DoDI 5000.82, Acquisition of Information Technology (IT) Policy and Procedures

Presented By:

Bob Skertic
Learning Director, Information Technology
Defense Acquisition University
bob.skertic@dau.edu

William Guthrie
IT Acquisition Lead
DoD CIO
William.l.Guthrie.civ@mail.mil

www.DAU.edu
DoD’s Strategy

- Deliver performance at the speed of relevance.
- Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting.
- Current processes are not responsive to need; the Department is over-optimized for exceptional performance at the expense of providing timely decisions, policies, and capabilities to the warfighter.
- Our response will be to prioritize speed of delivery, continuous adaptation, and frequent modular upgrades.
- We must not accept cumbersome approval chains, wasteful applications of resources in uncompetitive space, or overly risk-averse thinking that impedes change.

**IT Acquisition Policy Goals:**

- Establishes functional acquisition policy and procedures for all programs containing IT
- Restructures acquisition processes and procedures of all programs containing IT to a separate, functional acquisition policy
- Adheres to the Adaptive Acquisition Framework in DoDI 5000.02
- Synchronizes DoD IT acquisitions on standards, architecture, and cybersecurity
- Provide interoperability and secure IT systems across the joint force, increasing warfighter lethality

**Expected Outcomes:**

- Streamline and standardize activities to ensure interoperable and secure systems (Replaces Enclosure 11, DoDI 5000.02T)
- Deploy meaningful capability early and often
- Establish meaningful measures of progress that provide adequate insight into effort
Introduction to the New Acquisition of IT Policy

Purpose:

• Establishes functional acquisition policy and procedures for all programs containing IT (including National Security Systems (NSS))

• 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.

Applicability:

• OSD, Military Departments, Chairman Joint Chief of Staff, Joint Staff, COCOMs, DoD IG, all DoD Agencies, Activities and Components
Introduction to the New Acquisition of IT Policy

Procedures:

- IT-related statutory and regulatory requirements for the acquisition pathways are described within the Milestone and Phase Information (MPIR) tables.

- The DAU tool, Milestone Document IDentification (MDID), helps acquisition professionals quickly find the MPIR tables and ensure statutory and regulatory compliance at each milestone or other decision point.

- Milestone Decision Authorities/Decision Authorities (MDA/DA), functional sponsors and PMs will ensure that their program’s containing IT follow the guidance in this instruction.
DoDI 5000.02 Operation of the Adaptive Acquisition Framework

- Introducing the new acquisition pathway policy

**Tenets of the Defense Acquisition System**
1. Simplify Acquisition Policy
2. Tailor Acquisition Approaches
3. Empower Program Managers
4. Data Driven Analysis
5. Active Risk Management
6. Emphasize Sustainment

**DoDD 5000.01: The Defense Acquisition System**
**DoDI 5000.02: Operation of the Adaptive Acquisition Framework**

Enable execution at the speed of relevance
5000.02T was published in conjunction with 5000.02 to cover functional policies that have not been released yet. 02T will have enclosures cancelled as functional policies are released.

Currently in coordination

5000.02T was published in conjunction with 5000.02 to cover functional policies that have not been released yet. 02T will have enclosures cancelled as functional policies are released.
Introduction to the New Acquisition of IT Policy

**Information Technology**, as defined in Section 11101, Title 40, U.S.C.

**Information Technology.**—The term “information technology”—(A) with respect to an executive agency means 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 by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—(i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(B) 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, services (including support services), and related resources; but

(C) does not include any equipment acquired by a federal contractor incidental to a federal contract.

