DoD INSTRUCTION 5000.86

ACQUISITION INTELLIGENCE

Originating Components:	Office of the Under Secretary of Defense for Acquisition and Sustainment Office of the Under Secretary of Defense for Intelligence and Security
Effective:	September 11, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Approved by:	Ellen M. Lord, Under Secretary of Defense for Acquisition and Sustainment Joseph D. Kernan, Under Secretary of Defense for Intelligence and Security

Purpose: In accordance with the authority in DoD Directive (DoDD) 5135.02 and DoDD 5143.01, this issuance establishes policy, assigns responsibilities, and provides direction for the integration of intelligence in the acquisition life cycle in accordance with DoDD 5000.01.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff (CJCS), the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. POLICY.

a. Intelligence must be integrated into the acquisition life cycle to ensure agile and effective warfighting capability.

b. Defense acquisition programs must use relevant information produced by the Intelligence Community in all phases of the acquisition life cycle.

c. Collaboration between the requirements, acquisition, research and development (R&D), and intelligence communities must be implemented to ensure awareness of adversary capabilities and intentions.

d. Defense acquisition personnel will manage all potential threats to an acquisition effort and focus on the critical intelligence parameters (CIPs). If an adversary defeats the CIPs, it will impede lethality, survivability, sustainability, and technological advantage of the acquisition system.

e. A cadre of trained acquisition and intelligence professionals must be available to ensure the integration of intelligence into the acquisition life cycle.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT (USD(A&S)).

The USD(A&S):

a. Provides DoD-wide acquisition and sustainment priorities for intelligence into the DoD's intelligence requirements prioritization and capability risk management processes; monitors the status of planning for and sufficiency of intelligence inputs to acquisitions to ensure a consistent risk management approach is used in evaluating those inputs; and provides:

(1) Direction to DoD Components to ensure intelligence threat inputs and intelligence supportability considerations are integrated into all relevant acquisition processes.

(2) Policy and best practices, and establishes cross-cutting processes to aid acquisition identification of existing and forecast intelligence support gaps.

(3) Policy to support effective articulation and monitoring of CIPs by acquisition personnel.

b. In coordination with the Under Secretary of Defense for Intelligence and Security (USD(I&S)), Under Secretary of Defense for Research and Engineering (USD(R&E)), and the CJCS, develops DoD-level courses of action to mitigate risk associated with intelligence support gaps.

c. Establishes and submits to the Defense Intelligence Enterprise (DIE) cross-Service portfolio CIPs for monitoring and awareness.

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

(1) Includes intelligence content (e.g., intelligence processes, categories of intelligence products, security requirements, and intelligence cost within total lifecycle cost estimating) within training and education programs for the Defense Acquisition Workforce.

(2) Oversees the implementation of acquisition related training and credentialing of acquisition and intelligence personnel responsible for applying intelligence and planning for intelligence supportability as part of acquisition processes.

2.2. ASSISTANT SECRETARY OF DEFENSE FOR ACQUISITION.

Under the authority, direction, and control of the USD(A&S), the Assistant Secretary of Defense for Acquisition maintains and supports a staff element sufficient to support effective integration of intelligence requirements within life cycle acquisition organizations, programs, and processes. Staffing functions include, but are not limited to:

a. Serving as principal acquisition intelligence advisor to the Defense Acquisition Executive for acquisition review processes.

b. Overseeing acquisition intelligence policy and continuous process improvement.

c. Providing acquisition-specific training to the acquisition intelligence workforce.

d. Measuring acquisition intelligence performance.

2.3. USD(I&S).

The USD(I&S):

a. Oversees intelligence support to the acquisition life cycle.

b. Assists the USD(A&S), the USD(R&E), and the CJCS in mitigating acquisition risk associated with intelligence gaps.

c. Advises the Director of Operational Test and Evaluation concerning intelligence supportability requirements that affect operational testing of acquisition programs.

d. Through the Director for Human Capital Management:

(1) Oversees the implementation of training and credentialing of intelligence personnel providing intelligence to support the acquisition life cycle.

(2) Provides to the USD(A&S):

(a) Expertise in training, education, and credentialing program for acquisition personnel to acquire necessary intelligence skills.

(b) Intelligence content (e.g., intelligence process, categories of intelligence products and intelligence cost within total life cycle cost estimating) for inclusion in Defense Acquisition Workforce training and education programs.

(3) Oversees implementation and execution of talent management and workforce development activities for acquisition intelligence as part of broader Defense Intelligence career field management.

