DoD INSTRUCTION 5000.82

REQUIREMENTS FOR THE ACQUISITION OF DIGITAL CAPABILITIES

Originating Component:	Office of the DoD Chief Information Officer
Effective:	June 1, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 5000.82, "Acquisition of Information Technology (IT)," April 21, 2020
Approved by:	John B. Sherman, Chief Information Officer of the Department of Defense

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for the acquisition of digital capabilities.
- Assigns program responsibilities concerning the acquisition of digital capabilities as defined in this issuance for the acquisition pathways of the adaptive acquisition framework described in DoD Instruction (DoDI) 5000.02.
- Describes the responsibilities and procedures of principal acquisition officials in the acquisition of programs containing information technology (IT), including national security systems (NSS) within DoD authorities, across all acquisition pathways.

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to the OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) 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").

b. Requirements in this issuance are applicable to acquisition programs containing IT (including NSS within DoD authorities and defense business systems) regardless of dollar value or acquisition pathway.

1.2. POLICY.

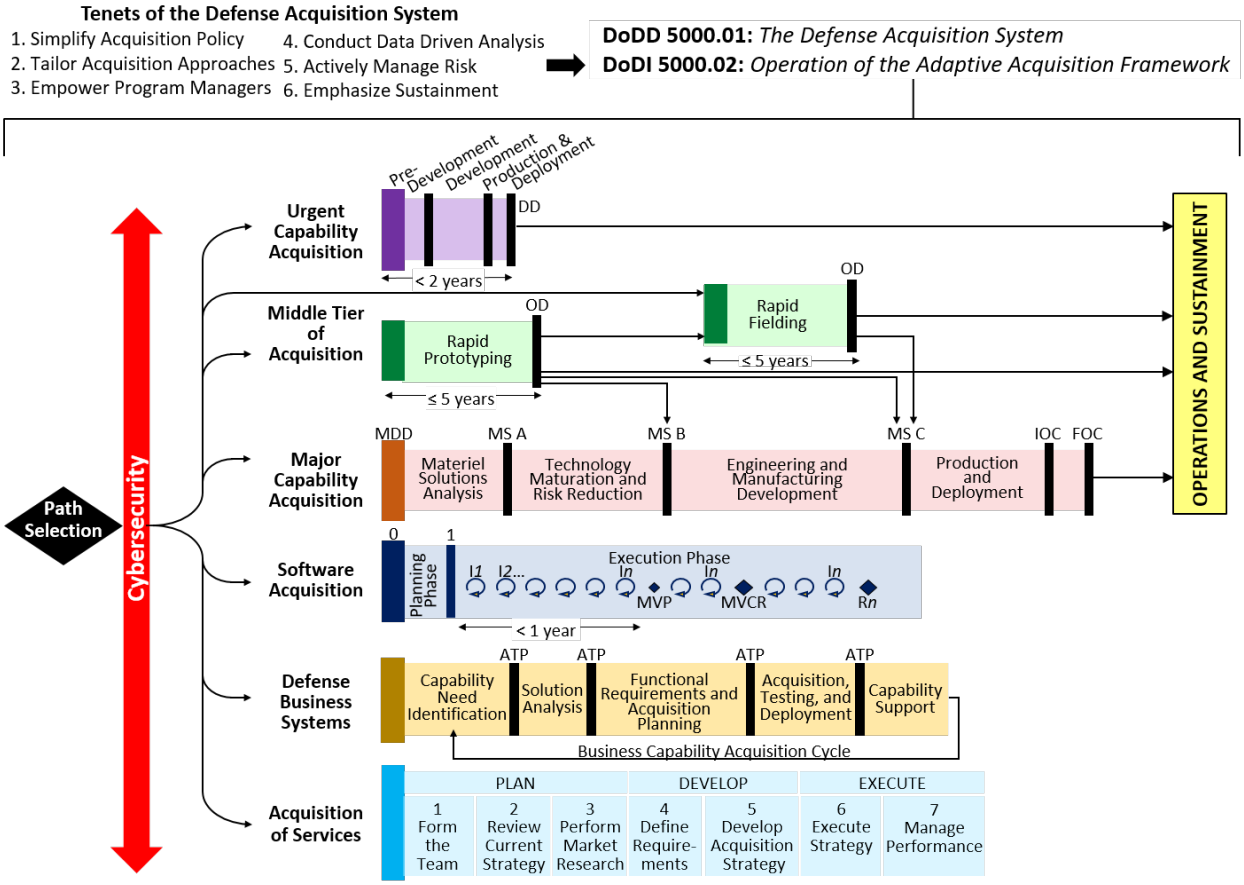
a. The acquisition of digital capabilities, as defined for the purposes of this issuance, supports the National Defense Strategy and the DoD Digital Modernization Strategy – DoD Information Resource Strategic Plan Fiscal Years 2019-2023 (also known and referred to in this issuance as the "DoD Digital Modernization Strategy"), and aligns with DoD IT, cybersecurity, and supply chain risk management (SCRM) policies, enterprise architectures, and technology and data standards. This alignment results in the delivery of interoperable, secure, survivable, and operationally resilient digital capabilities across the joint force.

b. Procurements, including vendor or contractor provided procurements, not specifically addressed in this issuance must be authorized by the contracting officer.

1.3. DEFENSE ACQUISITION SYSTEM (DAS) REALIGNMENT PLAN.

The overarching management principles that guide the DAS are described in DoDD 5000.01 and DoDI 5000.02. The DAS supports the National Defense Strategy by developing a lethal and effective force based on American technological innovation, and a culture of performance that yields decisive and sustained U.S. military advantage. To achieve this objective, the DoD will employ an adaptive acquisition framework comprised of acquisition pathways (see Figure 1), each with unique characteristics of the capability being acquired.

Figure 1. Adaptive Acquisition Framework



Legend:

ATP: Authority to Proceed	DD: Disposition Decision	FOC: Full Operational Capability
I: Iteration	IOC: Initial Operational Capability	MDD: Materiel Development Decision
MS: Milestone	MVCR: Minimum Viable Capability Release	MVP: Minimum Viable Product
OD: Outcome Determination	R: Release	

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (CIO).

The DoD CIO:

a. Establishes policies and prescribes procedures relating to digital capabilities as defined in this issuance and acquired as part of all programs and systems, across all the acquisition pathways defined in DoDI 5000.02, and for all DoD Components.

b. Provides and maintains:

(1) DoD cybersecurity policies pertaining to IT system and system component developers who manage programs that produce cyber solutions in accordance with DoDI 5000.90.

