Intelligence Support to the Adaptive Acquisition Framework (ISTAAF) Guidebook

September 2023

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 Integration & Interoperability/Acquisition Intelligence Division
3030 Defense Pentagon
Washington, DC 20301
osd.pentagon.ousd-a-s.mbx.acquisition-intelligence-div@mail.mil

Approved by

TREMPER.DAVID.E.1228812575 Digitally signed by TREMPER.DAVID.E.1228812575 Date: 2023.10.02 15:31:29 -04'00'

David Tremper

02-Oct-2023

Date

Deputy Assistant Secretary of Defense, Acquisition Integration & Interoperability (AI2)
Office of the Under Secretary of Defense for Acquisition and Sustainment

Contents

1.0 INTRODUCTION

1.1 Purpose

In 2022, the Defense Acquisition Guidebook was retired and replaced by a set of 13 modern guidebooks (https://aaf.dau.edu/guidebooks/) aligned with our new acquisition policies (see Table 1). These guidebooks support the Department's commitment to transition non-mandatory acquisition business practices to a more modern and agile set of guidance documents aligned with the Adaptive Acquisition Framework pathways and functional policies.

Table 1: Acquisition Guidebooks

Acquisition Guidebooks	
Intelligence	IT & Business Systems
Cost Estimating	Program Management
Cybersecurity	Technology and Program Protection
Engineering	Sustainment
Human Systems Integration	Test & Evaluation Enterprise
International Acquisition	Intellectual Property
Software Development	

The Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S) developed the Intelligence Support to the Adaptive Acquisition Framework (ISTAAF) Guidebook to support both acquisition professionals and acquisition intelligence professionals. It is designed to clarify the requirements and intent of providing intelligence support to the adaptive acquisition pathways.

1.2 Background

Acquisition decision makers must be aware of relevant threats to their programs, and acquisition intelligence plays a critical role in addressing intelligence dependencies (intelligence supportability) for the Department's warfighting capabilities. OUSD (A&S) established the Acquisition Intelligence Division (AID) under the Assistant Secretary of Defense for Acquisition to better enable intelligence integration through policy, guidance, and training support. For more information, visit the AID website: https://www.acq.osd.mil/asda/ae/ada/acquisition-intelligence.html

The 2022 National Defense Strategy (NDS) highlights the importance of ensuring our acquisition systems are resilient and agile in the face of threats with a focus toward the People's Republic of China (PRC) and preventing PRC dominance of key regions. The NDS also identifies the acute threat posed by Russia and other persistent threats, including those posed by North Korea, Iran, and violent extremist organizations.

10 U. S. Code §4211 directs development of an acquisition strategy for each major defense acquisition program, each major automated information system, and each major system approved by a milestone decision authority. Where appropriate, acquisition strategies should consider integrating current intelligence assessments into the acquisition process.

The ISTAAF Guidebook reinforces the Department's acquisition intelligence related policy contained within DoDI 5000.86, "Acquisition Intelligence," and attempts to improve overall awareness of acquisition intelligence related tools, methodologies, and best business practices from across the Department to enable the efficient and effective integration of intelligence (threat & intelligence supportability) into the Defense Acquisition System (DAS) to inform and influence decisions. Note that DoDIs, AAFDID, and similar instructions and directives are subject to change. We anticipate DIAS 5000.1 to supersede DIAD 5000.200 and DIAI 5000.002 in the first quarter of FY24. The next revision of this Guide will incorporate updated policies as appropriate.

ACQUISITION INTELLIGENCE

As defined in DoDI 5000.86, acquisition intelligence is the application of intelligence about adversary threats, and the planning for intelligence dependencies in acquisition i.e., threat and intelligence supportability.

- Threat: the sum of the potential strengths, capabilities, and strategic objectives of an adversary, which can limit or negate mission accomplishment or reduce force, system, or equipment effectiveness.
- Intelligence supportability: the identification and assessment of all intelligence support requirements, and anticipated shortfalls, throughout a capability's lifecycle.
- Intelligence support areas are found within the Threat and Intelligence Supportability and Certification Guide of the JCIDS Manual.

2.0 BUSINESS PRACTICES

Acquisition programs are highly dependent upon a variety of scientific and technical intelligence products throughout the acquisition life cycle. This drives the necessity to integrate intelligence throughout the life cycle of a program for all acquisition pathways. When integrated properly, intelligence helps ensure acquisition programs meet operational requirements. DoDI 5000.86, "Acquisition Intelligence," published on 11 Sep 20, covers roles and responsibilities of the Intelligence Community (IC) support to program managers (PMs). The following are best practices captured across the Services.

2.1 Dedicated Acquisition Intelligence Support

Program Offices should prioritize acquisition intelligence staffing (i.e., contract support, military, or civilians) as early as possible in the acquisition life cycle. This is critical to ensure the program is effectively scoped given the threat environment and informed Key Performance Parameters (KPPs): shaping the designs is best done early in the process as later in the lifecycle drives significant cost, schedule, and technical risks.