2.4. DIRECTORS FOR THE DEFENSE INTELLIGENCE AGENCY; NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY; NATIONAL RECONNAISSANCE OFFICE; AND DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY; AND THE NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE.

Under the authority, direction, and control of the USD(I&S), the Directors for the Defense Intelligence Agency; National Geospatial-Intelligence Agency; National Reconnaissance Office;

Defense Counterintelligence and Security Agency; and the National Security Agency/Chief, Central Security Service, provide intelligence support related to their specific areas of responsibility.

2.5. USD(R&E)

The USD(R&E):

a. Establishes a strategic intelligence and analysis cell that will focus on understanding the capabilities and vulnerabilities of potential adversaries, assessing U.S. capabilities, tracking global technology trends, assessing emerging threats, and identifying potential opportunities that warrant action and investment.

b. Establishes policy to ensure intelligence threat inputs and intelligence supportability requirements are considered and integrated into R&D efforts.

c. Reviews DIE assessments on the advancement of the adversary threat and evaluates those assessments for any impact on R&D efforts, including development analysis and decisions.

d. In coordination with the USD(I&S), prioritizes intelligence product requirements that support R&D efforts, and ensures they are included in the DoD intelligence requirements prioritization and risk management processes.

e. Provides research and engineering policy, plans, advice, and assistance to the acquisition, intelligence, and requirements communities.

f. Identifies and oversees the integration of intelligence in cross-cutting demonstrations, prototyping, and experimentation activities, including strategic capability alternatives, across the DoD to inform new mission capabilities for the warfighter with focus on expediting transition timelines to meet critical challenges and operational needs.

g. Coordinates and provides acquisition intelligence considerations for use in DoD Component and USD(R&E) independent technology readiness assessments.

2.6. DIRECTOR OF OPERATIONAL TEST AND EVALUATION.

The Director of Operational Test and Evaluation engages with the USD(R&E); the USD(I&S); the USD(A&S); other OSD principals; DoD Component staff; and intelligence organizations throughout the DoD to ascertain the status of planning for and sufficiency of intelligence inputs for operational test and evaluation (T&E) and provides:

a. The operational T&E focal point for DoD-wide acquisition priorities for intelligence who works with the Office of the USD(I&S) and Joint Staff to integrate those priorities into the DoD's intelligence requirements prioritization and capability risk management processes.

b. Reviews DIE assessments on the advancement of the adversary threat and evaluates those assessments for any impact on operational T&E efforts.

2.7. SECRETARIES OF THE MILITARY DEPARTMENTS; COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND; AND DIRECTOR, MISSILE DEFENSE AGENCY.

a. The Secretaries of the Military Departments; the Commander, United States Special Operations Command; and under the authority, direction, and control of the USD(R&E), the Director, Missile Defense Agency:

(1) Oversee the application of intelligence threat inputs and planning for intelligence supportability within acquisition programs and across the acquisition life cycle.

(2) Ensure acquisition programs determine the intelligence products that are sufficient for a weapon system to perform its mission as part of the DoD's intelligence requirements and risk management processes.

(3) Oversee the prioritization of acquisition program intelligence requirements and apply courses of action to mitigate gaps and associated acquisition program risk in intelligence support to acquisition programs.

(4) Oversee the state of advancing threat timelines against acquisition program timelines for CIPs. The goal is to anticipate and evaluate the threat capability growth, and plan for and fund program risk mitigation (upgrades, etc.) within the content of the program of record before a CIP breach can occur. In the event that a CIP breach occurs, the program manager will convene the Configuration Steering Board to address mitigating actions.

(5) Ensure Service prototype boards are supported by acquisition intelligence personnel and are provided threat intelligence to inform merit-based prototype project selection.

(6) Manage the award of acquisition intelligence credentials for those personnel with requisite training and experience.

(7) Require that acquisition program plans and contracts provide technical data (e.g. mission system software algorithms, U.S. aircraft radar cross section data, parametric characteristics and performance data) that enables acquisition program determination of intelligence data dependency and sufficiency.

(8) Oversee acquisitions to ensure that acquisition intelligence professionals have facilitated the intelligence needs for programs.

b. In coordination with the Secretaries of the Military Departments; the Commander, United States Special Operations Command; and the Director, Missile Defense Agency, coordinate unique special operations and missile defense requirements in support of their respective acquisition programs.