(2) Guidance, standards, and tools that support DoD cybersecurity policies.

(3) DoD cybersecurity policies that affect the software acquisition pathway, including the processes, IT systems, and tools used to manage and develop software solutions.

c. Coordinates with the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), the Under Secretary of Defense for Research and Engineering (USD(R&E)), the Intelligence Community CIO, the Director of Operational Testing and Evaluation (DOT&E), the CJCS, and the Commander, Joint Interoperability Test Command on:

(1) Interpreting and implementing cybersecurity policies and associated guidance, standards, and tools that support the adaptive acquisition framework.

(2) Developing interoperability requirements.

(3) Interoperability test and certification.

(4) Overseeing IT interoperability in coordination with DoD Components and other mission partners.

(5) Cyber SCRM (C-SCRM).

(6) Operational resilience requirements.

d. Establishes processes and procedures to:

(1) Identify IT standards gaps in the acquisition of digital capabilities, as defined in this issuance, and requires mitigation plans for gaps in the absence of acceptable IT standards.

(2) Request policy exceptions in accordance with DoDIs 8330.01, 8320.02, and 8510.01.

e. In coordination with the USD(A&S) and Under Secretary of Defense for Intelligence and Security (USD(I&S)), prepares joint recommendations to protect national security by reducing supply chain risk in accordance with Section 3252 of Title 10, United States Code (U.S.C.), and the August 20, 2021 Deputy Secretary of Defense (DepSecDef) Memorandum.

2.2. USD(A&S).

The USD(A&S):

a. As the Defense Acquisition Executive (DAE), executes delegated statutory authorities on behalf of the Secretary of Defense, when necessary, to protect national security by reducing supply chain risk in accordance with relevant authorities, including Section 3252 of Title 10, U.S.C., Section 1323 of Title 41, U.S.C., and the August 20, 2021 DepSecDef Memorandum. This includes related work directly supporting the Adaptive Acquisition Framework in accordance with DoDI 5000.02.

b. In coordination with the USD(R&E) and DoD CIO, requires that SCRM is a key acquisition process consideration in accordance with DoDI 5200.44.

c. In coordination with the CJCS, DoD CIO, DOT&E, USD(I&S), and USD(R&E), establishes cyber survivability requirements, engineering, and testing processes for acquisition and risk assessment, mitigation, and remediation processes for sustainment.

2.3. USD(R&E).

The USD(R&E):

a. Provides the underpinning research, technology development, and technical advice to the DoD CIO and the Commander, United States Cyber Command, in:

(1) Operationalizing command and control.

(2) Positioning, navigation, and timing alternatives.

(3) Electromagnetic spectrum management to better inform DoD policies.

b. Provides policy and procedures for:

(1) Technology and program protection in accordance with DoDI 5000.83.

(2) Engineering defense systems in accordance with DoDI 5000.88.

(3) Test and evaluation in accordance with DoDI 5000.89.

c. In coordination with the DoD CIO, provides policy and procedures for SCRM in accordance with DoDI 5200.44 and the August 20, 2021 DepSecDef Memorandum.

d. Ensures appropriate test facilities, test ranges, tools, and related modeling and simulation capabilities are maintained within the DoD to support test and evaluation (T&E) for the acquisition of digital capabilities, as defined in this issuance.

2.4. USD(I&S).

The USD(I&S):

a. Advises the DoD CIO on security, intelligence, and counterintelligence requirements to support the acquisition of digital capabilities, as defined in this issuance, including NSS in coordination with the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS).

b. Advises the DoD Component heads on security, counterintelligence, and intelligence matters that:

(1) Support acquisition programs containing a component of IT, networking, cybersecurity, electromagnetic spectrum, or position, navigation, and timing (PNT), where the Component acquisition executive (CAE) is the milestone decision authority (MDA).

(2) Are related to requests for exceptions to policy.

(3) Address identified gaps in IT standards and mitigation plans in the absence of acceptable standards.

(4) Provide risk assessment when there is basis to identify a significant supply chain risk to an NSS, in accordance with Section 3252 of Title 10, U.S.C.

c. Defines roles to support intelligence responsibilities in accordance with DoDI 5200.44 and the August 20, 2021 DepSecDef Memorandum.

2.5. DIRNSA/CHCSS.

Under the authority, direction, and control of the USD(I&S); the authority, direction, and control exercised by the DoD CIO over the activities of the Cybersecurity Directorate, or any successor organization, of the National Security Agency, funded through the Information System Security Program; and in addition to the responsibilities in Paragraph 2.7., the DIRNSA/CHCSS, as the National Manager for NSS and in coordination with the DoD Chief Information Security Officer, exercises authority over the security of DoD-identified NSS, in accordance with the National Security Directive 42.

2.6. DOT&E.

The DOT&E:

a. Provides policy and procedures for the operational testing of acquisition programs, and provides oversight of designated programs in accordance with Sections 139, 4172, and 4171 of Title 10, U.S.C.

b. Approves T&E plans for programs under their purview.

c. In coordination with the USD(R&E), provides support to acquisition program managers (PMs) in performing T&E.

2.7. DOD COMPONENT HEADS.

The DoD Component heads will ensure that their Component CIOs identify gaps in IT standards and mitigation plans in the absence of acceptable standards and, when necessary, submit requests for exceptions to policy to the DoD CIO. Statutory requirements may not receive exceptions, unless authorized in statute.

2.8. SECRETARIES OF THE MILITARY DEPARTMENTS AND COMMANDANT OF THE U.S. COAST GUARD.

In addition to the responsibilities in Paragraph 2.7., the Secretaries of the Military Departments and Commandant of the U.S. Coast Guard will appoint a Principal Cyber Advisor to:

a. Report directly to the Secretary of the Military Department or Commandant, providing advice regarding all cyber matters affecting the Military Service concerned.

b. Advise the Military Department on implementing the DoD Cyber Strategy by coordinating and overseeing execution of the Military Department's policies and programs relevant to:

(1) Cybersecurity management of DoD information systems.

(2) Acquisition of cybersecurity tools and capabilities.

(3) Establishment of a cybersecurity warfighting culture.

(4) Related cyber SCRM.

c. Take necessary action to protect national security by reducing supply chain risk in accordance with the provisions of Paragraph (b) of Section 3252 of Title 10, U.S.C.