Every Major Capability Acquisition (MCA) should have a dedicated, embedded, acquisition intelligence analyst. Acquisition intelligence professionals should be assigned to a Program Office to support PMs in the same fashion as dedicated finance, contracting, logistics, engineering, and security professionals.

Embedded acquisition intelligence professionals assist PMs by working with the IC to research and synthesize all-source intelligence to inform programmatic decisions.

2.2 Digital Interoperability

The Department is moving toward digital engineering. To remain relevant, the IC must move toward digital system management and use of model-based systems engineering. Digital interoperability for growing the Department of Defense (DoD) digital ecosystem is paramount in remaining ahead of our adversaries. When beginning a program, plan for the use of digital intelligence products. This enables direct incorporation into the program workflow and speeds up ingestion and reaction time to emerging threats. There is a growing list of digital intelligence products that can feed and improve a program's development, analysis of alternatives, testing, Critical Intelligence Parameter (CIP) breach reporting, and dependencies on manpower-intensive processing. For more on digital implementation, see Appendix 4.

2.3 Tailored/Dynamic Intelligence Reporting

Acquisition intelligence professionals provide tailored threat intelligence products for those programs for which there is no timely, standardized threat reporting from the Intelligence Community. Production Requests (PRs) for intelligence support and associated resources such as the Validated Online Lifecycle Threat (VOLT) repository Technology Targeting Risk Assessments (TTRAs), and threat models should] be tasked for programs having statutory or regulatory requirements (note that regulatory requirements for these IC products may be waived by an acquisition decision memorandum). Programs lacking statutory or regulatory requirements for such products should also obtain program-specific threat support tailored to integrate directly into program office decision processes. These intelligence products will adhere to the analysis standards delineated in Intelligence Community Directive (ICD) 203, Analytic Standards, ICD 206 Sourcing Requirements for Disseminated Analytic. While some of these products are produced by the Defense Intelligence Enterprise (DIE), others may be produced from open source, publicly available information or even academia. Some example reports are covered in Section 4, Table 2.

2.4 Integrated Intelligence Reporting Archives

Acquisition intelligence professionals should ensure reports are shared across programs and with counterparts throughout the Intelligence Community (in accordance with need to know, classification, and handling controls) through analytic interchanges and formal feedback. Sharing threat assessments helps inform the task-saturated DIE and other programs with similar threats. The Defense Intelligence Threat Library (DITL) on Joint Worldwide Intelligence Communications System (JWICS) and Secure Internet Protocol Router Network (SIPRNet) provides a single location were all foundational acquisition intelligence products (Threat Modules), program-specific repositories (VOLTs), and CIPs are hosted to increase discoverability and prevent the formation of discrete information silos within the intelligence community. Acquisitions intelligence professionals can also share threat assessments via SIPRNet, JWICS, and within collaboration forums like R-Space and iSPACE. Wherever possible, intelligence reporting should include XML data tagging of the contents in preparation for use in future digital intelligence capabilities across the Services. Using ICD standards to build tailored products sharpens the entire intelligence 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 professionals 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 208: *Write for Maximum Utility*: Establishes fundamental intelligence production principles and a common perspective from which to plan, organize, write, and disseminate intelligence products that provide the greatest use to customers.

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.

ICD 710: *Classification Management and Control Markings System:* Governs the implementation and oversight of the IC classification management and control markings system, which provides the framework for accessing, classifying, disseminating, and declassifying intelligence and intelligence related information to protect sources, methods, and activities.

3.0 THREAT REPORTING AND INTELLIGENCE SUPPORTABILITY

Acquisition intelligence professionals form a critical partnership between the acquisition and intelligence communities. The two fundamental mission areas for acquisition intelligence professionals are: 1) to inform PMs of threats to their systems; 2) document the intelligence supportability requirements over the entire life cycle of the system; and 3) track fulfillment of intelligence supportability requirements.

3.1 Threat

As defined by DoDI 5000.86, a threat is defined as “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.” Threat resources and reports that assist acquisition intelligence professionals in support of their PMs include Threat Modules, VOLTs, CIPs/Cyber CIPs, TTRAs, the Threat System Database (TSDB), the Army’s Threat Test Support Packages (TTSP), the Air Force’s Adversary Cyber Threat Assessments (ACTA), a variety of modeling and simulation (M&S) products, and their own organically produced tailored intelligence products. Threat Steering Groups (TSG’s, sometimes also called VOLT TSG’s) should also be used to help determine relevant threats and validate them for analysis as they relate to the particular acquisition program.

NOTE: As additional best practices are created, owners are encouraged to share developments with OUSD/A&S/AI2/AID so they can be disseminated across the entire workforce and integrated into Defense Acquisition University acquisition intelligence training modules.