2.8. CJCS.

The CJCS:

a. In accordance with the CJCS Instruction 5123.01 series and the Manual for the Operation of the Joint Capabilities Integration and Development System, oversees the integration of intelligence threat considerations and supportability requirements into the capability requirements process.

b. In coordination with the USD(A&S), the USD(R&E), and the USD(I&S), ensures joint warfighting requirements inform acquisition program development priorities and intelligence support priorities, in the development of courses of action to mitigate gaps in forecasted mission critical capability needs.

c. Manages the DoD-wide requirements prioritization and risk management framework for weapon system intelligence data needs.

d. In accordance with CJCS Instruction 5123.01H, and in coordination with the appropriate program office, capability sponsors, Functional Capabilities Board representatives, and other applicable stakeholders:

(1) Review CIP breaches and compromises of program information, as required.

(2) Recommend appropriate responses to requirements sponsors.

SECTION 3: INTELLIGENCE IN KEY ACQUISITION DOCUMENTS AND FUNCTIONS

3.1. INTELLIGENCE SUPPORT.

The DIE products that specifically support acquisition programs include, though are not limited to: threat modules; validated on-line life-cycle threat reports (including CIPs in accordance with DIA Instruction 5000.002); and technology targeting risk assessments.

3.2. INTELLIGENCE INFORMATION IN KEY ACQUISITION DOCUMENTS AND FUNCTIONS.

Acquisition program managers and other stakeholders must address intelligence requirements as they apply to certain acquisition documents and functional areas including but not limited to: acquisition strategies; analysis of alternatives; contracting; engineering and test plans; program protection; and life-cycle mission data planning. Threat focus for each of these must be oriented on the emerging or future projected threat (at a minimum, the threat at system initial operational capability plus 10 (IOC+10) years).

a. Acquisition Strategies.

Acquisition strategies must include:

(1) Characterization of the threat.

(2) Identification of intelligence supportability plans, risks, and cost drivers.

(3) Residual risk to inform stakeholders.

b. Analysis of Alternatives.

(1) Analysis must provide a comparison of emerging or future threat characterization and forecast intelligence supportability with the capability requirements for system IOC+10 years at a minimum.

(2) Threat analysis must be considered in evolutionary acquisition, prototyping, and a modular open systems approach.

c. Capability Requirements Documents.

Capability requirements documents must include:

(1) Characterization of the threat in comparison with the capability requirements (key performance parameters (KPPs), key system attributes (KSAs), and additional performance attributes (APAs)).

(2) Intelligence supportability assessment of the specified Joint Capabilities Integration and Development System intelligence supportability requirements categories (refer to Joint Capabilities Integration and Development System Manual or CJCS Instruction 5123.01H).

d. Request for Proposal and Other Transaction Authority.

(1) Supporting acquisition intelligence personnel will provide the contracting process with intelligence considerations to ensure effective research and prototype solutions are incorporated into the request for proposal or other transaction authority.

(2) The request for proposal or other transaction authority will compare threat characterization with the capability requirements to translate requirements into technical engineering level specifications that exceed threat parameters. Friendly and threat technical requirements must be compared and assessed in a mission assurance framework that incorporates broader manufacturing value chains and crosscutting industrial based sector variables to ensure risk, opportunity and life cycle cost are considered.

e. Systems Engineering Plan.

(1) Modular Open Systems Approach.

When using this approach, a systems engineering plan must:

(a) Provide characterization of the threat in comparison with the capability requirements (KPPs, KSAs, and APAs).

(b) Include prioritization of intelligence requirements.

(2) Modeling and Simulations.

Modeling and simulations must:

(a) Provide characterization of the threat in comparison with the capability requirements (KPPs, KSAs, and APAs).

(b) Include prioritization of intelligence requirements.

f. Test and Evaluation Master Plan.

(1) Developmental T&E.

(a) Early engagement with intelligence personnel can identify threat representation(s) (e.g., models and simulations, stimulators, foreign material needing to be acquired) needed to support test events. These threat representations must be integrated into the test and evaluation master plan (including costs, assets, needed test resources, and capabilities linked to test events) and used to support resource documentation (e.g., program objective memorandum).

(b) Acquisition planners must document how intelligence requirements, priorities, and associated resources necessary for test will be integrated into the overarching T&E program.

(c) Threat focus must be oriented on the emerging or future projected threat (at a minimum, the threat at IOC+10 years) and associated data.

(2) Operational T&E.

(a) Threat representations supporting an operational test event must be validated and accredited to ensure they are accurate portrayals of threat systems. Anticipated costs for threat representations (including surrogates, foreign materiel acquisition, or modeling and simulation applications) must be included in the test and evaluation master plan, and intelligence requirements should be prioritized.

(b) Characterization of the threat will be made in comparison with the capability requirements (KPPs, KSAs, and APAs).

