DoD Instruction 5000.82

Acquisition of Information Technology (IT)

Originating Component: Office of the DoD Chief Information Officer

Effective: April 21, 2020

Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

Incorporates and Cancels: Enclosure 11, "Requirements Applicable to All Programs Containing Information Technology (IT)," to DoD Instruction 5000.02T, "Operation of the Defense Acquisition System," January 7, 2015, as amended

Approved by: Dana Deasy, Department of Defense Chief Information Officer

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

- Establishes functional acquisition policy and procedures for all programs containing IT (including National Security Systems (NSS)), pursuant to the relevant sections of Titles 10, 40, and 44, United States Code (U.S.C.), but excluding equipment acquired by contractors that is incidental to the performance of a DoD contract, such as telephones, computers, and fax machines.

- Assigns program responsibilities in accordance with the authority in DoDDs 5144.02 and 8000.01.

- Restructures acquisition processes and procedures of all programs containing IT to a separate, functional acquisition policy that adheres to the Adaptive Acquisition Framework described in DoD Instruction (DoDI) 5000.02.

TABLE OF CONTENTS

FIGURES

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 the 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 instruction as the "DoD Components").

1.2. POLICY.

a. The acquisition of IT supports the National Defense Strategy and the DoD Digital Modernization Strategy by synchronizing DoD IT acquisitions to ensure the standards, architecture, and cybersecurity implementation necessary to provide interoperable and secure IT systems across the joint force, increasing warfighter lethality.

b. This instruction:

(1) Guides the DoD approach to IT acquisitions and procedures relating to acquisition programs and systems containing IT, regardless of dollar value and including NSS.

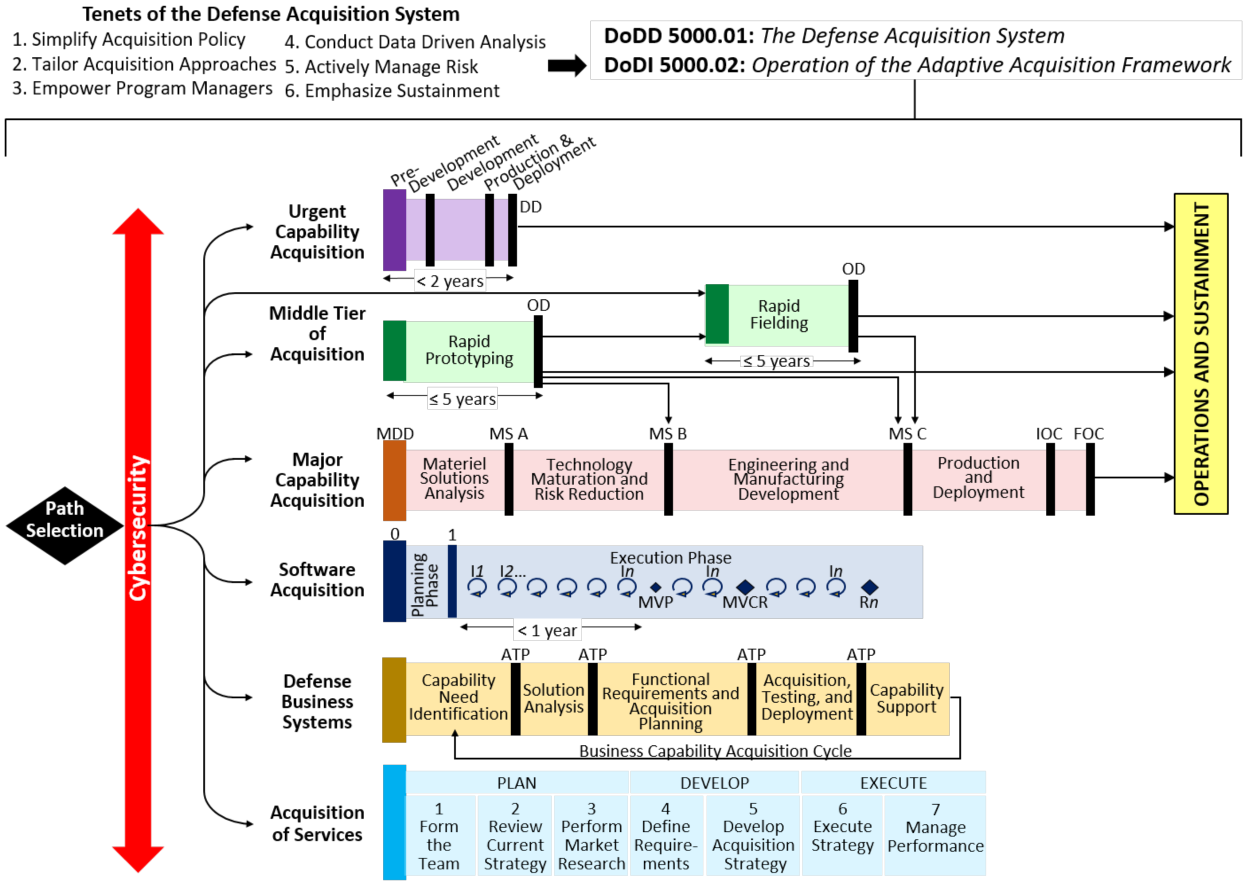
(2) Together with amplifying guidance found in the Milestone Document Identification (MDID) (available at https://www.dau.edu/mdid/Pages/Default.aspx), provides the documentary requirements to execute each acquisition pathway.