3.2 Intelligence Supportability

Intelligence supportability includes reviewing a program's intel-driven DOTMLPF-P (i.e., Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy). It is vital to assess and document program requirements as soon as possible so the IC is prepared to provide the necessary support intelligence before a system is fielded. A new system/capability may require increased Intelligence Mission Data (IMD) or processing capability; an increase in the number of intelligence professionals 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 (e.g., fuel, storage, parts, power, etc.), each program should document the intelligence supportability requirements needed to operate so the IC can prioritize resources to support them. A Service specific example is the USAF's Intelligence Health Assessment (IHA) report used to summarize a program's intelligence supportability requirements and identify any personnel gaps that could impact a program's Initial Operating Capability. PMs use lifecycle mission data planning to capture IMD needs, threat models and a Lifecycle Mission Data Plan (LMDP) to identify new data requirements (see Section 4.5).

4.0 INTELLIGENCE SUPPORT TO THE ADAPTIVE ACQUISITION FRAMEWORK (AAF) PATHWAYS

4.1 Major Capability Acquisition (MCA)

4.1.1 Key Points

- ***Overview:*** *The MCA pathway is typically limited to Acquisition Category (ACAT) I-III programs and intelligence support largely mirrors legacy acquisition programs including formal intelligence products such as a VOLT or TTRA.*
- ***Threat analysis:*** *VOLT is required for ACAT 1D programs unless waived by MDA or Director, Operational Test and Evaluation (DOT&E) (if program is on the DOT&E Oversight List). TTRA is required for milestone A.*
- ***Intelligence supportability:*** *Life cycle mission planning is necessary if a system is dependent on IMD; acquisition intelligence professionals should work with PM to determine if an LMDP is needed and aid in its development.*

Intelligence support to MCA programs, which can include Major Defense Acquisition Programs (MDAPs) and programs designated as ACAT I-III, begins in the planning phase, and continues throughout the entire acquisition process (DoDI 5000.85). This support can be categorized as either threat assessments or intelligence supportability assessments (ISAs). The methodology will include full featured threat assessments to inform requirements and analysis of alternatives (AoA); comprehensive ISAs to inform AoA; and continued updates prior to milestone decision points (including Request for Proposal [RFP]