SECTION 3: PROCEDURES

3.1. GENERAL.

MDAs, decision authorities (DAs), IT functional sponsors, PMs, and functional service managers (FSMs) will ensure that their programs containing a component of IT, networking, cybersecurity, electromagnetic spectrum, or PNT follow the guidance provided in this issuance as it pertains to:

a. IT, as defined in Section 11101 of Title 40, U.S.C.

b. NSS, as defined in Section 3552 of Title 44, U.S.C.

c. Information systems, as defined in Section 3502 of Title 44, U.S.C.

d. Enterprise architecture, as defined in Section 3601(4) of Title 44, U.S.C.

e. Information security, as defined in Section 3552 of Title 44, U.S.C.

f. Information and communications technology (ICT), as defined in DoD Manual (DoDM) 8400.01 and in DoDI 5200.44.

g. IT services, as defined in this issuance.

h. Modular open systems approach for IT, as defined in Section 4401 of Title 10, U.S.C. and Section 801(b through d) of Public Law 113-291.

i. Operations security, as defined in National Security Presidential Memorandum 28 and in accordance with DoDI 5205.08.

3.2. CLINGER-COHEN ACT (CCA) COMPLIANCE.

a. Overall Concept.

(1) Subtitle III of Title 40, U.S.C., also known and referred to in this issuance as Divisions D and E of the CCA, applies to all IT investments, including NSS within DoD authorities.

(2) For all programs that acquire digital capabilities as defined in this issuance, including NSS, regardless of acquisition pathway, acquisition category (ACAT) level, or business category (BCAT) level, and for all IT service acquisitions, the MDA or DA will not initiate a program nor an increment of a program, approve entry into any phase of the acquisition process that requires formal MDA or DA approval, or authorize execution of a contract for the applicable acquisition phase until:

(a) The sponsoring DoD Component, PM, or FSM provides a plan to the MDA or DA to satisfy the applicable acquisition requirements of the CCA. The plan will use documentation already required as part of the acquisition pathway. The tables in the Adaptive Acquisition Framework Documentation Identification tool, (available at https://www.dau.edu/aafdid/Pages/about.aspx) will be used to identify the program information that supports CCA compliance:

1. For "Software Acquisition," the "CCA Compliance" table (available at https://www.dau.edu/aafdid/Pages/SWA-Clinger-Cohen-Act-Compliance.aspx) identifies the program information for software programs in accordance with DoDI 5000.87.

2. For "Major Capability Acquisition," the "CCA Compliance" table (available at https://www.dau.edu/aafdid/Pages/CCA-Compliance.aspx) identifies the program information for major capability, urgent, middle-tier, and defense business system programs in accordance with associated pathway policies.

(b) If required by the acquisition pathway, the sponsoring DoD Component, PM, or FSM provides the plan to the DoD CIO, DoD Component CIO, or their designee for approval.

(3) Changes to the acquisition strategy that invalidate the previous compliance conditions must be reported to the MDA or DA and must comply with the applicable requirements of this issuance as identified in this section.

b. Information Resources and Investment Management.

In coordination with the IT functional sponsor and DoD Component CIO, the PM will manage the acquisition to enable DoD-wide information resources and investment management. Acquisitions will:

(1) Align with DoD strategic priorities as defined in the National Defense Strategy and DoD Digital Modernization Strategy.

(2) Leverage available enterprise services, enterprise contracts, and commercial-off-the-shelf technology to the extent practicable to improve efficiencies.

(3) Sufficiently justify cost as defined in documentation already required as part of the adaptive acquisition pathway.

(4) Comply with the applicable requirements of this issuance.

(5) Be registered in the DoD IT Portfolio Repository or Secret IT Portfolio Repository to support IT portfolio management and rationalization analysis if applicable.

(6) Align with an investment registered in the DoD IT investment portal, Select and Native Programming Data Input System for Information Technology, to support the DoD budget.

c. Post-Implementation Review (PIR).

(1) In coordination with the IT functional sponsor and DoD Component CIO, the PM will develop a plan and conduct a PIR for all fully deployed digital capabilities as defined in this issuance, including NSS within DoD authorities.

(2) PIRs:

(a) Report the degree to which doctrine, organization, training, materiel, leadership, education, personnel, facilities, and policy changes have achieved the established measures of effectiveness for the desired capability.

(b) Evaluate systems for effectiveness and efficiency and decide whether continuation, modification, or termination of the system is necessary to meet mission requirements.

(c) Document lessons learned.

(3) PIR documentation requirements are provided in Table 1.

Table 1. PIR Documentation Requirements.

Acquisition Pathway	Requirement
Urgent Capability	PIR requirements will be included in the post-fielding assessment(s), the disposition assessment, and the disposition decision.
Middle Tier Capability	PIR requirements will be included in the test strategy or an assessment of test results, included in the acquisition strategy.
Major Capability	For major weapons systems, PIR requirements will be included in the initial operational T&E plans included in the T&E master plan. PIR requirements must be met before proceeding with full-rate production or full-deployment decision, as appropriate.
Software	PIR requirements will be included in the software acquisition value assessment.
Defense Business System	PIR requirements will be included in the capability support reviews during the capability support phase.
Services	PIR requirements will be included in the quality assurance surveillance plan and in the execution of this plan.

3.3. INFORMATION ENTERPRISE ARCHITECTURE (IEA).

a. The DoD IEA serves as a framework for DoD's "target state." It is intended to guide development of digital capabilities, as defined in this issuance, in alignment with policy and standards and to support continuous modernization.

b. The DoD IEA, including architecture guidance (e.g., reference architecture and reference designs), enables the improvement of IT and computing infrastructure, including business processes, interoperability, the application of IT and NSS standards, and managing information resources. Information resources management includes eliminating duplicate IT and NSS per authorities pursuant to Titles 10 and 40, U.S.C. All acquisitions of digital capabilities as defined in this issuance must be traceable to the DoD IEA as described in the appropriate acquisition guide at https://aaf.dau.edu/aaf.

c. IT standards employed must be selected from the current approved version of the DoD IT Standards Registry within the Global Information Grid Technical Guidance Federation service in accordance with DoDI 8310.01. The standards selected must be sufficient to enable the interoperability and cybersecurity required for joint operations in accordance with DoDIs 8330.01, 8320.02, and 8510.01.

d. All acquisitions of digital capabilities, as defined in this issuance, must be designed and developed, to the maximum extent practicable, with a modular open systems approach to enable incremental and agile development, to resist and respond to emerging or anticipated cyberspace threats, and to enhance competition, innovation, and interoperability in accordance with Section 4401 of Title 10, U.S.C.

e. The DoD IEA will be curated with reviews and approvals by the governing bodies responsible for its maintenance in accordance with Enterprise Architecture Executive Panel Terms of Reference and Digital Modernization Infrastructure Executive Committee Charter. All derived and associated reference architectures and designs will also be curated to maintain consistency and unity of effort by organizations that use these guiding documents. Annual verification and validation reports will be generated certifying the consistency of the DoD IEA, references architectures, and reference designs.