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 through the development of 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 that objective, the DoD will employ an adaptive acquisition framework comprised of acquisition pathways (see Figure 1), each tailored for the unique characteristics of the capability being acquired. This instruction describes the responsibilities of principal acquisition officials and the functional characteristics of the acquisition of IT as it applies to the acquisition pathways.

Figure 1. Adaptive Acquisition Framework

This instruction describes the functional responsibilities and procedures of principal acquisition officials in the acquisition of programs containing IT, including NSS, across all acquisition pathways.



Tenets of the Defense Acquisition System
1. Simplify Acquisition Policy
2. Tailor Acquisition Approaches
3. Empower Program Managers
4. Conduct Data Driven Analysis
5. Actively Manage Risk
6. Emphasize Sustainment
DoDD 5000.01: The Defense Acquisition System
DoDI 5000.02: Operation of the Adaptive Acquisition Framework
Path Selection
Cybersecurity
Urgent Capability Acquisition
Pre-Development
Development
Production & Deployment
DD
< 2 years
Middle Tier of Acquisition
Rapid Prototyping
OD
≤ 5 years
Rapid Fielding
OD
≤ 5 years
Major Capability Acquisition
MDD
MS A
MS B
MS C
IOC
FOC
Materiel Solutions Analysis
Technology Maturation and Risk Reduction
Engineering and Manufacturing Development
Production and Deployment
Software Acquisition
0
1
Planning Phase
Execution Phase
I1
I2...
In
MVP
In
MVCR
In
Rn
< 1 year
Defense Business Systems
ATP
ATP
ATP
ATP
Capability Need Identification
Solution Analysis
Functional Requirements and Acquisition Planning
Acquisition, Testing, and Deployment
Capability Support
Business Capability Acquisition Cycle
Acquisition of Services
PLAN
DEVELOP
EXECUTE
1 Form the Team
2 Review Current Strategy
3 Perform Market Research
4 Define Require-ments
5 Develop Acquisition Strategy
6 Execute Strategy
7 Manage Performance
OPERATIONS AND SUSTAINMENT

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 procedures relating to the acquisition of all programs and systems containing IT, across all of the acquisition pathways defined in DoDI 5000.02, and for all components and agencies of the DoD.

b. Ensures DoD IT standards are established and maintained, in accordance with DoDI 8310.01.

c. Identifies gaps in IT standards for acquisition programs and systems containing IT, including NSS, and ensures mitigation plans are identified for gaps in the absence of acceptable standards.

d. For suppliers or products requiring action pursuant to Section 806 of Public Law 111-383, also known as the "Ike Skelton National Defense Authorization Act for Fiscal Year 2011," and in coordination with the Under Secretary of Defense for Intelligence and Security (USD(I&S)) and the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), prepares and executes an action package that contains the 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 significant supply chain risk, the scope of applicability, and the required or recommended mitigations.

2.2. USD(I&S).

The USD(I&S):

a. Advises the DoD CIO on security, intelligence, and counterintelligence requirements, in support of the acquisition of IT, including NSS.

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

(1) IT acquisition in programs where the Component acquisition executive is the milestone decision authority (MDA).