release, Preliminary Design Review, Critical Design Review, etc.) (

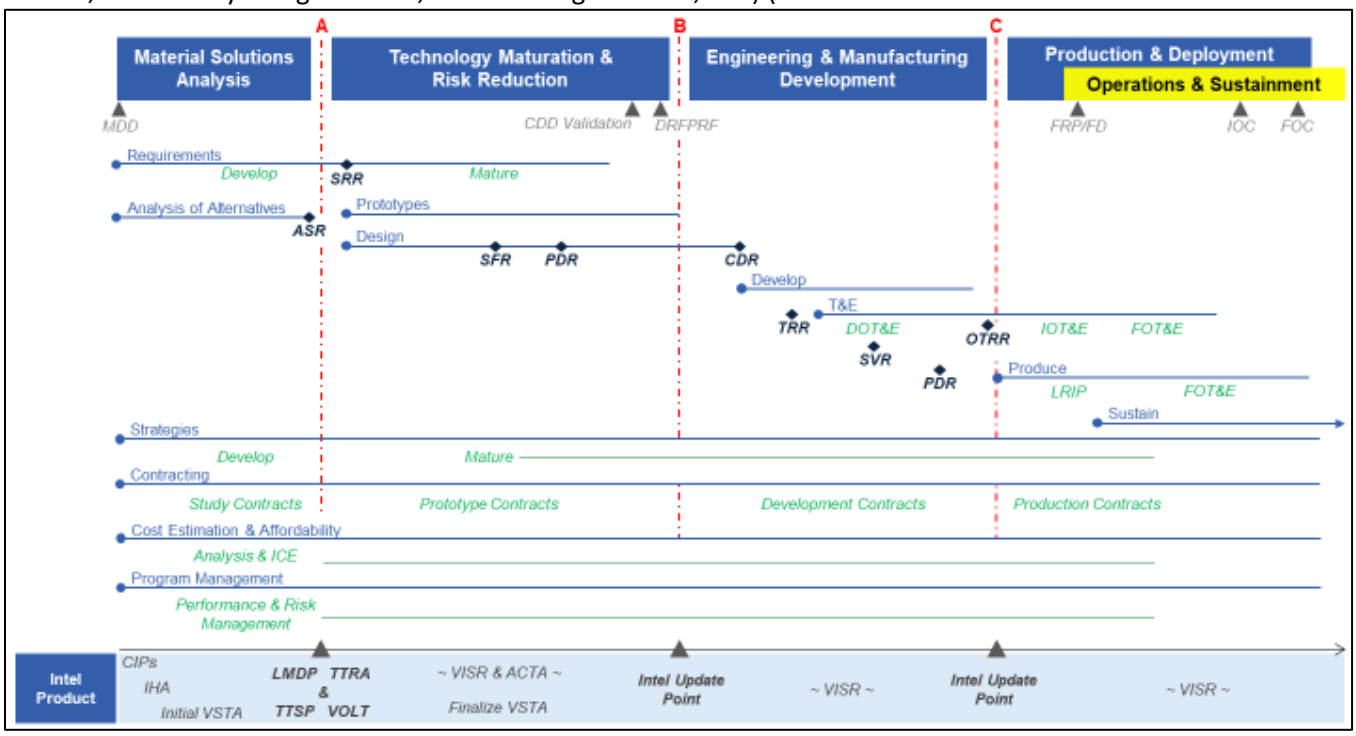


Figure 1 and https://aaf.dau.edu/aaf/mca/). For an MCA program, the threat assessment repositories and products may include a VOLT, TTRA or continuously produced, organically tailored threat products.

4.1.2 Threat Analysis

MDAPs and programs on the DOT&E Oversight List require a unique system-specific VOLT to support capability development and PM assessments of mission needs and capability gaps. Based on DITL Threat Modules, VOLTs provide the PM with technology projections and adversary capability trends for the next 10-20 years. DIA validates VOLTs for ACAT ID programs, while DoD Components produce and validate VOLTs for ACAT IB/C programs and below. Although most MCA programs require VOLTs, this requirement can be waived by the MDA (and the Director, DOT&E if the program is on the DOT&E Oversight List). Program offices that choose to waive the VOLT should collaborate with the IC to tailor organic threat analysis to meet the program office's current and future threat demands.

In accordance with the JCIDS process, the requirements sponsor, and Component capability developer will jointly develop CIPs (including Cyber CIPs) to inform S&T investments and program upgrades.

The second component of the MCA threat assessment, the TTRA, forms the analytic foundation for counterintelligence assessments in the associated Program Protection Plan (PPP). It is prepared by the DoD Component and coordinated with the DoD Component intelligence analytical centers per DoDI O-5240.24. DIA validates the report for ACAT ID programs; the DoD Component is the validation authority for ACAT IB/C and below. TTRAs are required only for milestone A (Table 2).

4.1.3 Intelligence Supportability

Life cycle mission data planning is only required if the system is dependent on IMD. It is the acquisition strategy and the systems engineering plan that define how the capability will use intelligence data

required to operate the system. Gaps in IMD diminish the capabilities of systems and can expose vulnerabilities. Acquisition intelligence professionals help PMs determine if they need an LMDP plan and assist in new data development. They also aid program entry into the DoD requirements prioritization and production planning processes for Electronic Warfare Integrated Reprogramming (EWIR), Signatures, Characteristics and Performance (C&P), Order of Battle, Geospatial Intelligence (GEOINT) products, and threat models. A valuable resource in this process is the Acquisition Intelligence Requirements Enterprise System (AIRES) for which more information can be found in Appendix 2.