3.4. IT CATEGORY MANAGEMENT AND DOD ENTERPRISE SOFTWARE INITIATIVE (ESI).

a. When acquiring commercial IT, PMs, FSMs, and acquisition personnel must consider government contracting laws and regulations and suitability of using DoD IT category management best-in-class purchasing solutions, DoD ESI, Federal category management procurement vehicles, and DoD-wide joint enterprise license agreements and DoD Component-level enterprise software licenses. PMs and acquisition personnel will document these considerations in the acquisition strategy, including selection rationale. These purchasing vehicles and DoD ESI are not intended to dictate the products or services to be acquired.

b. PMs and acquisition personnel will document intellectual property considerations in the acquisition strategy in accordance with DoDI 5010.44.

3.5. CYBERSECURITY, OPERATIONAL RESILIENCE, AND CYBER SURVIVABILITY.

All acquisition of digital capabilities, as defined in this issuance, must incorporate cyber requirements, in accordance with DoDIs 8500.01 and 8530.01, including the operational mission-based design and assessment of survivability, operational resilience, cybersecurity risk management, and cyberspace defense. All cyber relevant requirements must be engineered into the design and specifications of the system and software based on mission risk to withstand cyber threats. PMs must apply all engineering policy, guidance, and principles to integrate and balance requirements, including cyber relevant requirements in accordance with DoDIs 5000.83 and 5000.88.

a. Cybersecurity Risk Management Framework (RMF) for Digital Capabilities.

Cybersecurity RMF steps and activities, as described in DoDI 8510.01, should be initiated as early as possible and fully integrated into the DoD acquisition process, including requirements management, systems and software engineering, and T&E. Integration of the RMF in acquisition processes can potentially reduce the effort to achieve authorization to operate (ATO) and subsequent security controls management requirements throughout the system life cycle.

b. Cybersecurity Strategy (CSS).

(1) All acquisitions containing IT, including NSS, will have a CSS, in accordance with DoDI 8500.01. The CSS is a statutory requirement, pursuant to Section 811 of Public Law 106-398, for mission essential and mission critical IT systems and a regulatory requirement for all IT systems in accordance with this issuance and DoDI 8580.1.

(2) The CSS outlines plans for, and implementation status of, projected cybersecurity activities across all phases of a system's lifecycle. The CSS is applicable to all adaptive acquisition framework pathways, and retains operational relevance beyond milestone and decision points into system sustainment.

(3) The program office and the system owner will actively review, update, employ, and maintain the CSS for the life of the system. The CSS is a foundational document to support the program office in the development of key program elements, including:

(a) Requirements generation and development.

(b) The program protection plan.

(c) T&E.

(d) Attaining and maintaining an ATO.

(e) Cyberspace defense, continuous monitoring, C- SCRM, and recurring cyber risk assessments in the operations and sustainment phase.

(f) Decommission and system disposal.

(4) Appropriate review of the CSS will take place as identified in Table 2.

Table 2. CSS Review Requirements

Acquisition Pathway	Requirement
Major Capability ACAT ID Pathway Programs	The PM will develop a CSS and obtain Component CIO and DoD CIO approval as part of the program protection plan before the MDA makes milestone decisions or provides an update to the program protection plan before contract awards are authorized.
Major Capability Non-ACAT ID Pathway Programs	The PM will develop a CSS as part of the relevant documentation that results in an acquisition strategy customized to the unique characteristics and risks of their program to gain approval from the respective CIO.
Defense Business System BCAT I Programs	The PM will develop a CSS and obtain Component CIO and DoD CIO approval as part of the program protection plan before the MDA makes milestone decisions or provides an update to the program protection plan before contract awards are authorized.
IT Services Services ACAT I Programs	The PM will develop a CSS as part of the relevant documentation that results in an acquisition strategy customized to the unique characteristics and risks of their program to gain approval from the respective CIO.
Urgent Capability Acquisition, Operation of the Middle Tier of Acquisition, Software Acquisition	The PM will develop a CSS as part of the relevant documentation that results in an acquisition strategy customized to the unique characteristics and risks of their program to gain approval from the respective CIO.
If the contract award is authorized as part of an acquisition milestone decision, a separate review of the CSS before contract award authorization is not required.	

(5) The approved CSS will be an appendix to the program protection plan in accordance with DoDI 5000.83. Otherwise, it will be a stand-alone required document.

c. C-SCRM.

(1) MDAs, DAs, IT functional sponsors, PMs, and FSMs will minimize ICT supply chain risks to DoD's warfighting capabilities, business, and enterprise information systems to maintain a technological advantage. The application of risk management practices will begin during the design of applicable systems and before the acquisition of critical programs and technology, ICT, critical components, or their integration within applicable systems, whether acquired through a commodity purchase, system acquisition, or sustainment process in accordance with DoDI 5200.44.

(2) DoD Components will manage C-SCRM risk by:

(a) Having the Component trusted systems and network focal point(s) determine and prioritize requests for threat analysis of suppliers of critical components.

(b) Assigning DoD Component specialists to assist the Director, Defense Intelligence Agency in conducting threat analysis of suppliers of critical components and submitting those requests, in accordance with DoDI 5200.44.

(c) Leveraging basic supply chain risk due diligence capabilities for decision support and continuous monitoring of suppliers for both ICT and critical items, in accordance with DoDI 5200.44.

(d) Engaging the relevant trusted systems and network focal point for guidance on managing identified risk using DoD Components and enterprise risk management resources, in accordance with DoDI 5200.44.

(e) Applying assurance best practices, processes, techniques, and procurement tools before acquiring or integrating critical components into applicable systems at any point in the system life cycle, in accordance with DoDI 5200.44.

(f) Implementing cyber T&E at the earliest opportunity for mission critical components and functions and potential supply chain risks, in accordance with DoDI 5200.44 and DoDI 5000.89.

(g) Implementing tailored acquisition strategies, contract tools, and procurement methods for critical components in applicable systems, including to ensure that Sections 252.239-7018 of the Defense Federal Acquisition Regulation Supplement (DFARS) as prescribed by Section 239.7306 of the DFARS is appropriately applied.