(2) Security, counterintelligence, and intelligence matters related to waiver or extension requests that address identified gaps in IT standards and mitigation plans in the absence of acceptable standards.

c. Defines roles established to support intelligence responsibilities related to the standards and mitigations addressed in Paragraphs 2.1.d. and 3.7 of this instruction concerning supply chain risk management in support of DoD trusted systems and networks (TSNs).

2.3. USD(A&S).

The USD(A&S) defines roles established to support acquisition responsibilities related to the standards and mitigations addressed in Paragraphs 2.1.d and 3.7 of this instruction concerning supply chain risk management in support of DoD TSNs.

2.4. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING.

The Under Secretary of Defense for Research and Engineering:

a. Ensures IT acquisition programs, where the USD(A&S), in his or her capacity as the Defense Acquisition Executive (DAE), is the MDA, follow the policy and procedures outlined in this instruction and Enclosures 4 and 5 of DoDI 5000.02T.

b. Provides guidance and oversight regarding the development, engineering, and test and evaluation (T&E) plans for IT acquisition programs where the DAE is the MDA.

2.5. DOD COMPONENT HEADS.

The DoD Component heads:

a. Ensure that IT in programs delegated to, or under the authority of, the Component, follow the policies and procedures outlined in this instruction.

b. Ensure their Component CIOs identify gaps in IT standards and mitigation plans in the absence of acceptable standards and, when necessary, submit waivers or extension requests to the DoD CIO. Statutory requirements may not be waived, unless authorized in statute.

SECTION 3: PROCEDURES

3.1. GENERAL.

a. The Milestone and Phase Information Requirements (MPIR) tables found at the MDID contain IT-related statutory and regulatory requirements at each of the milestones and other decision points for the acquisition pathways. MDAs, decision authorities (DAs), IT functional sponsors, and program managers (PMs) will follow the applicable IT-related information requirements contained therein to ensure statutory and regulatory compliance.

b. MDAs/DAs and functional sponsors, and PMs will ensure that their programs containing IT follow the additional guidance provided in this instruction, as it pertains to:

(1) IT, as defined in Section 11101 of Title 40, U.S.C.

(2) IT enterprise architecture, as defined in Section 3601(4) of Title 44, U.S.C.

(3) NSS, as defined in Section 3552 of Title 44, U.S.C.

(4) Information systems, as defined in Section 3502 of Title 44, U.S.C.

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

(6) IT services, as defined in DoDI 5000.74 and this instruction.

(7) Modular Open Systems Approach for IT, as defined in Section 2322a of Title 10, U.S.C. and Section 801(b-d) of Public Law 113-291.

c. MDAs and DAs ensure:

(1) IT acquisition requirements are included at applicable decision points and milestones of assigned programs. These requirements must include interoperability plans and testing in accordance with DoDIs 8330.01, 8320.02, and 8410.03.

(2) With functional sponsors, their programs containing IT, 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 DoDI 4151.20.

(3) Acquisition of systems containing IT, including NSS, plan and execute an efficient and effective T&E program, to include cybersecurity procedures, in accordance with Enclosures 4 and 5 of DoDI 5000.02T. Supplemental guidance on cybersecurity and cloud T&E plans is contained in the Cybersecurity T&E Guidebook 2.0.

3.2. CLINGER-COHEN ACT (CCA) COMPLIANCE.

a. Subtitle III of Title 40, U.S.C., also known and referred to in this issuance as Division E of the CCA, applies to all IT investments, including NSS.

b. For all programs that acquire IT, including NSS, at any acquisition category (ACAT) level or business system category level, the MDA will not initiate a program nor an increment of a program, approve entry into any phase of the acquisition process that requires formal acquisition milestone approval, or authorize execution of a contract for the applicable acquisition phase until:

(1) The sponsoring DoD Component or PM has satisfied the applicable acquisition phase-specific requirements of the CCA as shown in the CCA compliance table found in the MPIR tables of the MDID.

(2) The PM has reported CCA compliance to the MDA and the DoD Component CIO or their designee for approval.

c. The CCA Compliance table located in the MPIR/MDID identifies the specific requirements for CCA compliance. These requirements will be satisfied to the maximum extent practicable through documentation developed during the Adaptive Acquisition Framework pathways. To report compliance, the PM will prepare a table similar to the MPIR/MDID to indicate which documents demonstrate compliance with the CCA's requirements. The PM's table will provide links to the cited documents and serve as the PM's CCA compliance report.