**Information Technology Enterprise Architecture**, as defined in Section 3601(4), Title 44, U.S.C.

(4) “enterprise architecture”—(A) means—(i) a strategic information asset base, which defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform the mission; and (iv) the transitional processes for implementing new technologies in response to changing mission needs; and

(B) includes—(i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan;
Introduction to the New Acquisition of IT Policy

**National Security Systems (NSS), as defined in Section 3552, Title 44, U.S.C.**

(6) (A) The term “national security system” means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which—(I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

**Information Systems, as defined in Section 3502, Title 44 U.S.C (4) (8)**

the term “information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information;

**IT Services, as defined in DoDI 5000.74 and 5000.82 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).
Introduction to the New Acquisition of IT Policy

**INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT), as defined in DoD Manual (DoDM) 8400.01**

**ICT.** Previously referred to as “electronic and information technology,” any equipment or interconnected system or subsystem of **equipment that is used in the creation, conversion, or duplication of data or information.** ICT also includes any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, reception, or broadcast of data or information. The term includes, but is not limited to: electronic content, including e-mail, electronic documents and Internet and Intranet websites; telecommunications products, including video communication terminals; computers and ancillary equipment, including external hard drives; software, including operating systems and applications; information kiosks and transaction machines; videos; IT services; and multifunction office machines that copy, scan, and fax documents.

**MODULAR OPEN SYSTEMS APPROACH (MOSA) FOR IT, as defined in Section 2446A of Title 10 U.S.C. and Section 801(b-d) Public Law 113-291**

**Open systems approach.**--The term ```open systems approach``` means, with respect to an **information technology system, an integrated business and technical strategy** that-- (A) **employs a modular design** and uses **widely supported and consensus-based standards** for key interfaces; (B) is subjected to successful validation and verification tests to ensure key interfaces comply with widely supported and consensus-based standards; and (C) uses a **system architecture that allows components to be added, modified, replaced, removed, or supported by different vendors** throughout the lifecycle of the system to afford opportunities for enhanced competition and innovation while yielding-- (i) significant cost and schedule savings; and (ii) **increased interoperability.**
MDAs/DAs must ensure that:

- IT acquisition requirements are included at applicable decision points and milestones of all IT programs. **IT acquisition requirements must include interoperability plans and testing.** Interoperability means data, information and networked interoperability.

- They work with IT Functional Sponsors to ensure all programs containing IT (including NSS), **properly account for and report software maintenance and sustainment.**

- For all programs containing IT (including NSS) **plan and execute an effective T&E program to include cybersecurity testing** (Reference Cybersecurity T&E Guidebook v2.0)

- For all programs regardless of ACAT level or business system category, that each program is Title 40, **Clinger-Cohen Act (CCA) compliant.** CCA compliance must be reported prior to any acquisition decision (acquire, milestone advancement, authorization execution of a contract) and compliance must be shown based on the phase-specific CCA requirements as shown in the Milestone Phase Information Requirements (MIPR)/Milestone Document IDentification tool (MDID).

IT Functional Sponsor must ensure that:

- A Post-Implementation Plan (PIR) plan is developed and conducted for all fully-deployed IT, including NSS.

- PIR will provide a DOTMLPF-P analysis; evaluate systems for effectiveness and efficiency, recommend future state of program; document lessons learned; for major weapons systems, must include OT&E plans in the TEMP and ensure PIR requirements are met prior to full-rate production/full deployment; includes a post-fielding weapons systems assessment; for software acquisitions, a value assessment must satisfy PIR requirements.
OVERVIEW

The DoD IEA is the DoD’s “to be” IT Enterprise Architecture (Enterprise Reference Architecture model that all programs must design solutions in compliance with)

Based on the DoD Digital Modernization Strategy that has four (4) priority technological areas: Cloud; Artificial Intelligence; Cybersecurity and Command, Control and Communications (C3)

Solutions based on approved standards in the DoD IT Standards Registry within the Global Information Grid Technical Guidance Federation service.

