Intelligence Support to the Adaptive Acquisition Framework (ISTAAF) Guidebook

September 2021

Office of the Under Secretary of Defense for Acquisition and Sustainment

Washington, D.C.

Intelligence Support to the Adaptive Acquisition Framework (ISTAAF) Guidebook

Office of the Under Secretary of Defense for Acquisition and Sustainment/Acquisition Enablers/Acquisition Intelligence Division
3030 Defense Pentagon
Washington, DC 20301
osd.pentagon.ousd-a-s.mbx.acquisition-intelligence-div@mail.mil

Approved by

CADMAN.DAVID.S.1229303615 Digitally signed by CADMAN.DAVID.S.1229303615 Date: 2021.09.09 13:55:08 -04'00'

September 9, 2021

David Cadman — Date

Acting Deputy Assistant Secretary of Defense, Acquisition Enablers
Office of the Under Secretary of Defense for
Acquisition and Sustainment

Intelligence Support to the Adaptive Acquisition Framework (ISTAAF) Guidebook Change Record

Date	Change	Rationale

This page is intentionally blank.

Contents

Tables

1 INTRODUCTION

1.1 Purpose

This Guide replaces the Defense Acquisition Guide Chapter 7 “Intelligence Support and Acquisition” and supports the new Adaptive Acquisition Framework. It provides optional guidance to Program Managers (PMs) and the acquisition intelligence (Acq/Intel) analysts who support them in order to acquire, integrate, manage, mitigate, and use intelligence to deliver maximum warfighting capability at minimum risk to cost, schedule, performance, and national security. This Guide provides links to exemplars, best practices, and resources for intelligence support to Department of Defense (DoD) acquisition processes. Additionally, PMs and analysts are encouraged to review related guides produced by the other Services in hopes of improving the knowledge, skills, and abilities of the workforce. If Service-specific Guides contain conflicting information with this Guide, follow your Service-specific guide.

1.2 Background

Intelligence support should be integrated into the acquisition life cycle to ensure intuitive, responsive and effective warfighting capabilities are delivered uncompromised, regardless of the acquisition pathway. Collaboration among the requirements, acquisition, test, research and development, and intelligence community is critical to ensure awareness of adversary capabilities, intentions, opportunities to target, and assessed threat levels. Acquisition Intelligence is the program office function that identifies and manages intelligence dependencies Acquisition program managers and other stakeholders must address these intelligence dependencies in certain acquisition documentation including acquisition strategies, analysis of alternatives, capability requirements documents, requests for proposals, systems engineering plans, test and evaluation master plans, program protection plans, concepts of operations, and life-cycle mission data plans..

For additional questions about Intel support to acquisitions, the Defense Acquisition Intelligence focal points (organizations and/or individuals) are:

- U.S. Office of the Under Secretary of Defense for Acquisition and Sustainment/Acquisition Enablers/Acquisition Intelligence Division: osd.pentagon.ousd-a-s.mbx.acquisition-intelligence-div@mail.mil
- U.S. Air Force: usaf.pentagon.af-a2.list.af-a2o-front-office@mail.mil
- U.S. Army: usarmy.pentagon.hqda-dcs-g-2.list.dami-fit-distribution
- U.S. Navy: DON_Intel_Acquisition@navy.mil (pending)

- Defense Intelligence Agency: disl118@coe.ic.gov (NIPRnet) or #NEDIAC_TLA-3_All@dia.smil.mil (SIPRNet).

2 ACQUISITION INTELLIGENCE BUSINESS PRACTICE

New Program Office technologies are highly dependent upon a variety of scientific and technical intelligence products throughout the acquisition lifecycle. This technological dependence, combined with rapidly evolving threats, challenges the delivery of DoD warfighting capabilities. It also drives the necessity to integrate intelligence throughout the lifecycle of a program for all acquisition pathways. When integrated properly, intelligence helps ensure capability requirements are realistic and translatable into engineering specifications that can compete in future operational environments and inform threat representations to ensure capability designs will meet national security requirements. DoDI 5000.86 (Acquisition Intelligence), published on 11 Sep 20, covers roles and responsibilities of the Intelligence Community (IC) support to PMs. The following are **best practices** captured across the Services:

2.1 Dedicated Acq/Intel Support

Program Offices should prioritize Acq/Intel staffing (i.e. contract support, military, or civilians) as early as possible in the acquisition lifecycle. Dedicated, embedded Acq/Intel analytic support takes a huge burden off PMs by being their liaisons to the intelligence community (IC). Efficiencies are gained by using Intel analysts who can task the IC for support, research all-source Intel reporting, synthesize that Intel, and make sound analytic judgments on threat to inform program office decisions. Dedicated Acq/Intel analysts assigned to a Program Office support PMs in the same fashion as dedicated finance, contracting, logistics, engineering, and security professionals.

2.2 Baked-In Digital (Machine-to-Machine) Interoperability

Baking-in digital interoperability for growing the DoD digital ecosystem is paramount to remain ahead of our adversaries. To this end, any machine-to-machine interfacing is beneficial. When digital interoperability is considered from the start, the growing list of digital Intel threat products can feed and improve a program's development decision choices (ie. supporting Digital Engineering), analysis of alternatives, testing environments, Critical Intelligence Parameter (CIP) breach reporting, and eventually artificial intelligence capabilities that can reduce dependencies on manpower-intensive processing. (See Section 2.4 for use of 'XML data tagging')

2.3 Use of Tailored/Dynamic Intel Reporting

Acq/Intel analysts are filling gaps with tailored threat Intel products for those programs for which there is no timely, formal threat reporting from the DIE. Production Requests (PRs) for statutory and regulatory Intel threat products like Validated On-line Lifecycle Threat (VOLTs), Validated IMD Supportability Reports (VISRs), and Technology Targeting Risk Assessments (TTRAs) should still be tasked for programs that require them. For all

others, Acq/Intel analysts can provide tailored, non-validated, threat products for program office consumption. These products and assessments are compiled using existing, validated, 'finished intelligence' produced by the DIE, as well as open source reporting and unfinished intelligence sources. Many times, these types of threat reports are preferable to no threat Intel at all. Examples of a few are covered in Section 4, Table 1.

2.4 Use of SIPRNet and JWICS Intel Sites to Reduce Stove-Piped Intel Reporting Archives

Acq/Intel analysts should share tailored reports liberally, with the widest possible dissemination (in accordance with need to know, classification, and handling controls). When Intel analysts produce tailored threat assessments, they should share them with the DIE (and specifically with the Intelligence Production Centers the used as resources to build their reports). Sharing tailored threat assessments helps inform the task-saturated DIE and likely informs other programs with similar threats. Analysts can share threat assessments via Secure Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communications System (JWICS), and within collaboration forums like R-Space and iSPACE. Although not mandated, wherever possible, Intel reporting should include 'XML data tagging' of the contents in preparation for use in future digital intelligence capabilities across the Services. Using Intel Community Directive (ICD) standards to build tailored products sharpens the entire Intel workforce. (Link to ICDs)

- ICD 203: *Analytic Standards:* establishes IC analytic standards that govern the production and evaluation of analytic products; articulates the responsibility of intelligence analysts to strive for excellence, integrity and rigor in their analytic thinking and work practices.
- ICD 206: *Sourcing Requirements for Disseminated Analytic Products:* establishes the requirements for sourcing information in disseminated analytic products.
- ICD 501: *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*: directs the IC to foster an enduring culture of responsible sharing and collaboration within the DIE; provides an improved capacity to warn of and disrupt threats to the US; provides more accurate, timely and insightful analysis to inform decision making by the President, senior military commanders and other executive branch members.

3 THREAT REPORTING AND INTELLIGENCE SUPPORTABILITY

Acq/Intel analysts are liaisons between the acquisition and intelligence communities. The two fundamental mission areas for Acq/Intel analysts are: to inform PMs of **threats** to their systems and document the **intelligence supportability** requirements of a system over the entire lifecycle for the DIE to determine if the program can be supported.