3.3. POST-IMPLEMENTATION REVIEW (PIR).

The IT functional sponsor, in coordination with the DoD Component CIO and PM, is responsible for developing a plan and conducting a PIR for all fully-deployed IT, including NSS.

a. PIRs will:

(1) 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.

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

(3) Document lessons learned from the PIR.

b. For major weapons systems, the PIR requirements should be included in the follow-on operational T&E plans included in the T&E Master Plan. This means:

(1) PIR requirements must be met before proceeding with full-rate production or full-deployment decision, as appropriate.

(2) The post-fielding assessment(s), the disposition assessment, and the disposition decision for urgent operational needs, as described in DoDI 5000.81, satisfies the requirement for a PIR.

c. For software acquisitions, the software acquisition value assessment acquisition satisfies the PIR requirement.

3.4. DOD INFORMATION ENTERPRISE ARCHITECTURE (IEA).

The DoD IEA is considered the "ITEA" and provides the DoD's "to-be" architecture to realize the overarching goals of the Digital Modernization Strategy through four priority technological areas: cloud; artificial intelligence; cybersecurity; and command, control, and communications (C3).

a. PMs must develop solution architectures that support the DoD IEA (Increment 1 of Version 3.0 of the DoD IEA), applicable references, mission area and component architectures, and DoD Component architecture guidance. A program's solution architecture should define capability and interoperability requirements, establish and enforce standards, and guide security and cybersecurity requirements, in accordance with DoDIs 8500.01 and 8530.01.

b. The standards used to form the standard viewpoints of integrated architectures will be selected from those contained in the current approved version of the DoD IT Standards Registry within the Global Information Grid Technical Guidance Federation service. The standards selected must be sufficient to enable the interoperability and cybersecurity required for joint operations, in accordance with the National Security Strategy. The IT will be tested to measures of performance derived from the solution architecture.

c. All milestone and decision point approvals will be designed and developed, to the maximum extent practicable, with a modular open system approach to enable incremental development and enhance competition, innovation, and interoperability, in accordance with Section 2446a of Title 10, U.S.C.

3.5. C3.

C3 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.

a. Waveform Management.

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

b. Spectrum Supportability.

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

c. Positioning, Navigation, and Timing (PNT).

In accordance with the National Defense Strategy and DoDD 4650.05, DoD Components 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, in accordance with DoDI 4650.08, at each acquisition milestone for all platforms and systems producing or using PNT information.

3.6. CYBERSECURITY.

Cyber threats present a risk to all DoD IT. All acquisition of IT must incorporate cybersecurity requirements, in accordance with DoDI 8500.01, to include operational resilience, risk management, and cyberspace defense.

a. Cybersecurity Risk Management Framework (RMF).

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 effort to achieve authorization to operate and subsequent security controls management requirements throughout the system life cycle.

b. Cybersecurity Strategy (CSS).

All acquisitions of systems containing IT, including NSS, will have a CSS, in accordance with DoDI 8580.1. The CSS is a statutory requirement, pursuant to Section 811 of Public Law 106-398, also known as the “Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001,” for mission essential and mission critical IT systems and a regulatory requirement for all IT systems under this instruction and DoDI 8580.1. For mission essential and mission critical IT systems, this CSS may be an appendix to the program protection plan (PPP) for applicable Adaptive Acquisition Framework pathways as identified in Enclosures 3 and 13 of DoDI 5000.02T.

(1) For ACAT ID programs, the DoD CIO will review and approve the CSS before the MDA makes milestone decisions or contract awards.

(2) For non-ACAT ID programs and systems, the PM will submit the CSS to the cognizant DoD Component CIO for review before the MDA makes milestone decisions or contract awards.

(3) CIOs will document the results of all reviews of the program's compliance with the CSS, in accordance with DoDI 8580.1.

(4) If contract award is authorized as part of an acquisition milestone decision, a separate review of the CSS before contract award is not required.

(5) The approved cybersecurity strategy will be an appendix to the PPP, if specified by Enclosures 3 and 13 of DoDI 5000.02T; otherwise it will be a stand-alone required document.

