DoD Instruction 5200.50

Assured Access to Trusted Microelectronics

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective:	June 27, 2025
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Approved by:	Emil Michael, Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive 5137.02 and the requirements in Section 231(d) of Public Law 114-328, as amended by Section 276(3) of Public Law 116-283, this issuance establishes policy, assigns responsibilities, and provides procedures to ensure the DoD's assured access to trusted microelectronics.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance 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 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").

1.2. POLICY.

To ensure assured access to trusted microelectronics for the DoD and to mitigate threats from adversaries that put at risk microelectronics supply chains and the performance of DoD microelectronics systems and technologies, the DoD will:

a. Employ risk-based assessments to inform decisions on microelectronics systems, technologies, and services.

b. Improve and expand the microelectronics innovation ecosystem.

c. Increase the supplier base for microelectronics.

d. Ensure robust sustainment of microelectronics technology for DoD applications.

e. Assess future DoD microelectronics needs.

SECTION 2: RESPONSIBILITIES

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

The USD(R&E):

a. Establishes DoD education and training to advance the microelectronics-related knowledge base and capabilities of the DoD.

b. Establishes and maintains efforts, including public-private partnerships, grants, and other cooperative agreements, to:

(1) Advance the next generation of microelectronics technology.

(2) Identify, develop, and mature the future science and technology and engineering microelectronics workforce.

c. In coordination with the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)):

(1) Develops and promotes best practices for assured access to trusted microelectronics.

(2) Develops and maintains methods, practices, and technologies for the evidence-based assurance of microelectronics in DoD systems.

(3) Provides strategic guidance for technical requirements of microelectronics. including radiation-hardened microelectronics and security and exportability of DoD systems.

2.2. USD(A&S).

The USD(A&S):

a. Establishes and maintains efforts, including contracts, public-private partnerships, grants, and other cooperative agreements, to obtain, preserve, and enhance assured access to a trusted microelectronics supplier base as needed by DoD programs.

b. Provides DoD programs and defense contractors with assured access to trusted microelectronics, including trusted state-of-the-art (SOTA) microelectronics, either:

(1) Directly through Defense Microelectronics Activity (DMEA) accredited trusted suppliers, where appropriate; or

(2) Through long-term, enterprise-wide, assured access contracts executed by the DMEA.

c. In coordination with the USD(R&E):

(1) Through the DMEA:

(a) Establishes processes to assess current and future DoD microelectronics needs to assure the DoD has access to trusted microelectronics, including trusted SOTA microelectronics.

(b) Establishes procedures and criteria enabling assured access to trusted microelectronics and the use of evidence-based assurance.

(2) Establishes guidance for assured access to trusted microelectronics for the DoD.

d. Through the DMEA:

(1) Establishes and expands assured access to trusted microelectronics, including trusted SOTA microelectronics, as needed.

(2) Establishes criteria for accrediting trusted suppliers and guidance for using DMEA accredited trusted suppliers to support DoD microelectronics needs.

(3) Provides guidance, technologies, or support to programs, as requested, to ensure assured access to trusted microelectronics.

2.3. DOD CHIEF INFORMATION OFFICER.

The DoD Chief Information Officer supports assured access to trusted microelectronics in accordance with DoD Instructions (DoDIs) 5000.82, 5000.83, 5000.90, 5200.44, and 8500.01.

2.4. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)).

The USD(I&S):

a. Oversees security activities to help enable assured access to trusted microelectronics in accordance with DoDI O-5240.24.

b. Coordinates with the Intelligence Community to ensure that such security activities are fully informed by threats and risks.

2.5. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE.

Under the authority, direction, and control of the USD(I&S) and in addition to the responsibilities in Paragraph 2.7., the Director, National Security Agency/Chief, Central Security Service, provides capabilities and analysis tools to support assured access to trusted microelectronics as it relates to the National Security Agency's cryptographic mission in accordance with National Security Directive 42.

2.6. UNDER SECRETARY OF DEFENSE FOR POLICY.

The Under Secretary of Defense for Policy:

a. Provides policy oversight for international technology transfer activities that support assured access to trusted microelectronics in accordance with:

(1) DoD Directive 5111.01.

(2) Subchapter C of Chapter VII of Title 15, Code of Federal Regulations (also known as the "Export Administration Regulations").

(3) Subchapter M of Chapter I of Title 22, Code of Federal Regulations (also known as the "International Traffic in Arms Regulations").

b. Establishes policy for international partners and allies to participate in the microelectronics innovation ecosystem to support assured access to trusted microelectronics for the DoD.

2.7. DOD COMPONENT HEADS.

The DoD Component heads:

a. Establish Component policies, plans, and procedures to implement this issuance.

b. Provide expertise, analysis capabilities, and other resources, as needed, to support assured access to trusted microelectronics.

c. Procure custom designed or custom manufactured microelectronics from DMEA accredited trusted suppliers, when available and in accordance with DoDI 5200.44.

d. Use one or more of the following, as appropriate, to meet DoD microelectronics needs based on availability and applicability of an approved approach:

(1) DMEA accredited trusted suppliers.