(c) Threat focus must be oriented on the emerging or future projected threat (at a minimum, the threat at system IOC+10 years), and associated data.

g. Program Protection Plan.

A program protection plan will include:

(1) Threat reports that provide all-source intelligence analysis of suppliers of critical components to inform risk management decisions.

(2) Counterintelligence artifacts on the threat as part of systems security-related planning.

(3) As part of support to the anti-tamper plan included in the Annex to the program protection plan, an analysis of threats to the loss of critical program information through reverse engineering.

(4) International involvement, if any, and any related risks to critical program information and critical components.

h. Concept of Operations.

A concept of operations will document:

(1) How the system will be employed and the environment in which it is expected to perform each mission, including intelligence supportability requirements.

(2) Any operational measures that must be taken for the protection of critical program information and critical components embedded in the system.

i. Life-cycle Mission Data Plan.

(1) The life-cycle mission data plan is the program manager's plan that must articulate how the program and other organizations intend to address specific program needs for intelligence mission data required to operate mission systems in accordance with DoDD 5250.01.

(2) The life-cycle mission data plan must include the results from requirements prioritization and risk management for weapon system intelligence data needs.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
APA	additional performance attribute
CIP	critical intelligence parameter
CJCS	Chairman of the Joint Chiefs of Staff
DIE	Defense Intelligence Enterprise
DoDD	DoD directive
IOC+10	initial operational capability plus 10 (years)
KPP	key performance parameter
KSA	key system attribute
R&D	research and development
T&E	test and evaluation
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
acquisition intelligence	The application of intelligence such as foundational military intelligence about adversary threats and planning for intelligence dependency in acquisition projects, programs, and operations. This is not a new intelligence discipline.
acquisition life cycle	Defined in the Defense Acquisition University Glossary of Defense Acquisition Acronyms and Terms.
analysis of alternatives	Defined in the Defense Acquisition University Glossary of Defense Acquisition Acronyms and Terms.
CIP	Defined in Defense Intelligence Agency Directive 5000.200.
Configuration Steering Board	Defined in the Defense Acquisition University Glossary of Defense Acquisition Acronyms and Terms.
DIE	Defined in DoDD 5143.01.
intelligence integration	The act or process of incorporating and coordinating intelligence across the acquisition and requirements communities to address critical organizational and programmatic challenges requiring enhanced intelligence support to design, produce, field, and support advanced military capabilities. It encompasses accurate threat information, identification of intelligence support requirements, and intelligence supportability assessments.
intelligence requirement	Defined in the DoD Dictionary of Military and Associated Terms.
intelligence supportability	The availability, suitability, and sufficiency of intelligence information and capabilities to support the requirements or system defined in capability development documents.
modular open systems approach	An approach that integrates technical requirements with contracting mechanisms and legal considerations to support a more rapid evolution of capabilities and technologies throughout the product life cycle through the use of architecture modularity, open systems standards, and appropriate business practices.
research and engineering	Defined in DoDD 5134.3.

TERM	DEFINITION
risk management	Defined in the DoD Dictionary of Military and Associated Terms.
threat	The intention and capability of an adversary to undertake actions that would be detrimental to the interest of the United States. The sum of the potential strengths, capabilities, and strategic objectives of any adversary which can limit or negate mission accomplishment or reduce force, system, or equipment effectiveness.

REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 5123.01H, "Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)," August 31, 2018

Chairman of the Joint Chiefs of Staff, "Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS), August 31, 2018

Defense Acquisition University, "Glossary of Defense Acquisition Acronyms and Terms," current edition

Defense Intelligence Agency Directive 5000.200, "Intelligence Threat Support for Major Defense Acquisition Programs," June 19, 2018[1]

Defense Intelligence Agency Instruction 5000.002, "Intelligence Threat Support for Major Defense Acquisition Programs," June 19, 2018[2]

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

DoD Directive 5134.3, "Director of Defense Research and Engineering (DDR&E)," November 3, 2003

DoD Directive 5135.02, "Under Secretary of Defense for Acquisition and Sustainment (USD(A&S))," July 15, 2020

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

DoD Directive 5250.01, "Management of Intelligence Mission Data (IMD) in DoD Acquisition," January 22, 2013, as amended

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

[1] Available on the SECRET Internet Protocol Router Network at https://diateams.dse.dia.smil.mil/sites/issuances/lists/DIA%20Policies/Allitems.aspx

[2] Available on the SECRET Internet Protocol Router Network at https://diateams.dse.dia.smil.mil/sites/issuances/lists/DIA%20Policies/Allitems.aspx