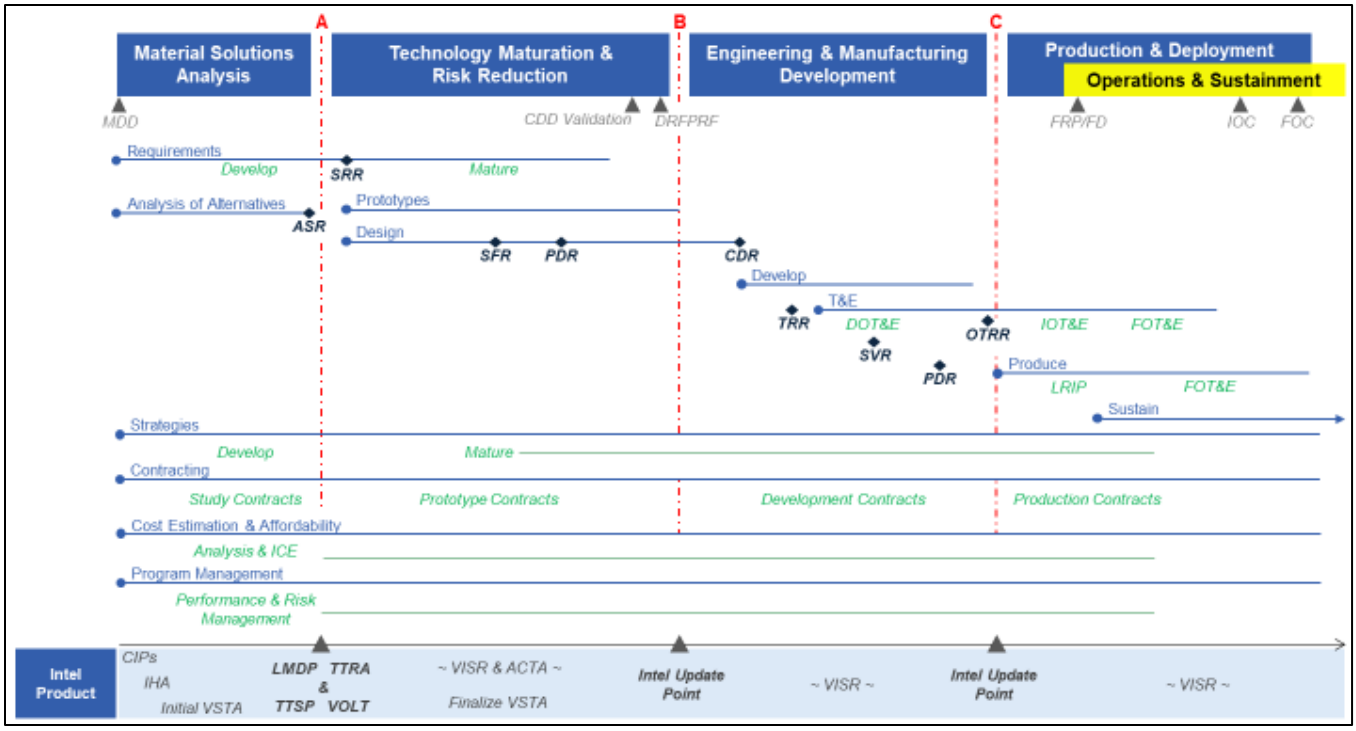


Figure 1: MCA Pathway Intelligence Integration Roadmap.

Table 2. MCA Milestone and Phase Information Requirements[1]

INFORMATION REQUIREMENT	PROGRAM TYPE1			LIFE-CYCLE EVENT1,2,3								SOURCE	TYPE	APPROVAL AUTHORITY
	MDAP	ACAT II	ACAT ≤ III	MDD	MS A	CDD Val	Dev RFP Rel	MS B5	MS C	FRP Dec	OTHER			
Life-Cycle Mission Data Plan	•	•	•		•		✓	✓	✓	✓		This table	Regulatory	DoD Component
Regulatory; only required if the system is dependent on Intelligence Mission Data. A draft[4] update is due for Development RFP Release; approved at Milestone B.														
Technology Targeting Risk Assessment	•	•	•		•							This Table; DIA Directive 5000.200; DIA Instruction 5000.002	Regulatory	Validation by DIA or DoD Component
Regulatory. Prepared by the DoD Component and coordinated with the DoD Component intelligence analytical centers per DoDI O-5240.24. Forms the analytic foundation for counterintelligence assessments in the associated PPP. DIA will validate the report for ACAT ID; the DoD Component will be the validation authority for ACAT IB and IC and below.														
Validated On-line Life-cycle Threat (VOLT) Report	•	•	•	•	✓		✓		✓	✓		This Table; DIA Directive 5000.200; DIA Instruction 5000.002	Regulatory	DIA or DoD Component
Regulatory. MDAPs require a unique system-specific VOLT report to support capability development and PM assessments of mission needs and capability gaps against likely threat capabilities at IOC. The VOLT report uses the bi-annual Defense Intelligence Threat Library Threat Modules as its analytic foundation. The threat modules provide the PM projections of technology and adversary capability trends for the next 20 years. VOLT reports are required for all other programs unless waived by the MDA. In conjunction with the VOLT, the requirements sponsor and Component capability developer will collaboratively develop critical intelligence parameters in accordance with the JCIDS. Programs on the DOT&E Oversight List require a unique, system-specific VOLT, unless waived by both the MDA and the DOT&E. DoD Components produce a VOLT. DIA validates the VOLT for ACAT ID programs; the DoD Component validates the VOLT for ACAT IB and IC programs and below.														

4.2 Middle Tier Acquisition (MTA)

4.2.1 Key Points

- ***Overview:*** *The MTA pathway allows capabilities to be prototyped or fielded within five years. It may be used to accelerate capability maturation before transitioning to another acquisition pathway.*
- ***Threat analysis:*** *Given the reduced timeline, program offices should consider requesting a waiver for a VOLT and instead leveraging their organic intelligence support to tailor threat analysis in a form and on a schedule that best permits integration into program office decision processes. An initial threat analysis should be completed during the requirements phase. A supply chain risk assessment is recommended to identify and address any concerns with contractors under consideration conducted via the Service's established supply chain risk management process.*
- ***Intelligence supportability:*** *ISAs should be completed during the requirements phase and should be reviewed whenever there is a significant change in the mission-critical system requirements/capabilities and before full-rate production (if prototyping).*

The MTA pathway is intended to fill a gap in the DAS for those capabilities that have a level of maturity that allows them to be prototyped or fielded within five years (https://aaf.dau.edu/aaf/mta/). The MTA pathway may be used to accelerate capability maturation before transitioning to another acquisition pathway or may be used to minimally develop a capability before rapidly fielding (DoDI 5000.80). As with MCA programs, intelligence support to MTA programs is categorized as either threat assessments or ISAs. There is no specified ISA product.