3.1 Threat

A threat is defined as an adversary's intent, capability and opportunity to target, exploit or compromise U.S. Government critical technologies, programs or information. Evolving threats drive the need for acquisition resiliency and flexibility for systems to remain relevant in a modern battlespace. Threat resources and reports that assist Acq/Intel analysts in support of their PMs include: Defense Intelligence Agency's (DIA) Defense Intelligence Threat Library modules, DIA and IPC VOLT Reports, Critical Intelligence Parameters (CIPs), TTRAs, the Threat System Database (TSDB), Threat Test Support Packages (TTSP), and Adversary Cyber Threat Assessments (ACTA).

NOTE: As additional best practices are created, owners are encouraged to share developments with the OUSD/A&S/AE Acquisition Intelligence Division so they can be disseminated across the entire workforce and integrated into Defense Acquisition University Acq/Intel training modules.

3.2 Intelligence Supportability

Intelligence supportability includes a review of a program's Intel-driven DOTMLPF-P (i.e., Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy). Intel Health Assessments (IHAs) are reports used to summarize a program's Intel supportability requirements and in turn, identify any gaps that could impact a program's Initial Operating Capability (IOC). It is vital to assess and document a program's requirements as soon as possible so the IC can prepare before a system is delivered for operational use. A new system/capability may require increased Intelligence Mission Data (IMD) or processing capability; an increase in the number of intelligence analysts at operating locations; or new classified facilities in which to operate the system/capability. Just as any program office will document the requirements for consumables (fuel, storage, parts, power, etc.), each program should document the intelligence supportability requirements needed to operate so the IC can prioritize their resources to support them. PMs use Lifecycle Mission Data Plans (LMDP) to capture IMD needs (see Section 4.5). Intel Health Assessments (IHA) are used to capture all Intel support requirements

4 INTELLIGENCE INTEGRATION TO THE ADAPTIVE ACQUISITION FRAMEWORK (AAF)

The AAF drives more acquisition flexibility for PMs; to remain ahead of current and emerging threats; to take advantage of new technologies; to increase interoperability via a digital ecosystem; to reduce schedule/costs; and enhance national security. The AAF helps PMs respond to the Acquisition Agility Act (AAA) of Fiscal Year (FY) 2017 (part of the National Defense Authorization Act of FY2017) and the focus on a more “agile” Defense Acquisition System (DAS). In addition to being flexible with changes in technology and capability evolutions within the decision cycle of a warfighting program, PMs should be able to respond to dynamic threats provided by the IC.

Acq/Intel Intelligence support to agile acquisition is predicated on clear and thorough communication within the PMO. Acq/Intel analysts should work proactively with the PM and technical staff to gain insight into a system’s capabilities, components, and attributes. This improves the analyst’s ability to request appropriate threat intelligence and produce relevant threat products to inform programmatic decision points. Early (and regularly updated) intelligence supportability assessments will help the Acq/Intel analysts ensure responsive threat reporting throughout the acquisition lifecycle.

Intelligence support to agile acquisition is tailorable and valuable to any Acquisition Pathway. Per DoDI 5000.02, there are six acquisition pathways a PM can choose that best fit their program’s acquisition type. The Acq/Intel analyst should work with the PM to identify which threat products are most beneficial to their program. What follows is a summary of the types of intelligence products that can be tailored for each acquisition pathway.

NOTE: The VOLT is required for Major Capability Acquisitions and programs on the Director Operational Test & Oversight (DOT&E) oversight list, but can be valuable to Middle Tier and Urgent Capability Pathways if the DIE is able to produce one. Regardless of a program’s acquisition pathway, the VOLT is also included among DIE products that PMs must use in developing their cyber security strategy and risk assessments. Program offices are highly encouraged to formally request Intel support through a Production Requirement (PR) in COLISEUM, regardless of which Pathway is used. The PR articulates the demand signal so the DIE can advocate for more resources to answer requests it currently cannot support. The bottom line is if a non-ACAT ID PM needs intel, the Acq/Intel analysts have multiple options other than a VOLT.