(h) Notifying the relevant MDA, authorizing official, and the DoD CIO of mission critical threats and vulnerabilities that cannot be reasonably addressed and verified through regular testing, technical mitigation, countermeasures, or risk management procedures in accordance with DoDI 5200.44.

(i) Reducing supply chain risk in accordance with Section 3252 of Title 10, U.S.C.

(j) Coordinating and collaborating with the DoD CIO to ensure supply chain risks that impact cybersecurity posture will be considered, tested, analyzed, and mitigated if possible, during cybersecurity assessments. This requires that applicable intelligence, counterintelligence, and security-related threats inform DoD CIO for deliberate and mitigating actions to reduce overall risks to DoD in accordance with DoDI 5200.44.

(k) Integrating operations security into the planning, execution, and assessment of supply chain risk management activities in accordance with DoDD 5205.02E and DoDI 4140.01.

d. Operational Resilience for Digital Capabilities.

(1) The operational resilience requirements for digital capabilities, as defined in this issuance, will be integrated and implemented with other systems engineering and systems security engineering requirements.

(2) Operational resilience must be verified and validated through rigorous developmental and operational T&E in accordance with DoDI 5000.89.

(3) Mission deficiencies in operational resilience must be reported, tracked, and remediated in accordance with DoDI 8510.01 and 5000.89.

e. Cyber Survivability for Digital Capabilities.

(1) All acquisitions of digital capabilities, as defined in this issuance, must incorporate, to the maximum extent practicable, the Joint Staff Cyber Survivability Attributes by following the Joint Capabilities Integration and Development System requirement for the cyber survivability endorsement as part of the mandatory system survivability key performance parameter in accordance with appropriate acquisition pathway policies.

(2) Cyber survivability must be verified and validated through rigorous developmental and operational T&E in accordance with DoDI 5000.89.

(3) Cyber survivability risk posture must be reported, tracked, and managed in accordance with DoDI 8510.01 and 5000.89.

3.6. COMMAND, CONTROL, AND COMMUNICATIONS.

a. Overall Concept.

Command, control, and communications systems are fundamental to all military operations, delivering critical information necessary to plan, coordinate, and control forces and operations across the full range of DoD missions.

b. Waveform Management.

DoD Components that acquire, develop, or modify IT NSS communications waveforms (systems or services), including wireless communications products and associated technologies, must comply with DoDI 4630.09.

c. Spectrum Supportability.

(1) PMs will submit written determinations, in coordination with the Defense Spectrum Organization and Joint Spectrum Center, to the DoD Component CIO or equivalent that the electromagnetic spectrum necessary to support the operation of the system during its expected life cycle is or will be available in accordance with DoDI 4650.01.

(2) DoD Component spectrum-dependent system developers will identify and mitigate regulatory, technical, and operational spectrum supportability risks in accordance with DoDI 4650.01.

d. PNT.

In accordance with the National Defense Strategy and DoDD 4650.05, DoD Components must recognize that resilient PNT information is essential to the execution, command, and control of military missions, and to the efficient operation of information networks necessary for continuous situational awareness by Combatant Commanders and other senior decision makers. All MDAs and DAs must determine and confirm navigation warfare compliance at each acquisition milestone for all platforms and systems producing or using PNT information in accordance with DoDI 4650.08.

e. Communications Programs of Record.

In accordance with Section 168 of Public Law 116-92 (also known and referred to in this issuance as "the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2020"), a current or future communications program of record may not be procured, unless the communications equipment:

(1) Mitigates geolocation of a transmission that would allow a like echelon enemy force to target the user.

(2) Securely communicates classified information in a contested communications environment that includes operationally representative jamming.

(3) Reduces, within 2 years of continued development and upgrades, electronic signature and susceptibility to geolocation by using low probability of intercept/detect waveforms, or other capability that would provide the same resiliency on the battlefield.

(4) Utilizes a waveform that is either made available through the Department of Defense Waveform Information Repository, or is a commercial off the shelf waveform available for government licensing with waveform analysis through the Joint Tactical Networking Center Tactical Communications Marketplace.

(5) Is otherwise eligible to be granted a waiver authority in accordance with Section 168(b) of the NDAA for FY 2020.

3.7. DATA CENTERS AND CLOUD SERVICES.

a. DoD Data Center Optimization.

Pursuant to Section 2867 of Public Law 112-81 (also known and referred to in this issuance as the "NDAA for FY 2012"), PMs will obtain DoD CIO approval before obligating funds for developing and modernizing data centers. This approval has been delegated to the DoD Component CIOs, except for obligations of development and modernization resources closing

within 12 months as reported in the DoD authoritative data center inventory, for data centers without a record in the DoD data center inventory, for the establishment of a new data center, or for the expansion of an existing data center beyond 18 percent of its current floor space.

(1) PMs supporting acquisitions on behalf of Military Departments will obtain approval from their Departmental CIO or in accordance with guidance issued by their CIO before obligating funds for data servers, data centers, or IT used in data centers.

(2) For Defense Agencies and DoD Field Activities, PMs will receive DoD CIO approval before obligating funds for data center requirements via the IT purchase request process.

b. Cloud Services.

(1) DoD Components will take full advantage of cloud services in alignment with and to achieve the goals of the DoD Digital Modernization Strategy and the requirements of Section 1064(d) of Public Law 115-232.

(2) DoD Components will ensure that no new system or application will be approved for development or modernization without an assessment that such a system or application is already, or can and would be, cloud-hosted without compromising the security or integrity of the capability or service delivery.

(3) DoD Components will ensure that their respective program executive offices take steps necessary to accelerate adoption of cloud-based digital infrastructure and development security operations that enables rapid deployment, scaling, testing, and optimization of software as an enduring capability.

(4) Before establishing new cloud computing contracts, DoD Components will leverage available enterprise cloud contracts to satisfy cloud computing requirements. Requests to use or establish contracts that duplicate functions provided by enterprise cloud contracts will require DoD CIO approval. A list of approved enterprise cloud contracts is available at https://intelshare.intelink.gov/sites/SWMod.

(5) PMs and FSMs will follow Subpart 239.76 of the DFARS when contracting for cloud services.

(6) PMs and FSMs will refer to and implement the current version of the DoD Cloud Computing Security Requirements Guide (CC SRG) when deciding to acquire, use, or implement any application, system, or service that leverages cloud services. The Defense Information Systems Agency publishes the CC SRG, which establishes the DoD security requirements for cloud services.