Intelligence support to MTA programs must be flexible given the pathway's short timeline; therefore, the requirements generation phase is a critical injection point for threat and supportability. MTAs should leverage organic intelligence support and other DIE products as required. The MTA requirements generation lasts less than six months. In rapid prototyping, prototype development starts shortly after requirements development (Figure 3). In the rapid fielding path, production and fielding activities start immediately following requirements generation (Figure 4).

4.2.2 Threat Analysis

AID recommends that programs take advantage of the flexibility to determine how to satisfy the need for threat support by leveraging VOLTs. The emphasis should be on providing program-specific/tailored threat analysis in a format and on a schedule that best permits integration into program office decision processes.

AID recommends that programs take advantage of the flexibility of the MTA pathway to determine how to satisfy the need for threat support. The emphasis should be on providing program-specific/tailored threat analysis in a format and on a schedule that best permits integration into program office decision processes. A threat analysis should be completed during the requirements phase of both the rapid fielding and prototyping paths. In rapid prototyping, threat analyses should be reviewed yearly and whenever there is a significant change in the mission-critical system requirements or capabilities. In rapid fielding, threat analyses should be reviewed if there is a significant change in requirements or capabilities. Additionally, the requirements sponsor and Component capability developer will collaboratively develop CIPs in accordance with the JCIDS Manual. Intelligence professionals must use the Defense Intelligence Threat Library as a resource for researching existing CIPs.

4.2.3 Intelligence Supportability

A program's supporting acquisition intelligence professional can assist with identifying threat information and intelligence data needed to support rapid prototyping and fielding. In rapid prototyping, ISA should be reviewed before full-rate production and whenever there is a significant change in the mission-critical system requirements or capabilities. In rapid fielding, an ISA may only take place during the requirements phase but should be reviewed with any significant change in requirements or capabilities. The acquisition strategy should include guidance on integration of intelligence especially for intelligence data and support to T&E.