Table 4-1 Intelligence Support Product Matrix

	Validated On-line Lifecycle Threat (VOLT)	Technology Targeting Risk Assessment (TTRA)	Critical Intel Parameters (CIPs)	Intelligence Health Assessment (IHA)	AF Adversary Cyber Threat Assessment (ACTA)	Army Threat Test Support Package (TSSP)	DIA Validated IMD Supportability Report (VISR)
Acquisition Pathway							
Urgent Capability Acquisition	X		X	X	X	X	X
Middle Tier Acquisition	X		X	X	X	X	X
Major Capability Acquisition	X	X	X	X	X	X	X
Software Acquisition	X	X	X	X	X		
Defense Business Systems Acquisition	X		X	X	X		
Defense Acquisition of Services	X			X			
Continued on next page							
Acquisition Docs Supported by Intelligence							
Acquisition Strategy	X			X	X		X
Analysis of Alternatives (AoA)	X			X	X		
Capability Requirements Document (CRD)	X			X	X		X
Requests for Proposal (RFP)	X						X
System Engineering Plan (SEP)	X		X		X		X
Test and Evaluation	X				X	X	X

Master Plan (TEMP)							
Program Protection Plan (PPP)	x	x	x		x		
Concept of Operations (CONOPS)	x		x	x	x		
Lifecycle Mission Data Plan (LMDP)				x			

4.1 Validated On-line Lifecycle Threat (VOLT) Reports

The VOLT report is the authoritative threat assessment tailored for one specific program. A VOLT report includes threat modules and is written to articulate the relevance of each module to a specific acquisition program or planned capability. Acq/Intel analysts can request Portfolio VOLTs or Family-of-System VOLTs to serve multiple ACAT I-III programs, but Major Capability Acquisitions and programs on the DOT&E oversight list require a unique, system-specific VOLT. VOLT production starts with the establishment of a Threat Steering Group composed of the program office representatives, DIA/Service Intel Production Center rep, DevOps Test representatives, and the program's Acq/Intel analyst. The goal is to identify the program's Key Performance Parameters (KPPs), critical components/functions, and relevant threats, including a review or addition of CIPs. Exemplars of VOLT reports are available on SIPRNet at https://threatlibrary.d-se.dia.smil.mil/VOLTs/ or JWICS at https://threatlibrary.dodiis.ic.gov/VOLTs/

Key points:

- IPCs produce VOLT reports and DIA validates those produced for ACAT ID or IAM programs.
- VOLT reports can be used to support multiple programs with similar performance attributes, or those that share an employment concept of operations (CONOPs) and have a similar employment timeline.
- DIA contact information and the VOLT report request form are available on SIPRNet at https://threatlibrary.dse.dia.smil.mil/Resources, and JWICS at https://threatlibrary.dodiis.ic.gov/Resources and https://intellipedia.intelink.sgov.g-ov/wiki/TLA-3_Contacts

4.2 Critical Intelligence Parameters (CIPs)

A CIP is a defined threat capability or threshold at which a foreign system may compromise mission effectiveness of a U.S. system or systems. If an adversary capability

breaches a CIP, it will impede the lethality, survivability, sustainability, and technological advantage of the system(s) in acquisition. CIPs therefore receive focused intelligence analysis and reporting that informs revisions to requirements, incremental upgrades, or potentially new acquisition programs in order to ensure capabilities remain technologically competitive on the modern battlefield. Acq/Intel analysts help the program office to identify CIPs and submit them via PRs in COLISEUM. Periodically reviewing open CIPs enables risk-based decisions for program resiliency. CIPS are monitored and tracked in COLISEUM. Examples of CIPs are available at the following SIPRNet site: https://intellipedia.intelink.sgov.gov/wiki/Critical_Intelligence_Parameter#.28U.29_cip_examples

Key points:

- CIPs submitted to IPCs become part of the program's VOLT page in the Threat Library and are monitored to keep acquisition and requirements communities informed on high priority threat developments.
- CIP development should consider predictive and future threats in addition to current threats.
- A CIP is analogous to an objective KPP in an adversarial system capability.
- CIPs are considered "breached" when adversary capability advancements exceed a critical parameter.

4.3 Technology Targeting Risk Assessments (TTRAs)

A TTRA is a country-by-country assessment that quantifies risks to a) Critical Program Information (CPI); b) enabling or advanced technologies for weapons systems or programs; and c) facilities such as laboratories, factories, research and development sites (e.g., test ranges) and military installations. TTRAs are an important foundation for the Multi-disciplined Counterintelligence Threat Assessment (MDCITA) which reports adversary collection capabilities relative to the program's critical information and the protection of that information. The TTRA is a MS-A requirement document for ACAT I-III programs that have identified CPI.