(a) PMs and FSMs will only acquire and use cloud services from a DoD or non-DoD cloud service provider that has been granted provisional authorization (PA) by the Defense Information Systems Agency at or above the information impact level required for the DoD information being processed or stored by the cloud service, in accordance with Subpart 239.76 of the DFARS. Cloud services possessing a PA are listed in the Defense Information Systems

Agency's DoD Cloud Service Catalog at https://dod365.sharepoint-mil.us/sites/DISA-RE-Apps/cas/SitePages/CASHome.aspx.

(b) PMs and FSMs will ensure cloud services of non-DoD providers are securely connected to DoD networks in accordance with the CC SRG and ensure via testing that the cybersecurity posture of the DoD is not compromised. Cybersecurity developmental, operational, or integrated T&E is required in emulated and live environments before operational use of any cloud service.

(7) PMs and FSMs will analyze cloud options and report all appropriate information on cloud service usage and investments for each cloud service within Defense Information Technology Investment Portal/Select and Native Programming Data Input System for Information Technology as directed in DoD CIO annual IT budget guidance.

(8) PMs and FSMs that acquire or use cloud services remain responsible for testing end-to-end security and computer network defense requirements before use to ensure that requirements are met and adequately supported by a cybersecurity service provider in accordance with DoDI 8530.01.

(a) Before operational use, all applications, services, and information systems being delivered using a cloud service will conduct cybersecurity developmental, operational, or integrated T&E in emulated and live environments in accordance with DoDI 5000.89, and will have or be covered by an interim approval to test or ATO granted by the PM's or FSM's authorizing official.

(b) Leveraging the DoD PA for the cloud service, the ATO will cover the use of the cloud service and any DoD-provided software, data, networks, system connections, and processes that comprise the application, service, or information system.

(9) Operations and sustainment for cloud services will include a plan for recurring threat hunting commensurate with the DoD operational mission or capabilities associated with the cloud services.

3.8. SOFTWARE.

a. MDAs and DAs and their functional sponsors will ensure their programs containing digital capabilities as defined in this issuance (including NSS) properly account for and report software maintenance and sustainment as defined and reported pursuant to Sections 2460, 2464, and 2466 of Title 10, U.S.C., and in accordance with DoDIs 4151.20 and 5000.87.

b. PMs will verify that software assurance for software development and testing, software development and test environments, processes, and tools are consistent with DoDI 5200.44.

c. When appropriate, PMs will use development security operations as the preferred approach for software delivery.

3.9. DATA AND INFORMATION.

a. Data.

(1) PMs will publish data assets in the DoD federated data catalog along with common interface specifications. Details can be found in applicable guidance on the DoD Adaptive Acquisition Framework website at https://aaf.dau.edu.

(2) In accordance with the May 5, 2021 DepSecDef Memorandum, the DoD Data Strategy, and DoDI 8320.02, PMs will:

(a) Maximize data sharing and rights for data use as all DoD data is an enterprise resource.

(b) Use automated data interfaces that are externally accessible and machine readable, as appropriate.

(c) Ensure interfaces use industry-standard, non-proprietary protocols and payloads, as appropriate.

(d) Implement industry best practices for secure authentication, access management, encryption, monitoring, and protection of data at rest, in transit, and in use, as appropriate.

(e) Store data in a manner that is platform and environment-agnostic, uncoupled from all infrastructure dependencies, and maximally portable, as appropriate.

b. Interoperability.

(1) Acquisition programs containing digital capabilities, as defined in this issuance, will develop the appropriate system and data-level interoperability requirements and information support plans. They will also plan for interoperability testing and certification in accordance with DoDIs 8320.02, 8330.01, and 8410.03.

(2) PMs in defense intelligence components will require that acquisitions of digital capabilities be able to share data, integrate, and collaborate in accordance with Intelligence Community Directive 501.

c. Information Protection.

(1) PMs of DoD IT systems (including those supported through contracts with external sources) that collect, maintain, use, or disseminate information will comply with DoDI 5200.01, 5000.83, 5000.90, and 8500.01 to ensure information is protected and measures are in place to prevent unauthorized disclosure. Furthermore, PMs will perform cybersecurity testing of systems, actively hunt for cyber intrusions, and conduct system security scans at a frequency commensurate with the information stored and protected, as appropriate.

(2) PMs will ensure DFARS clauses 252.204-7012, 252.204-7020, and 252.204-7021 are included in solicitations to safeguard controlled unclassified information (CUI) on the contractors' information systems in accordance with DoDI 8582.01.

(3) The protection of CUI resident in non-Federal systems and organizations is of paramount importance to Federal agencies and can directly impact the ability of the Federal Government to successfully conduct its assigned missions and business operations. DoD and non-Federal organizations will enact assessment procedures and methodology that can be employed to conduct assessments of the CUI security requirement.

d. Privacy.

PMs will ensure personally identifiable information is managed in a manner that protects privacy and conforms to applicable legal, regulatory, and policy requirements regarding privacy.

(1) Personally identifiable information will be collected, maintained, disseminated, and used in accordance with DoDI 5400.11 and DoD 5400.11-R.

(2) Privacy impact assessments will be completed on DoD IT and electronic collections in accordance with DoDI 5400.16.

e. Information Quality.

(1) The quality of information publicly distributed by PMs will meet basic information quality standards with the attributes of utility, objectivity, and integrity in accordance with DoDI 8170.01. An additional level of quality is warranted in those situations involving influential scientific, financial, or statistical information results.

(2) Scientific and technical information, as defined in DoDI 3200.12, will be managed to make scientific knowledge and technological innovations fully accessible to the research community, industry, the military operational community, and the general public within the boundaries of law, regulation, other directives, and executive requirements.

f. Intelligence Data.

PMs in defense intelligence components will require that IT acquisitions for systems that process or handle U.S. person information enable the collection, retention, and dissemination of U.S. person information in accordance with DoDM 5240.01, and that intelligence data systems maintain data in accordance with DoDI 5200.01.

g. Records Management.

(1) PMs will comply with the records management requirements of:

(a) Chapter 31 of Title 44, U.S.C., also known as the "Federal Records Act of 1950, as amended," including the Presidential and Federal Records Act Amendments of 2014.

(b) Public Law 107-347, also known as the "E-Government Act of 2002."

(c) Section 1236 of Title 36, Code of Federal Regulations.

(d) Office of Management and Budget Circular No. A-130.

(e) DoDI 5015.02.

(2) Electronic information system and IT services will incorporate records management and preservation considerations. Any records contained in systems or IT services will be managed in accordance with National Archives and Records Administration-approved records disposition schedules (available at https://www.archives.gov/about/records-schedule).