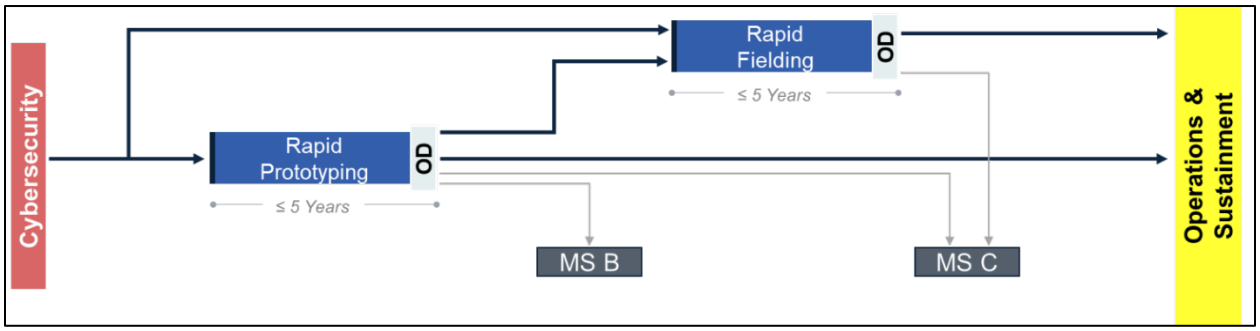
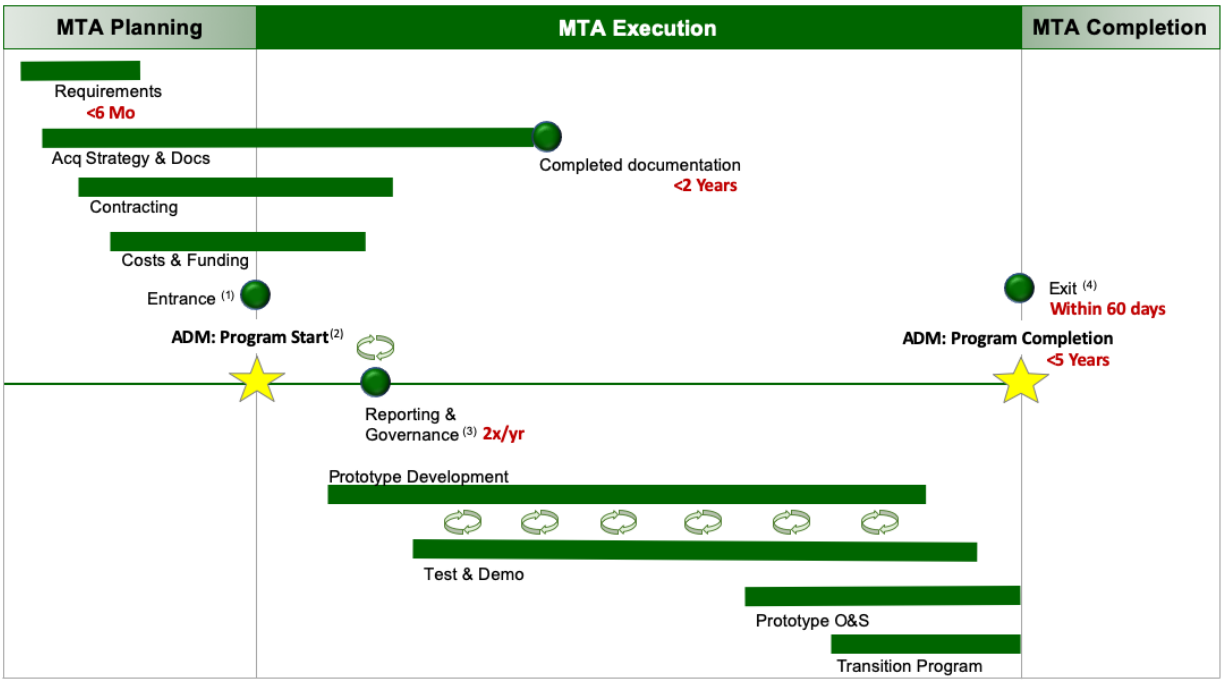
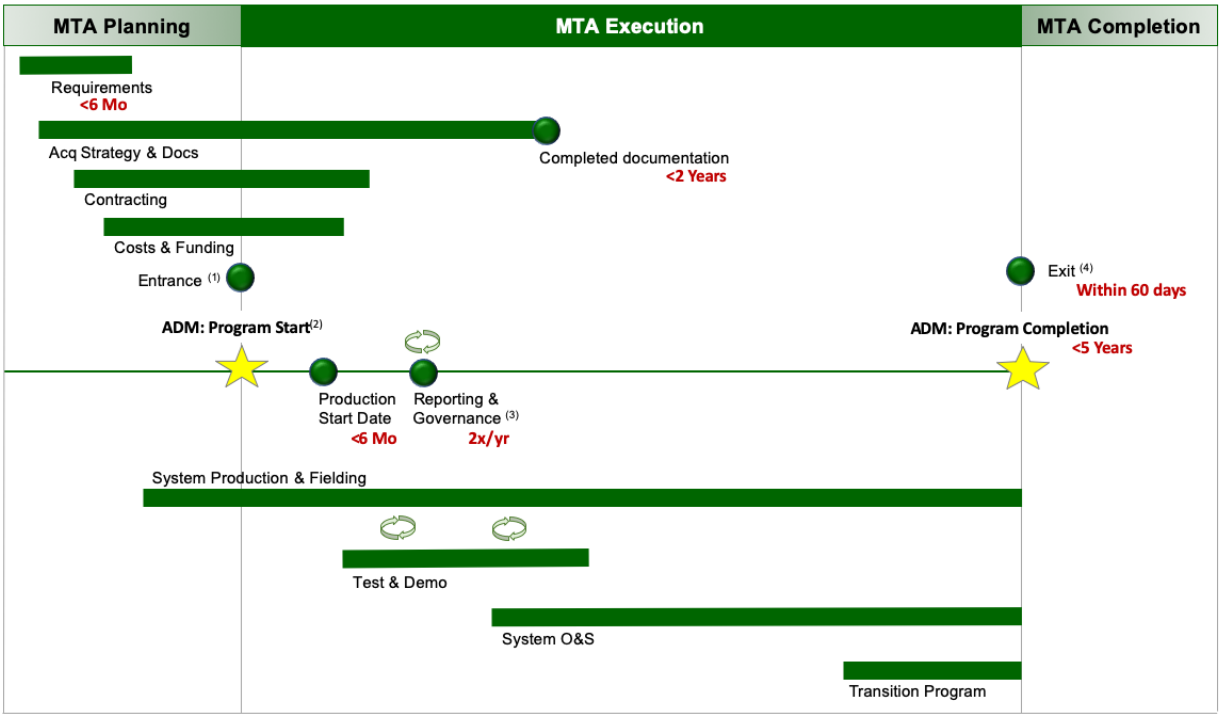


Figure 2: MCA Pathway Intelligence Integration Roadmap



(1) *Major Systems*: Acquisition Decision Memorandum(ADM) signed by the Decision Authority (DA), Acquisition Strategy (which includes [1] Security, Schedule & Production Risks; [2] Test Strategy/Results; and [3] Transition Plan), and Program Identification Data (PID)
Non-Major Systems: ADM signed by the DA, PID
(2) Major Defense Acquisition Programs (MDAPs) require Under Secretary of Defense for Acquisition & Sustainment (USD(A&S)) Prior Written Approval
(3) Updated PID submitted twice a year with President's Budget and Program Objective Memorandum submissions to Office of Secretary of Defense (OSD)
(4) Signed Outcome ADM, Final PID, Assessment of Test Results