(2) Evidence-based assurance.

(3) Risk-based methods approved by the DoD Component head after considerations of the factors in DoDI 5200.44.

e. Ensure records and information established and created in accordance with this issuance are retained in accordance with DoDI 5015.02 and DoD Component records management disposition schedules.

SECTION 3: PROCEDURES

3.1. GENERAL.

Microelectronics and their supporting supply chains face unprecedented and constantly changing and evolving security risks that threaten national security and the performance of DoD systems and technologies. Assured access to trusted microelectronics:

a. Employs tools, best practices, industry standards, and methods to mitigate the risks of adverse impacts to or from microelectronics.

b. Extends throughout the life cycle of microelectronics from initial concept to final disposal.

3.2. ASSURED ACCESS TO TRUSTED MICROELECTRONICS.

Microelectronics products and services for DoD systems are most often obtained from a global supply chain. This requires the DoD to have multiple options to maintain assured access to trusted microelectronics by managing the risks from supply chain disruptions and malicious activity during all phases of design, manufacturing, packaging, test, and distribution. The DoD will:

a. Safeguard controlled unclassified information, including controlled unclassified technical information, export-controlled information, and proprietary business information (e.g., intellectual property), in accordance with DoDIs 3200.12, 5200.48, and 5230.24.

b. Safeguard classified information in accordance with Volume 2 of DoD Manual 5200.01.

c. Use DMEA accredited trusted suppliers, in accordance with DoDI 5200.44.

d. Actively manage diminishing manufacturing sources and material shortages (e.g., potential for technology end-of-life), in accordance with DoDI 4245.15.

e. Where appropriate, request guidance or support from the DMEA to ensure assured access to trusted microelectronics and mitigate or resolve research, prototyping, and acquisition issues.

3.3. EVIDENCE-BASED ASSURANCE.

DoD Components will use evidence-based assurance to justify the claim that risks have been mitigated in support of DoD systems and technology needs. Evidence-based assurance will be used, as applicable, to inform to inform decisions on microelectronics systems, technologies, and services used in DoD systems. Evidence-based assurance will consider, among other factors:

a. Third-party intellectual property strategy to identify and manage the full spectrum of intellectual property and related microelectronics matters, in accordance with DoDI 5010.44.

b. Microelectronics security features.

c. Microelectronics test verification and validation results.

d. Anti-counterfeiting best practices in accordance with DoDI 4140.67.

e. The use of a DMEA accredited trusted supplier.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
DMEA	Defense Microelectronics Activity
DoDI	DoD instruction
SOTA	state-of-the-art
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
assured access	The ability of the DoD to guarantee the availability of microelectronics parts at the necessary volumes and with the performance characteristics required to meet the needs of the DoD.
DMEA accredited trusted suppliers	Suppliers of microelectronics and microelectronics services that have been accredited by the DMEA as being sufficiently trustworthy for the design, manufacturing, test, or distribution of microelectronic components used in national security systems based on evidence-based assurance of the integrity of the associated people and processes.
evidence-based assurance	Justified confidence that assurance has been or will be achieved through a risk-informed, logical evaluation of evidence supported by data.
microelectronics innovation ecosystem	All entities involved in microelectronics technology development from early research concepts through incorporation into systems or products.
national security system	Defined in Section 3552(b)(6)(A) of Title 44, U.S.C.

TERM	DEFINITION
SOTA microelectronics	Microelectronics that embody the latest advancements in technology, design, and manufacturing processes.
trusted microelectronics	Microelectronics that the DoD can trust to function as intended and that are free of exploitable vulnerabilities either intentionally or unintentionally designed or inserted as part of a system at any time during the life cycle of the system.

REFERENCES

Code of Federal Regulations, Title 15, Chapter VII, Subchapter C (also known as the "Export Administration Regulations")

Code of Federal Regulations, Title 22, Chapter I, Subchapter M (also known as the "International Traffic in Arms Regulations")

DoD Directive 5111.01, "Under Secretary of Defense for Policy (USD(P))," June 23, 2020

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

DoD Instruction 3200.12, "DoD Scientific and Technical Information Program (STIP)," August 22, 2013, as amended

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

DoD Instruction 4245.15, "Diminishing Manufacturing Sources and Material Shortages Management," November 5, 2020

DoD Instruction 5000.82, "Requirements for the Acquisition of Digital Capabilities," June 1, 2023

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 5010.44, "Intellectual Property (IP) Acquisition and Licensing," October 16, 2019

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks," February 16, 2024

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

DoD Instruction 5230.24, "Distribution Statements on DoD Technical Information," January 10, 2023

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

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

DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Information," February 24, 2012, as amended

National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems (U)" July 5, 1990

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

Public Law 116-283, Section 276(3), "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021," January 1, 2021

United States Code, Title 44, Section 3552(b)(6)(A)