3.7. TSN.

NSS and other information systems that have a high impact level for any of the three security objectives (confidentiality, integrity, or availability) must identify and protect mission critical functions and components as required by DoDI 5200.44. TSN planning and implementation activities are documented in PPPs, in accordance with Enclosures 3 and 13 of DoDI 5000.02T and relevant cybersecurity plans and documentation. PMs will manage TSN risk by:

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

b. Requesting threat analysis of suppliers of critical components (supplier all source threat analysis).

c. Requesting security validation of supplier development environment, in accordance with DoDI 8582.01.

d. Requesting suppliers' verification of compliance and reporting requirements of Part 252.204 of the Defense Federal Acquisition Regulation.

e. Verifying cybersecurity resiliency of the TSN through rigorous testing of network components and operations.

f. Engaging the TSN focal point identified by the DoD Component, in accordance with DoDI 5200.44, for guidance on managing identified risk, including supply chain risk management controls.

g. Applying TSN best practices, processes, techniques, and procurement tools before the acquisition of critical components or their integration into applicable systems.

3.8. CLOUD COMPUTING.

DoD Components will take full advantage of cloud computing in alignment with and to achieve the goals of the DoD Digital Modernization Strategy, the requirements of Section 1064(d) of Public Law 115-232, and the security guidance of the current DoD Cloud Computing Security Requirements Guide. Specifically:

a. 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.

b. DoD Components will ensure their respective Program Executive Offices take steps necessary to accelerate adoption of cloud-based digital infrastructure that enables rapid deployment, scaling, testing, and optimization of software as an enduring capability.

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

a. When acquiring commercial IT, PMs and acquisition personnel must consider, taking into account government contracting laws and regulations, the suitability of using DoD IT Category Management purchasing solutions, the DoD ESI, Federal Category Management procurement vehicles, and DoD Component level enterprise software licenses, PMs and acquisition personnel will document these considerations in the acquisition strategy, to include selection rationale. These purchasing vehicles are not intended to dictate the products or services to be acquired.

b. For procurement of commercial software that is within the scope of a core enterprise technology agreement, adherence to DoDD 8470.01E is required. Additional detail is provided in:

(1) Subpart 208.74 of the Defense Federal Acquisition Regulation Supplement.

(2) Office of Management and Budget Policy Memorandums M-19-13, M-16-02, M-16-12, and M-16-20.

(3) The DoD ESI website.

c. The DoD ESI does not dictate the products or services to be acquired.

3.10. DOD DATA CENTER CONSOLIDATION.

The June 9, 2014 DoD CIO Memorandum delegated revocable authority to approve spending on data centers (DCs) to Component CIOs while remaining compliant with Section 2867 of Public Law 112-81, also known as and referred to in this issuance as the “National Defense Authorization Act for Fiscal Year 2012.” This delegated authority does not apply to obligation of development and modernization resources within 12 months of closure as reported with the DoD authoritative DC inventory, DCs without a record in the DoD DC inventory, the establishment of a new DC, or expansion of an existing DC beyond 18 percent of its current floor space.

a. Any PM who intends to obligate funds for data servers, DCs, or the IT used therein, must obtain prior approval from the cognizant DoD Component CIO and submit quarterly DC obligation reports to the DoD CIO's DC Consolidation office.

(1) Quarterly DC obligation reports must be submitted within 45 calendar days following the end of each fiscal year (FY) quarter and signed by the DoD Component CIO.

(2) To maintain the revocable authority, DoD organizations must:

(a) Maintain complete and accurate records within the DoD DC inventory database.

(b) Maintain accurate budget data within the Select & Native Program Data Input System-IT system website.

(c) Submit quarterly DC obligation reports to the DoD CIO.

b. DoD organizations participating in the DoD’s IT purchase request process do not need to comply with the approval and reporting requirements outlined in Paragraph 3.10.a. because the IT purchase request process meets the intent of those requirements.

3.11. INFORMATION PROTECTION.

PMs of DoD IT systems (including those supported through contracts with external sources) that collect, maintain, use, or disseminate information must comply with DoDI 5200.01, Enclosures 3 and 13 of DoDI 5000.02T, and other DoD Information Security guidance to ensure information is protected and measures are in place to prevent unauthorized disclosure.

a. Privacy.