Focus is interoperability and cybersecurity using MOSA design.
C3 systems deliver critical information across the full range of DoD missions

- **Waveform Management**: Must comply with DoDI 4630.09, “Communication Waveform Management and Standardization”
- **Spectrum Support**: Must comply with DoDI 4650.01, “Policy and Procedures for Management and Use of the Electromagnetic Spectrum”
- **Positioning, Navigation, and Timing (PNT)**: Must comply with DoDD 4650.05, “POSITIONING, NAVIGATION, AND TIMING (PNT),” and DoDI 4650.08, “POSITIONING, NAVIGATION, AND TIMING (PNT) AND NAVIGATION WARFARE (NAVWAR)”
Cybersecurity Alignment

- All programs must incorporate cybersecurity requirements IAW DoDI 8500.01, “Cybersecurity”
- Must include operational resilience, risk management and cyberspace defense
- Risk Management Framework (RFM): Must comply with DoDI 8510.01, “Risk Management Framework for DoD Information Technology (IT)” in order to achieve your Authority to Operate (ATO)
- All programs containing IT, including NSS, will have a Cybersecurity Strategy (CSS)
Trusted Systems and Networks (TSN) Alignment

PMs will manage TSN risk by:

- Mission critical functions and components must be protected by DoDI 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)”; Documented in the Program Protection Plan (PPP)

- Must conduct a criticality analysis to identify mission critical functions and critical components

- Must do a threat analysis of suppliers and gain a security validation of their development environment (Supply Chain Risk Management (SCRM)); request supplier disclosure of compliance and reporting requirements

- Verify cybersecurity resiliency of the TSN; requires rigorous network testing

- Engage with DoD Component’s TSN focal point on managing identified risk and SCRM

- Apply TSN best practices and lessons learned before acquisition of critical system components
Cloud Computing (Security Requirements Guide (SRG))

DoD Components will:

- Align with 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
- Obtain SRG compliance prior to adopting cloud computing as a solution for that capability
- Ensure their respective Program Executive Offices take necessary steps to accelerate the adoption of cloud computing in support of their systems
Acquisition of Information Technology (IT) Policy and Procedures

IT Management Requirements

• When acquiring commercial IT, PMs and acquisition personnel must abide by government contracting laws and regulations, the suitability of using DoD IT Category Management purchasing solutions, the DoD Enterprise Software Imitative (ESI), Federal Category Management procurement vehicles, DoD Component level enterprise software licenses all documented in the PM’s Acquisition Strategy.

• Commercial software acquisition must be IAW DoDD 8470.01E, “DOD EXECUTIVE AGENT (DOD EA) FOR COMMERCIAL SOFTWARE PRODUCT MANAGEMENT OF CORE ENTERPRISE TECHNOLOGY AGREEMENTS (CETAS)”

• DoD Data Center Management requirements are discussed. Any PM who intends to obligate funds for Data Centers must obtain prior approval from the cognizant DoD Component CIO; must submit quarterly Data Center obligation reports to the DoD CIO’s Data Center Consolidation office.

• Information Protection. PMs must comply with DoDI 5200.01, “DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)”
  • Includes Privacy, Information Quality, and Intelligence Data

• Records Management must comply with applicable statutes and regulations for information created, collected and retained electronically.

• 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
Acquisition of Information Technology (IT) Policy and Procedures

Summary – IT Acquisition Functional Policy (DoDI 5000.82)

- Supports the National Defense Strategy (NDS) to ensure DoD IT acquisitions **deliver performance at the speed of relevance**
- Supports the DoD Digital Modernization Strategy to **ensure interoperability and cybersecurity are achieved for seamless, transparent data and information sharing across DoD**
- Establishes functional acquisition policy and procedures for all programs containing IT
  - **Consolidates all DoD IT management policy under one regulation**
  - Restructures acquisition processes and procedures of all programs containing IT to a separate, functional acquisition policy (**Modular Policy Management**)
- **Adheres to the Adaptive Acquisition Framework** in DoDI 5000.02
- **Synchronizes DoD IT acquisitions on standards, architecture, and cybersecurity**
- **Provides interoperable and secure IT systems across the joint force**, increasing warfighter lethality
  - **Aligns all programs with IT** with the DoD Information Enterprise Architecture standards
Questions and Answers (Q&A)

Bob Skertic
Learning Director, Information Technology
Defense Acquisition University

bob.skertic@dau.edu