY DEPARTMENTS.

In addition to the responsibilities in Paragraph 2.9., the Secretaries of the Military Departments:

a. In coordination with the USD(R&E); the DoD CIO; the USD(A&S); the USD(I&S); and the Commander, USCYBERCOM, review intelligence and counterintelligence assessments of known ICT supplier threats and determine associated risks affecting DoD information systems, networks, weapon systems, and defense critical infrastructure. Identify ICT supply chain risks and indicate whether the risk applies to an individual procurement transaction only or to a class of procurements and direct or recommend specific mitigation actions.

b. Pursuant to Section 3252 of Title 10, U.S.C. and DFARS Part 239.73, make determinations and take actions for their Military Department when necessary to protect national security by reducing ICT supply chain risk. In accordance with Section 3252(c) of Title 10, U.S.C. and DFARS Part 239.7303(b), the Secretaries of the Military Departments may delegate this responsibility no lower than the service acquisition executive for the department concerned.

c. Send required congressional notifications for any determinations made by the Military Department to exclude products or sources from procurement based on identification of supply chain risk pursuant to Section 3252 of Title 10, U.S.C. and DFARS Part 239.73.

d. Provide notice to the USD(A&S) of all actions taken pursuant to DFARS Parts 239.7305(a), (b), or (c) during the annual reporting period, for consolidated annual reporting.

2.11. COMMANDER, USCYBERCOM.

In addition to the responsibilities in Paragraph 2.9., the Commander, USCYBERCOM:

a. In coordination with the USD(R&E), the DoD CIO, the USD(A&S), the USD(I&S), and the Secretaries of the Military Departments, reviews intelligence and counterintelligence assessments of known ICT supplier threats and determines associated risks affecting DoD information systems, networks, weapon systems, and defense critical infrastructure. Identifies ICT supply chain risks in accordance with Section 3252 of Title 10, U.S.C. and directs or recommends specific mitigation actions.

b. Takes all necessary and appropriate actions to secure, defend, and operate the DOD information network in accordance with existing authorities, to include:

(1) In coordination with the Director, National Security Agency, may independently conduct operational and technical observations and assessments in support of the use of the authority in Section 3252 of Title 10, U.S.C..

(2) Periodically monitor the DOD information network for DoD use of hardware, software, or services that have been excluded from acquisition actions pursuant to Section 3252 of Title 10, U.S.C.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CNSSI	Committee on National Security Systems Instruction
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DMEA	Defense Microelectronics Activity
DoD CIO	DoD Chief Information Officer
DoDI	DoD instruction
IC	intelligence community
ICT	information and communications technology
JFAC	Joint Federated Assurance Center
NDAA	National Defense Authorization Act
SCRM	supply chain risk management
TSN	trusted systems and networks
U.S.C.	United States Code
USCYBERCOM	United States Cyber Command
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
all-source intelligence	Defined in DoD Dictionary of Military and Associated Terms.

TERM	DEFINITION
assurance	A level of confidence that systems, including hardware, software, supply chains, and their constituent elements, function as intended, and only as intended, and are free of known vulnerabilities, either intentionally or unintentionally designed, or inserted as part of the system throughout the life cycle.
control system	Defined in National Institute of Standards and Technology Special Publication 800-82.
critical component	A component that is or contains ICT, including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and that delivers or protects mission critical functionality of a system or, 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 that systems engineers perform to identify mission critical functions and components. This includes identifying 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.
cybersecurity	Defined in Committee on National Security Systems Instruction (CNSSI) No. 4009.
defense critical infrastructure	Defined in DoD Dictionary of Military and Associated Terms.
enclave	Defined in CNSSI No. 4009.
hardware assurance	The confidence that hardware functions as intended and is free of known vulnerabilities either intentionally or unintentionally designed or inserted as part of the hardware throughout the life cycle.
high-interest commodity ICT	Commercial off-the-shelf or other non-developmental ICT requiring risk attention due to some or all of these factors: high volume of use; elevated importance due to its functions; or frequent use in systems, networks, or weapon systems.