Key points:

- Each Military Dept's supporting Defense CI Component produces the TTRA. DIA validates the TTRA for ACAT ID and ACAT IAM programs while the Military Dept's IPCs validate the TTRA for ACAT IC, IAC, and lower programs.
- CPI can include information about facilities, applications, capabilities, processes, and end-items; elements or components critical to a military system or network mission effectiveness; and technology that would reduce the U.S. technological advantage if it came under foreign control.

- The process for obtaining a TTRA involves coordination between DIA and the supporting Defense CI Component which gathers programmatic information necessary to aid the analytic process.

- The TTRA forms the analytic foundation for the CI assessments (e.g., MDCITA and CI Support Plan) in the Program Protection Plan (PPP).

- CI resource: DoDI O-5240.24, Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA), establishes policy, assigns responsibilities, and provides procedures for the conduct of the CI activities supporting RDA and is available by emailing the following address: whs.pentagon.esd.mbx.dod-directives@mail.smil.mil.

4.4 Intelligence Health Assessments (IHAs)

IHAs evaluate the nine JCIDS categories to ensure Intel support for a system is documented. The PM uses the results of an IHA to identify and document Intel production requirements, CIPs, IMD, the level of intelligence support needed, the integration of intelligence information into program decision making and system engineering, and to involve any applicable foreign military sales stakeholders.

4.5 Lifecycle Mission Data Plans (LMDPs)

The LMDP is the PM's plan that defines how the capability intends to use intelligence data required to operate the system. Gaps in IMD diminish the capabilities of systems and can expose vulnerabilities. If a program uses IMD, it will need an LMDP.

The types of IMD are:

- Characteristics and Performance (C&P) data of adversary systems;

- Order of Battle data that enable prioritization and defense against enemy systems;

- Signatures data that enable detection and distinction between friendly, neutral and enemy systems;

- Geospatial Intelligence (GEOINT) data that provide mapping and locating data;

- Electronic Warfare Integrated Reprogramming (EWIR) data that identify and counteract enemy radar and detection.

Acq/Intel analysts help PMs determine if they need an LMDP and assist in LMDP development. They also aid program entry into the DoD requirements prioritization and production planning processes for EWIR, Signatures, C&P, Order of Battle, and GEOINT products.

A program's LMDP is updated before each milestone decision in order to enable updated availability assessments and associate risk mitigation decisions. Reasons include: new adversary threats emerging in the battlespace; program/capability requirements change; new IMD has been produced since the previous milestone; product types, standards, and specifications change at the Intelligence Production Centers.

When gaps are forecasted, program offices receive feedback regarding those shortfalls, the cost, and courses of action being taken to close critical shortfalls. (See Section 4.6 ref DIA's VISR)

Key points:

If a program uses Intel mission data, they will need an LMDP.

- The LMDP requirement begins at MS-A and is updated in accordance with designated lifecycle events.
- For questions on identifying priorities and requirements for establishing an LMDP, contact DIA's Defense Technology and Long-Range Analysis Office, Acquisition Intelligence Division (TLA-3) at: IMDC_LMDP_Support@dia.smil.mil.
- A Program Executive Officer and Component Acquisition Executive-approved draft LMDP is due for a development Request for Proposal (RFP) release.
- The Annual Priorities and Risk Management Framework (PRMF) is a requirements and prioritization process to inform, drive, and optimize DIE support and production. Requirements documented in previous cycles constitute the baseline. Service customers should modify existing or submit new requirements continuously. New or recently updated LMDPs significantly assist this process. J285 submits PRMF tasks to Services to capture any other IMD requirements not previously identified. J285 consolidates and then submits the Annual PRMF to IPCs for annual production plans. The Annual PRMF presents the highest priority requirements to support production planning and forecasting across the FYDP while recognizing that a variety of factors, including adjustments by requirements managers, will affect out-year production. Questions concerning priorities and requirements for production planning within the Joint Staff PRMF should be directed to the Joint Staff/J285 at: js.pentagon.j2.list.j285-all@mail.mil.
- PMs or Acq/Intel analysts who need assistance in the development of LMDPs or who wish to learn more about IMD production, should contact DIA's Intelligence Mission Data Center at: IMDC_LMDP_Support@dia.smil.mil.