(3) DoD Component CIOs will ensure that records management requirements are integrated into the Component IT governance processes for portfolio management, risk management, capital planning, enterprise architecture, business process design, system development, and lifecycle management. PMs will work with DoD Component records officers early and throughout the acquisition process to properly address records management requirements.

3.10. FINANCIAL AUDITING.

a. For financial or non-financial systems or applications impacting internal controls relevant to multiple DoD financial audits, PMs and FSMs will obtain annual system and organization control Type II reports from cloud and data center hosting organizations and application service providers.

b. In those instances, where only a single DoD audit is impacted, an alternate solution is the inclusion of a right to audit clause in the relevant service organization contract.

c. In accordance with the May 20, 2019 DoD CIO and Under Secretary of Defense(Comptroller)/Chief Financial Officer Memorandum, PMs and FSMs will work with their financial and contract personnel to:

(1) Determine if their cloud or data center hosting organization or application service provider is affected.

(2) Ensure service organizations and relevant sub-service organizations submit system and organization control Type II reports.

3.11. SECTION 508, ACCESSIBILITY OF ICT FOR INDIVIDUALS WITH DISABILITIES.

a. PMs and FSMs will ensure that ICT developed, procured, maintained, and used by the DoD allows persons with disabilities access to information that is comparable to that afforded to persons without disabilities in accordance with:

(1) Section 794(d) of Title 29, U.S.C., (also known as "Section 508 of the Rehabilitation Act" and referred to in this issuance as "Section 508").

(2) Specific component or organizational accessibility standards that meet or exceed Section 508 requirements.

b. For exceptions to Section 508 compliance, refer to DoDM 8400.01.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
ACAT	acquisition category
ATO	authorization to operate
BCAT	business category
C-SCRM	cyber supply chain risk management
CAE	Component acquisition executive
CCA	Clinger-Cohen Act
CC SRG	cloud computing security requirements guide
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
CSS	cybersecurity strategy
CUI	controlled unclassified information
DA	decision authority
DAE	Defense Acquisition Executive
DAS	Defense Acquisition System
DepSecDef	Deputy Secretary of Defense
DFARS	Defense Federal Acquisition Regulation Supplement
DIRNSA/CHCSS	Director, National Security Agency/Chief Central Security Service
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DOT&E	Director of Operational Test and Evaluation
ESI	enterprise software initiative
FSM	functional service manager
FY	fiscal year
ICT	information and communications technology
IEA	Information Enterprise Architecture
IT	information technology
MDA	milestone decision authority
NDAA	National Defense Authorization Act
NSS	national security systems
PA	provisional authorization

ACRONYM	MEANING
PIR	post-implementation review
PM	program manager
PNT	positioning, navigation, and timing
RMF	risk management framework
SCRM	supply chain risk management
T&E	test and evaluation
U.S.C.	United States Code
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
ACAT I	Acquisition category programs have three sub-categories: **ACAT 1B** for which the MDA is the Service acquisition executive. **ACAT ID** for which the MDA is the DAE, unless delegated. The "D" refers to the Defense Acquisition Board, which advises the USD(A&S) at major decision points. **ACAT IC** for which the MDA is the DoD Component head or, if delegated, the DoD Component acquisition executive.

TERM	DEFINITION
BCAT	Business system categories have three sub-categories. **BCAT I** is a priority defense business system expected to have a total amount of budget authority over the period of the current Future Years Defense Program in excess of $250,000,000. The MDA is the DAE or as delegated not below the CAE. **BCAT II** does not meet criteria for category I and is expected to have a total amount of budget authority over the period of the current Future Years Defense Program in excess of $50,000,000. The MDA is the CAE or as delegated. **BCAT III** does not meet criteria for category II. The MDA is the CAE or as delegated.
CAE	An individual who is responsible for all acquisition functions within their DoD Component. This includes both the Service acquisition executives for the Military Departments and acquisition executives in other DoD Components, such as the United States Special Operations Command and the Defense Logistics Agency, which also have acquisition management responsibilities.
CCA	Initially, Division D and Division E of Public Law 104-106, also known as "the NDAA for FY 1996". Division D of the NDAA for FY 1996 was the Federal Acquisition Reform Act, and Division E was the IT Management Reform Act. Both divisions of the NDAA for FY 1996 made significant changes to defense acquisition policy. The provisions of this legislation have been incorporated in Titles 40 and 44, U.S.C. For more information, see the Federal Acquisition Reform Act and IT Management Reform Act.
C-SCRM	A systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the cyber supply chain risks presented by the supplier, the supplied products and services, or the supply chain.
data servers	Defined as "data server farms" in the NDAA for FY 2012.

TERM	DEFINITION
digital capabilities	Capabilities acquired through the DoD Adaptive Acquisition Framework that contain a component of IT, including NSS, networking, cybersecurity, electromagnetic spectrum, or positioning, navigation, and timing, pursuant to the relevant Sections of Titles 10, 40, and 44 of U.S.C and National Security Directive 42, but excluding equipment acquired by contractors that is incidental to the performance of a DoD contract, such as telephones, computers, and facsimile machines. It also does not include any acquisition using non-appropriated funds under the guidelines outlined in DoDI 4105.67.
DoD information	Any information that is in DoD custody and control; relates to information in DoD custody and control; was acquired by DoD employees as part of their official duties or because of their official status within DoD, including information that is provided by the DoD to a non-DoD entity; or is developed by a non-DoD entity in support of an official DoD activity.
DoD IEA	The structured description of the DoD's IEA including the infrastructure, communications systems and services (e.g., systems and facilities for transferring data between persons and equipment), the computing systems and services (e.g., integrated sets of components for collecting, storing, and processing data for delivering information, knowledge, and digital products for organizations and individuals to manage their operations), and the controlled processes (e.g., the controllers, actuators, and sensors) that enable remote diagnostic and maintenance for the monitoring and control of critical infrastructure systems and services. The DoD IEA includes information enterprise reference and solution architectures.
enterprise architecture	Defined in Section 3601(4) of Title 44, U.S.C.
enterprise service	An IT service sponsored by a DoD Component that is available for use by other DoD Components.
ICT	Defined in DoDM 8400.01 and in DoDI 5200.44
information resources	Resources related to the compilation of information, such as personnel, equipment, funds, and IT.