TERM	DEFINITION
ICT	Includes all categories of ubiquitous technology used for gathering, storing, transmitting, retrieving, or processing information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, networks). ICT is not limited to information technology as defined in Section 11101 of Title 40, U.S.C. but reflects the merging of information technology and communications.
ICT SCRM	Also called "cyber SCRM," it is the process of identifying, assessing, and mitigating the supply chain risks associated with the development and use of distributed and interconnected information technology/operational technology and ICT product and service supply chains. The term is derived and modified for DoD use from National Institute of Standards and Technology documents and publications, to include National Institute of Standards and Technology Special Publication 800-161 and National Institute of Standards and Technology Interagency or Internal Report 8276.
ICT supply chain risk	The risk that any person may sabotage, maliciously introduce an unwanted function to, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or system to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such a system.
information system	Defined in CNSSI No. 4009.
information systems security engineering	Defined in CNSSI No. 4009.
mission critical functions	Any system function whose compromise would degrade the integrity or effectiveness of that system in achieving the core mission for which it was designed.
national security systems	Defined in Section 3552 of Title 44, U.S.C.
operational technology	The hardware, software, and firmware components of a system used to detect or cause changes in physical processes through the direct control and monitoring of physical devices.
simplified acquisition procedures	Defined in the Defense Acquisition University Glossary of Defense Acquisition Acronyms and Terms.

TERM	DEFINITION
software assurance	The level of confidence that software functions as intended and is free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the life cycle.
supply chain illumination	Continual visibility throughout the supply chain that provides an understanding of the tiers of a supply chain, a supply chain map, and vetting of suppliers against a defined set of supply chain criteria to identify and defend against threats.
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.
TSN	A state of security of a system or network in which its functions and components that are critical to conducting the system's intended missions have been protected from intentional malicious insertion-related threats and attacks to an acceptable level of risk through the use of robust systems engineering, system security engineering, ICT SCRM, security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, and information systems security engineering disciplines.
vulnerability	Defined in CNSSI No. 4009.

REFERENCES

Committee on National Security Systems Directive No. 505, "Supply Chain Risk Management," November 5, 2021

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," current edition

Defense Acquisition University Website, "DAU Glossary of Defense Acquisition Acronyms and Terms," https://www.dau.edu/glossary/Pages/Glossary.aspx

Defense Federal Acquisition Regulation Supplement, current edition

Deputy Secretary of Defense Memorandum, "Procedures for Supply Chain Risk Management in Support of DoD Trusted Systems and Networks," August 20, 2021

DoD Directive 5101.18E, "DoD Executive Agent for Printed Circuit Board and Interconnect Technology," June 12, 2016, as amended

DoD Directive 5137.02, "Under Secretary of Defense for Research and Engineering (USD(R&E))," July 15, 2020

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014, as amended

DoD Instruction 3020.45, "Mission Assurance Construct," August 14, 2018, as amended

DoD Instruction 4140.67, "DoD Counterfeit Prevention Policy," February 2, 2024

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," January 23, 2020, as amended

DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020, as amended

DoD Instruction 5000.90, "Cybersecurity for Acquisition Decision Authorities and Program Managers," December 31, 2020

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, as amended

DoD Manual 5220.32, Volume 1, "National Industrial Security Program: Industrial Security Procedures for Government Activities," August 1, 2018, as amended

DoD Policy Memorandum 15-001, "Joint Federated Assurance Center (JFAC) Charter," February 9, 2015

Federal Acquisition Regulation, current edition

Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, January 19, 2017

National Institute of Standards and Technology Interagency or Internal Report 8276, "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry," February 2021

National Institute of Standards and Technology Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security," current edition

National Institute of Standards and Technology Special Publication 800-161, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," current edition

National Security Presidential Directive-54/Homeland Security Presidential Directive-23, "Cybersecurity Policy," January 8, 2008

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

Office of the DoD Chief Information Officer, "Cybersecurity Strategy Outline and Guidance," current edition

Public Law 113-66, Section 937, "National Defense Authorization Act for Fiscal Year 2014," December 26, 2013

Public Law 114-328, Section 231, "National Defense Authorization Act for Fiscal Year 2017," December 23, 2016

Public Law 115-91, Sections 807 and 1659, "National Defense Authorization Act for Fiscal Year 2018," December 12, 2017

Public Law 115-232, Sections 889 and 1613, "John S. McCain National Defense Authorization Act for Fiscal Year 2019," August 13, 2018

Under Secretary of Defense for Acquisition, Technology, and Logistics and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "Report on Trusted Defense Systems in Response to National Defense Authorization Act, Section 254," December 22, 2009[1]

United States Code, Title 10, Section 3252

United States Code, Title 40, Section 11101

United States Code, Title 44, Section 3552

[1] Available on the Internet at https://rt.cto.mil/wp-content/uploads/2019/06/TrustedSystems-Exec_Summ-wAddendum-wTitlePgNoteinPDF.pdf