4.6 Validated IMD Supportability Reports (VISRs)

DIA's VISR is the assessment of LMDPs in support of the IMD producers and the acquisition process, as facilitated and coordinated by DIA/TLA-3. The VISR provides the program office and other stakeholders with a concise and consolidated view of IMD availability and production factors. The VISR provides a technical evaluation of the

enterprise's ability to support IMD demands throughout a weapon system's lifecycle. It gives decision makers the mission context about IMD production status (holdings and efforts to fill gaps) and warns intelligence enterprise of analytic and production demands; also facilitates IPC production/resource planning. The VISR also explains the IMD dependency, production suitability, and availability of IMD with additional recommendations to stakeholders.

Key Points:

- DIA/TLA-3 ties IMD requirements and any shortfalls to their associated KPPs/KSAs.
- The Dependency Determination explains traceability to acquisition program capabilities.
- The Production Suitability confirms whether IPCs can provide standard products. If not, the VISR highlights unique parameters or specifications.
- Availability Assessment is a gap analysis. Narratives and tables provide a breakdown by IMD product line and CL. The analysis also includes relevant reporting on the threat system from the Threat Library, VOLT, or CIP to highlight a critical gap.

VISR deliverables can assist the sponsor's risk assessment and the program's LMDP at a future milestone. The LMDP is key to identifying gaps in mission critical IMD prior to system deployment. The development and processing of an LMDP, and subsequent VISR, also makes DoD Intelligence Components (DODIC) aware of intelligence requirements of future systems. (Contact the DIA/TLA3 office in Section 1.2 POCs for more information.)

4.7 Threat Test Support Package (TTSP)

The TTSP is the baseline threat document for a specific test to describe the threat to be portrayed, specific guidance on threat targets and countermeasures, and how the threat fits into the overall Test and Evaluation (T&E) requirements. When a validated threat to a program exists, that threat should be portrayed during the program's T&E process and a TTSP prepared if data from the test supports a milestone decision review. Refer to Army Regulation 381-11 for detailed content and formats.

4.8 Adversary Cyber Threat Assessments (ACTAs)

ACTAs are produced by Acq/Intel analysts supporting the program office; however, ACTAs can be bolstered by an IPC when a Production Requirement (PR) is submitted in COLISEUM with specific questions. ACTAs are not considered 'finished intelligence' products from an IPC but may suffice when formal Intel threat products are not available. Many PMs will accept an Acq/Intel analyst threat product now while they wait for an IPC's 'finished intel' product. ACTAs provide a wide range of acquisition customers (e.g., PMs, systems security engineers, Security Control Assessors, Authorizing Officials, etc.) with

tailored cyber threat intelligence in support of a variety of program requirements (e.g., Risk Management Framework (RMF) implementation, design review analyses, technical requirements development, test planning, etc.). ACTAs utilize all-source intelligence products from the IC in combination with responses to follow-on PRs tailored to address the program's specific technical concerns. ACTAs take many forms and are tailored to what the program office needs (e.g.., textual report, briefing, threat matrices, etc). They can be initiated at any point in the acquisition life cycle but are commonly produced to support program office planning related to RMF implementation, as well as certification and accreditation reviews culminating in authority to operate (ATO) or authority to test (ATT). ACTA-derived cyber threat intelligence informs the measurement of cyber risk, supports the prioritization of system-level vulnerabilities for remediation, and can satisfy the cyber security threat requirements for a program's cyber security strategy. Refer to AF Life Cycle Management Center's Acq/Intel Guide page 51, for more details on ACTA. An ACTA example is available on SIPRNet at: https://intelshare.intelink.s-gov.gov/sites/afmc-a2-master/esc_xr2/ACTA/S_NF%20AWACS%20ACTA%20Exemplar.pptx.