TERM	DEFINITION
information resources management	The process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burdens on the public.
information security	Defined in Section 3552 of Title 44, U.S.C.
information system	Defined in Section 3502 of Title 44, U.S.C.
IT	Defined in Section 11101 of Title 40, U.S.C.
IT functional sponsor	The DoD or component leader in IT acquisitions, including NSS, responsible for conducting solution analysis and identifying the capability requirements necessary to meet operational mission functionality.
IT services	The performance of any services work related to IT and the operation of IT, including NSS. This includes outsourced IT-based business processes, outsourced IT, and outsourced information functions. IT service includes cloud services, infrastructure-as-a-service, platform-as-a-service, software-as-a-service, and other "as-a-service" terms.
MDA	A designated individual with overall responsibility for an acquisition program. The MDA will have the authority to approve entry of an acquisition program into the next phase of the acquisition process and will be accountable for cost, schedule, and performance reporting to higher authority, including congressional reporting.
modular open systems approach for IT	Defined in Section 4401 of Title 10, U.S.C. and Section 801 (b through d) of Public Law 113-291.
navigation warfare	Defined in Joint Publication 3-14.
NSS	Defined in Section 3552 of Title 44, U.S.C.
operational resilience	The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.

TERM	DEFINITION
operations security	Defined in National Security Presidential Memorandum 28 and in accordance with DoDI 5205.08.
scientific and technical information	Defined in DoDI 3200.12.
services ACAT I	Acquisitions of services with an estimated total value of $1 billion or more, or with an estimated total value in any 1 year of more than $300 million
solution architecture	A framework that portrays the relationships among all elements of a structure that addresses a problem. Used as a tool to improve joint operational processes and infrastructure and to promote common vocabulary, reuse, and integration.
T&E master plan	A plan that documents the overall structure and objectives of the T&E program. It provides a framework within which to generate detailed T&E plans and documents, schedule, and resource implications associated with the T&E program.

REFERENCES

Code of Federal Regulations, Title 36, Section 1236

Defense Acquisition University, "Adaptive Acquisition Framework," current edition

Defense Federal Acquisition Regulation Supplement, current edition

Defense Information Systems Agency, DoD Cloud Service Catalog[1]

Defense Information Systems Agency, DoD Cloud Computing Security Requirements Guide, Version 1, Release 3, March 6, 2017[2]

Deputy Secretary of Defense, "DoD Data Strategy 2020," September 30, 2020

Deputy Secretary of Defense, "DoD Digital Modernization Strategy - DoD Information Resource Management Strategic Plan Fiscal Years 2019-2023," July 12, 2019

Deputy Secretary of Defense Memorandum, "Creating Data Advantage," May 5, 2021

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

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD Chief Information Officer, "Charter for the Digital Modernization Infrastructure Executive Committee," July 13, 2020[3]

DoD Chief Information Officer, "Terms of Reference, Enterprise Architecture and Engineering Panel," May 1, 2015[4]

DoD Chief Information Officer and Under Secretary of Defense (Comptroller)/Chief Financial Officer Memorandum, "System and Organization Control Report Requirement for Audit Impacting Cloud/Data Center Hosting Organizations and Application Service Providers," May 20, 2019

DoD Directive 4650.05, "Positioning, Navigation, and Timing," June 9, 2016, as amended

DoD Directive 5000.01, "The Defense Acquisition System," September 9, 2020

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

DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, as amended

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

DoD Instruction 4105.67, "Nonappropriated Fund (NAF) Procurement Policy and Procedure," February 26, 2014, as amended

DoD Instruction 4140.01, "DoD Supply Chain Material Management Policy," March 6, 2019

DoD Instruction 4151.20, "Depot Maintenance Core Capabilities Determination Process," May 4, 2018, as amended

[1] Available at https://dod365.sharepoint-mil.us/sites/DISA-RE-Apps/cas/SitePages/CASHome.aspx
[2] Available at https://cyber.mil/dccs/ (CAC access required)
[3] Available at https://intelshare.intelink.gov/sites/dodjie/default.aspx (CAC access required)
[4] Available at https://intelshare.intelink.gov/sites/eaep/SitePages/Home.aspx (CAC access required)

DoD Instruction 4630.09, "Communications Waveform Management and Standardization," November 23, 2020

DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009, as amended

DoD Instruction 4650.08, "Positioning, Navigation, and Timing and Navigation Warfare," December 27, 2018, as amended

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 5000.87, "Operation of the Software Acquisition Pathway," October 2, 2020

DoD Instruction 5000.88, "Engineering of Defense Systems," November 18, 2020

DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020

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 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended

DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012, as amended

DoD Instruction 5205.08, "Access to U.S. Classified Cryptographic Information," February 16, 2018, as amended

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended

DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019, as amended

DoD Instruction 8310.01, "Information Technology Standards in the DoD," April 7, 2023

DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013, as amended

DoD Instruction 8330.01, "Interoperability of Information Technology, Including National Security Systems," September 27, 2022

DoD Instruction 8410.03, "Network Management (NM)," August 29, 2012, as amended

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 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System," July 9, 2004

DoD Instruction 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," December 9, 2019

DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

DoD Manual 8400.01, "Accessibility of Information and Communications Technology (ICT)," November 14, 2017

House of Representatives Report 104-222, "Federal Acquisitions Reform Act, "August 1, 1995

Intelligence Community Directive 501, "Intelligence Community Directive Discovery and Dissemination or Retrieval of Information within the Intelligence Community," January 21, 2009

Joint Publication 3-14, "Space Operations," April 10, 2018, as amended

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

National Security Presidential Memorandum 28, "National Operations Security Program," January 13, 2021

Office of Management and Budget Circular A-130, "Managing Information as a Strategic Resource," July 28, 2016

Office of the Secretary of Defense, "National Defense Strategy," 2020

Public Law 104-106, "National Defense Authorization Act for Fiscal Year 1996," February 10, 1996

Public Law 106-398, "Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001," October 30, 2000

Public Law 107-347, "E-Government Act of 2002," December 17, 2002

Public Law 112-81, Section 2867, "National Defense Authorization Act for Fiscal Year 2012," December 31, 2011

Public Law 113-291, Section 801(b through d), "Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015," December 19, 2014

Public Law 115-232, Section 1064(d), "John S. McCain National Defense Authorization Act for Fiscal Year 2019," August 13, 2018

Public Law 116-92, Section 168, "National Defense Authorization Act for Fiscal Year 2020," December 20, 2019

Senate 946, "Information Technology Management Reform Act," July 25, 1995

United States Code, Title 10

United States Code, Title 29, Section 794(d) (also known as "Section 508 of the Rehabilitation Act")

United States Code, Title 40

United States Code, Title 44