The 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. Personally identifiable information will be collected, maintained, disseminated, and used in accordance with DoDI 5400.11 and DoD 5400.11-R. Privacy impact assessments will be completed on DoD IT and electronic collections, in accordance with DoDI 5400.16.

b. Information Quality.

The quality of information publicly distributed by PMs must 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. Scientific and technical information, as defined in DoDI 3200.12, must 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.

c. Intelligence Data.

PMs in Defense Intelligence Components ensure 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 ensure that intelligence data systems maintain data, in accordance with DoDI 5200.01 and Intelligence Community Directive 503.

3.12. RECORDS MANAGEMENT.

For information created, collected, and retained in the form of electronic records, PMs must comply with the records management requirements of 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; Public Law 107-347, also known as the "E-Government Act of 2002;" Section 1236 of Title 36, Electronic Code of Federal Regulations; Office of Management and Budget Circular No. A-130; and DoDI 5015.02.

a. Electronic information system and IT services must incorporate records management and preservation considerations. Any records contained in the systems or IT services must be managed in accordance with National Archives and Records Administration-approved records disposition schedules.

b. The Component CIO will ensure the records management requirements are integrated into the DoD Component IT governance processes for portfolio management, risk management, capital planning, enterprise architecture, business process design, and system development. PMs must work with Component records officers early and throughout the acquisition process to properly address records management requirements.

3.13. SECTION 508 – ACCESSIBILITY OF ICT FOR INDIVIDUALS WITH DISABILITIES.

PMs will ensure that ICT developed, procured, maintained, and used by the DoD will allow persons with disabilities access to information that is comparable to that afforded persons without disabilities, in accordance with Section 794(d) of Title 29, U.S.C., also known and referred to in this issuance as "Section 508 of the Rehabilitation Act" (Section 508), or in accordance with specific component/organizational accessibility standards that meet or exceed Section 508 requirements. For exceptions to Section 508 compliance, refer to DoDM 8400.01.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
ACAT	acquisition category
C3	command, control, and communications
CCA	Clinger-Cohen Act
CIO	Chief Information Officer
DA	decision authority
DAE	Defense Acquisition Executive
DAS	Defense Acquisition System
DC	data center
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
ESI	Enterprise Software Initiative
FY	fiscal year
ICT	information and communications technology
IEA	information enterprise architecture
IT	information technology
MDA	Milestone Decision Authority
MDID	Milestone Document Identification
MPIR	Milestone and Phase Information Requirements
NSS	National Security Systems
PIR	post-implementation review
PM	program manager
PNT	positioning, navigation, and timing
PPP	program protection plan
RMF	Risk Management Framework
T&E	test and evaluation
TSN	trusted system and network
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

G.2. DEFINITIONS.

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

TERM **DEFINITION**

ACAT I

Programs that are Major Defense Acquisition Programs. A Major Defense Acquisition Program is a program that is not a highly sensitive classified program and that is designated by the USD(A&S) as a Major Defense Acquisition Program; or that is estimated to require eventual expenditure for research, development, test, and evaluation, including all planned increments, of more than $525 million (FY 2020 constant dollars) or procurement, including all planned increments, of more than $3.065 billion (FY 2020 constant dollars). ACAT I programs have three sub-categories:

- **ACAT 1B** for which the MDA is the SAE.
- **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.

acquisition of IT

Additional acquisition guidance to some or all of the Adaptive Acquisition Framework pathways for programs, systems, or subsystems containing or dependent on IT.

CCA

Initially, Division D and Division E of the 1996 National Defense Authorization Act. Division D of the Authorization Act was the Federal Acquisition Reform Act and Division E was the IT Management Reform Act. Both divisions of the Act made significant changes to defense acquisition policy. The provisions of this Act B-33 have been incorporated in Titles 40 and 44, U.S.C. See Federal Acquisition Reform Act and IT Management Reform Act.

Component acquisition executive

An individual who is responsible for all acquisition functions within his or her DoD Component. This includes both the SAEs for the Military Departments and acquisition executives in other DoD Components, such as the U.S. Special Operations Command and the Defense Logistics Agency, which also have acquisition management responsibilities.

data servers

Defined as "data server farms" in the National Defense Authorization Act for FY 2012.

TERM **DEFINITION**

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

information system A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

IT Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; this includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, and services (including support services, and related resources). IT is equipment used by the DoD directly or is used by a contractor under a contract with the DoD that requires the use of that equipment. IT does not include any equipment acquired by a federal contractor incidental to a federal contract.