5 INTELLIGENCE SITES AND SYSTEMS TO BENEFIT ACQ/INTEL

The following websites and systems will benefit Acq/Intel analysts in the performance of their duties:

- DIA Intelligence Threat Library (DITL): The DITL is the repository of threat modules and VOLTS. As stated in Section 4.1, DIA maintains the Defense Intelligence Threat Library, where current VOLT reports can be found on SIPRNet at https://threatlibrary.dse.dia.smil.mil/volts and on the JWICS at https://threat-library.dodiis.ic.gov/volts.
- Threat System Database (TSDB): The TSDB, formerly called the Automated Joint Threat Systems Handbook, is a database and website on SIPRNet (https://tsdb.msic.dia.smil.mil) maintained by the T&E Threat Resource Activity under the DOT&E. The TSDB provides information on a variety of resources for use in T&E and training. It includes threat representative systems such as simulators, targets, models and simulations, and actual threat hardware/foreign materiel. It also provides information about threat testing facilities and ranges.
- Office of Naval Intelligence Requirements (ORCA/ELCA): Next generation cloud-based, machine-to-machine transfer of IMD and Modeling and Simulation data providing digital threat support for Navy Operations.
- Dept. of Navy ISR Requirements Tool (DIRT): Provides the ability to derive, document, and submit IMD and Modeling and Simulation data.
- DIA Machine-assisted Analytic Rapid Repository System (MARS): Enables machine-to-machine operations for Acq/Intel use and helps with Indications and Warning of emerging threats.
- R-Space/i-Space: Research and Intelligence collaboration sites respectively. Resides on SIPR/JWICS and requires certificate for access. These are great sites to read, comment, and share Intel articles/reporting for a wide variety of mission areas. The SIPR site is: https://ispace.dia.smil.mil/ispace4s/activity?focusstatu-supdate=true.
- Library of National Intelligence (LNI): The LNI was developed to respond to the findings and suggestions of the 9/11 Commission; the Iraqi Weapons of Mass Destruction Commission; and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. The LNI is part of the Director of National Intelligence's efforts to build a more collaborative Intelligence Community; improve information sharing and modernize the IC's business practices. The LNI is available on JWICS at https://ni.cia.ic.gov.

6 TRAINING OPPORTUNITIES

This section lists training events and initiatives across the Service Departments throughout the year. For more information regarding access, dates, and locations, contact the respective owning training providers. If readers are aware of other events, please pass them on to the OSD/A&S/AE Acq/Intel Division for inclusion in future versions of this guidance.

- Army/G2 iSTART: Virtual and in-person training event for Army FIOs and those interested in the Intel support to acquisition mission area.
- AF Life Cycle Management Center/Intelligence Directorate (AFLCMC/IN) Intelligence Formal Training Unit (IFTU): Virtual and in person training event several times during the year for AF's Acq/Intel workforce.
- DAU ACQ 110 Fundamentals of Acquisition Intelligence: This course provides a joint, service-level overview of Acq/Intel that addresses timely and effective communication between the intelligence, requirements, and acquisition communities throughout the acquisition lifecycle.

7 ACQUISITION INTELLIGENCE GROUPS AND COMMITTEES

- The Acquisition Intelligence Support Working Group (AISWG) is composed of representatives from the Military Service intelligence staffs, acquisition community, testing community, capabilities development community, and the Defense Intelligence All-Source Analytic Enterprise. The AISWG, chaired by DIA, meets regularly to identify and address issues affecting acquisition intelligence support throughout all stages of the defense acquisition process.
- The Joint Staff Annual Acquisition-Intelligence-Requirements Priorities and Risk Management Framework (PRMF) addresses cross-community challenges as the demand for intelligence exceeds production capacity; as advancing threats degrade U.S. strategic advantages; and as weapon system vulnerabilities are increasing.
- The Acquisition-Intelligence-Requirements Committee (AIRCOM) is an executive body chartered to increase the satisfaction of critical intelligence data requirements and coordinate across seams in authorities and resources. Their scope is threat Modeling and Simulation software models, Signatures, Characteristics and Performance, and Electronic Warfare Integrated Reprogramming.
- Joint Integration Cell (JIC) coordinates current and future Intel mission data sufficiency analysis efforts throughout the DoD. Led by Secretary of the Air Force, Administrative Assistant's Concepts, Development, and Management Office (SAF/CDM), the JIC ensures timely execution of funds, synchronizes intelligence support for model creation, monitors simulations, and reports outcomes to OUSD.

- Chief Modeling and Simulation Office (CMSO) oversees Modeling and Simulation efforts and resources across the Department of the Air Force.
- Intelligence Mission Data Standing Working Group (IMD SWG) is a committee under the DoD Functional Manager for Analysis (FM/A) with senior membership comprised of the senior scientists from each of the Service Intelligence Centers, and the Missile and Space Intelligence Center. The IMD SWG serves as a consulting body to recommend priorities across the DIE and to synchronize IMD production efforts across the IPCs and our Five Eye Allied Partners to meet consumer requirements.

REFERENCES

The references cited in this table focus on acquisition and intelligence issuances that provide additional information to the PM and the Acq/Intel analysts supporting them. In addition, DAU has a comprehensive site that links to many of the policies below: DAU Policy Site

Department of Defense
DoD Directive 5000.01, The Defense Acquisition System
DoD Directive 5240.01. DoD Intelligence Activities
DoD Directive 5240.02, Counterintelligence (CI)
DoD Instruction 5000.02, Operation of the Adaptive Acquisition Framework
DoD Instruction 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)
DoD Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
DoD Instruction 5240.18, Counterintelligence (CI) Analysis and Production
DoD Instruction 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers
DoD Manual 5000.78, Rapid Acquisition Authority (RAA)
Joint Chiefs of Staff
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) Chairman of the Joint Chiefs of Staff Instruction 3318.01, Acquisition Intelligence Requirements Annual Priorities and Risk Management Framework (restricted: must be accessed from a gov/.mil account)
Defense Intelligence Agency
Defense Intelligence Agency Directive 5000.200, Intelligence Threat Support for Major Defense Acquisition Programs, available on SIPRNet https://diateams.dse.dia.smil.mil/sites/issuances/DIA%20Policies%202/diad%205000.200%202018.pdf
Defense Intelligence Agency Instruction 5000.002, Intelligence Threat Support for Major Defense Acquisition Programs, available on SIPRNet https://diateams.dse.dia.smil.mil/sites/issuances/DIA%20Policies%202/diad%205000.002%202018.pdf
Department of the Air Force
Air Force Policy Directive 63-1 and Air Force Policy Directive 20-1, Integrated Life Cycle Management
Air Force Instruction 63-101/20-101, Integrated Life Cycle Management
Air Force Manual 63-119, Certification of System Readiness for Dedicated Operational Testing
Air Force Pamphlet 63-113, Program Protection Planning for Life Cycle Management
Air Force Pamphlet 63-128, Integrated Life Cycle Management

Department of the Army
Army Regulation 70-1, Army Acquisition Policy
Army Regulation 70-41, Armaments Cooperation
Army Regulation 70-77, Program Protection
Army Regulation 381-10, U.S. Army Intelligence Activities
Army Regulation 381-11, Intelligence Support to Capability Development
Department of the Army Pamphlet 70-3, Army Acquisition Procedures
Department of the Navy
Secretary of the Navy Instruction 5000.02F, Defense Acquisition System and Joint Capabilities Integration and Development System Implementation
Secretary of the Navy Instruction 5000.42, Department of the Navy Accelerated Acquisition for the Rapid Development, Demonstration and Fielding of Capability
Secretary of the Navy Instruction 5200.46, Department of the Navy Modeling, Simulation, Verification, Validation, and Accreditation Management
Secretary of the Navy Instruction 5400.15C, Department of the Navy Research and Development, Acquisition, Associated Life-Cycle Management, and Logistics Responsibilities and Accountability
Chief of Naval Operations Instruction 3811.1F, Threat Support to the Defense Acquisition System
Chief of Naval Operations Instruction 3880.6B, Scientific and Technical Intelligence Liaison Officer (STILO) Program and Intelligence Support for the Naval Research, Development, Test & Evaluation, and Acquisition Communities
Chief of Naval Operations Instruction 5000.53A, U.S. Navy Maritime Accelerated Acquisition