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 Services that include outsourced IT-based business processes, outsourced IT, and outsourced information functions (sometimes referred to as Cloud services, Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service, and other “as-a-Service” terms).

MDA Designated individual with overall responsibility for a 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.

TERM	DEFINITION
MDID	A tool found on the Defense Acquisition University portal that helps acquisition personnel filter through statutory and regulatory document requirements. This tool contains many of the IT-related information requirements mandated for acquisition compliance (e.g., CCA).
navigation warfare	Defined in Joint Publication 3-14.
NSS	Telecommunications or information systems operated by or on behalf of the Federal Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions. NSS do not include systems that are used for routine administrative and business applications (including payroll, finance, and personnel management applications).
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.
urgent operational need	Defined in DoDI 5000.81.

REFERENCES

Defense Federal Acquisition Regulation Supplement, current edition

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

DoD Cybersecurity Test and Evaluation Guidebook 2.0, April 25, 2018[1]

DoD Chief Information Officer Memorandum, "Approvals/Waivers for Obligations of Funds for Data Servers and Centers," June 9, 2014

DoD Cloud Computing Security Requirements Guide, Version 1, Release 3, March 6, 2017

DoD Digital Modernization Strategy, "DoD Information Resource Management Strategic Plan FY 19-23," July 12, 2019

DoD Directive 4650.05, "Positioning, Navigation, and Timing (PNT) Management," June 16, 2016

DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003, as amended

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

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended

DoD Directive 8470.01E, "DoD Executive Agent (DoD EA) for Commercial Software Product Management of Core Enterprise Technology Agreements (CETAs)," September 6, 2018.

DoD Enterprise Software Initiative Website, "DoD ESI," http://www.esi.mil

DoD Information Enterprise Architecture (IEA) Version 3.0, Increment 1, October 10, 2019

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

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

DoD Instruction 4630.09, "Communication Waveform Management and Standardization", July 15, 2015, as amended

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 (PNT) and Navigation Warfare (NAVWAR)," December 27, 2018

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

DoD Instruction 5000.02T, "Operation of the Defense Acquisition System," January 7, 2015, as amended

DoD Instruction 5000.74, "Defense Acquisition of Services," January 10, 2020, as amended

DoD Instruction 5000.81, "Urgent Capability Acquisition," December 31, 2019

[1] https://www.dau.edu/cop/test/Pages/Documents.aspx

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 & Networks (TSN),” November 5, 2012, as amended.

DoD Instruction 5400.11, “DoD Privacy and Civil Liberties Programs,” January 29, 2019

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

DoD Instruction 8310.01, “Information Technology Standards in the DoD,” February 2, 2015, as amended

DoD Instruction 8330.01, “Interoperability of Information Technology (IT), Including National Security Systems (NSS),” May 21, 2014, as amended

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

DoD Instruction 8410.03, “Network Management,” August 29, 2012, as amended

DoD Instruction 8500.01, “Cybersecurity,” March 14, 2014, as amended

DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” March 12, 2014, as amended.

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, 2001

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

Electronic Code of Federal Regulations (e-CFR) Part. 1236, “Electronic Records Management,” current edition

Global Information Grid (GIG) Technical Guidance Federation (GTGF)[2]

Intelligence Community Directive 503, “Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation” September 15, 2008

Milestone Document Identification (MDID)[3]

[2] Available behind CAC wall via https://gtg.csd.disa.mil/.

[3] Accessible via https://www.dau.edu/mdid/Pages/Default.aspx

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

Office of Management and Budget Memorandum M-16-02, "Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops," October 16, 2015

Office of Management and Budget Memorandum M-16-12, "Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing", June 2, 2016

Office of Management and Budget Memorandum M-16-20, "Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services," August 4, 2016

Office of Management and Budget Memorandum M-19-13, "Category Management: Making Smarter User of Common Contract Solutions and Practices," March 20, 2019

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 111-383, "Ike Skelton National Defense Authorization Act for Fiscal Year 2011," January 7, 2011

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

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

Select & Native Program Data Input System-Information Technology (SNAP-IT) website, DoD Information Technology Investment Portal," https://snap.cape.osd.mil/ITPortal/PortalHome.aspx.[4]

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

[4] Accessible behind a CAC wall.