Figure 3: Rapid Prototyping Path (DoDI 5000.80, paragraph 1.2.c)



(1) Major Systems: Acquisition Decision Memorandum(ADM) signed by the Decision Authority (DA), Acquisition Strategy (which includes [1] Security, Schedule & Production Risks; [2] Test Strategy/Results; and [3] Transition Plan), and Program Identification Data (PID)
Non-Major Systems: ADM signed by the DA, PID
(2) Major Defense Acquisition Programs (MDAPs) require Under Secretary of Defense for Acquisition & Sustainment (USD(A&S)) Prior Written Approval
(3) Updated PID submitted twice a year with President's Budget and Program Objective Memorandum submissions to Office of Secretary of Defense (OSD)
(4) Signed Outcome ADM, Final PID, Assessment of Test Results

Figure 4: Rapid Fielding Path (DoDI 5000.80, paragraph 1.2.d)

4.3 Urgent Capability Acquisition (UCA)

4.3.1 Key Points

- ***Overview:*** *Speed and flexibility is critical in meeting UCA timelines. Analysis of threats and intelligence data requirements must be completed in a matter of days or weeks and should be tailored to meet program needs in the most efficient manner possible.*
- ***Threat analysis:*** *With the PM and sponsor, intelligence professionals should quickly define and create an initial tailored threat assessment leveraging currently available intelligence information and sources throughout the IC to be used during the Pre-Development Phase that justifies the requirements. CIPs tied to the threat assumptions can be considered as well but may not be relevant early in the UCA lifecycle. A supply chain or vendor risk analysis can also be useful once selection of a source for acquisition/development is underway.*
- ***Intelligence supportability:*** *IMD requirements should be identified as early as possible (ideally during the Pre-Development and Development phases), to ensure intelligence information can be provided/produced on time. A thorough, tailored ISA should be created to ensure program needs will be met.*

The UCA pathway is designed to "provide warfighters with the capabilities urgently needed to overcome unforeseen threats, achieve mission success, and reduce risk of casualties…The acquisition; product support and sustainment processes; reviews; and documents are aggressively streamlined due to

operational urgency." (DoDI 5000.02, Section 4.2.a(2)). Figure 5 (below) illustrates the UCA pathway (https://aaf.dau.edu/aaf/uca/).

Figure 5: Life Cycle View of the Urgent Capability Acquisition Pathway

Speed is critical in meeting urgent operational needs, and the acquisition intelligence support to the program must match that urgency. DoD Component Heads are directed to "tailor and streamline program strategies and oversight of urgent capability acquisitions, as appropriate" (DoDI 5000.81, Section 2.7.a). During the Pre-Development Phase, program managers construct a tailored acquisition strategy that "should be brief and contain only essential information, such as resourcing needs and sources; key deliverables; performance parameters; key risks and mitigation approaches" (DoDI 5000.81, Section 4.2.c (4)(d)). Based on this guidance, analysis of threats and intelligence data requirements should be tailored to meet program timelines in the most efficient manner possible.

4.3.2 Threat Analysis

According to 5000.81, the Office of the Undersecretary of Defense for Intelligence and Security (OUSD(I&S)) "[a]dvises the Components on security, counterintelligence, and intelligence matters associated with their Urgent Capability Acquisition programs and works with them to assess threats and address vulnerabilities" (DoDI 5000.81, Section 2.5.b). This authority may be delegated to the program level and the assigned intelligence analyst in conjunction with the PM, should quickly define and create an initial tailored threat assessment that can be used during the Pre-Development Phase. UCA programs need to accomplish this analysis in a matter of days or weeks, not months or years. Acquisition intelligence professionals should take full advantage of currently available intelligence information, and leverage sources throughout the IC if necessary.

Periodic threat updates may not be able to affect the acquisition of the UCA once the Production and Deployment Phase starts, so any changes to the threat must be identified during the Development Phase at the latest. CIPs can be considered as well but may not be relevant early in the UCA life cycle. A supply chain or vendor risk analysis can also be useful once selection of a source for acquisition/development is underway.

4.3.3 Intelligence Supportability

UCA pathway programs should identify any IMD requirements as early as possible, ideally during the Pre-Development and Development Phases, to ensure intelligence information can be provided/produced with the appropriate speed for program success. A thorough, tailored intelligence supportability assessment should be created to satisfy PMs that their needs will be met.

Figure 6 (below) presents suggested timing of the various applicable intelligence products for the UCA pathway, providing maximum flexibility to program managers.

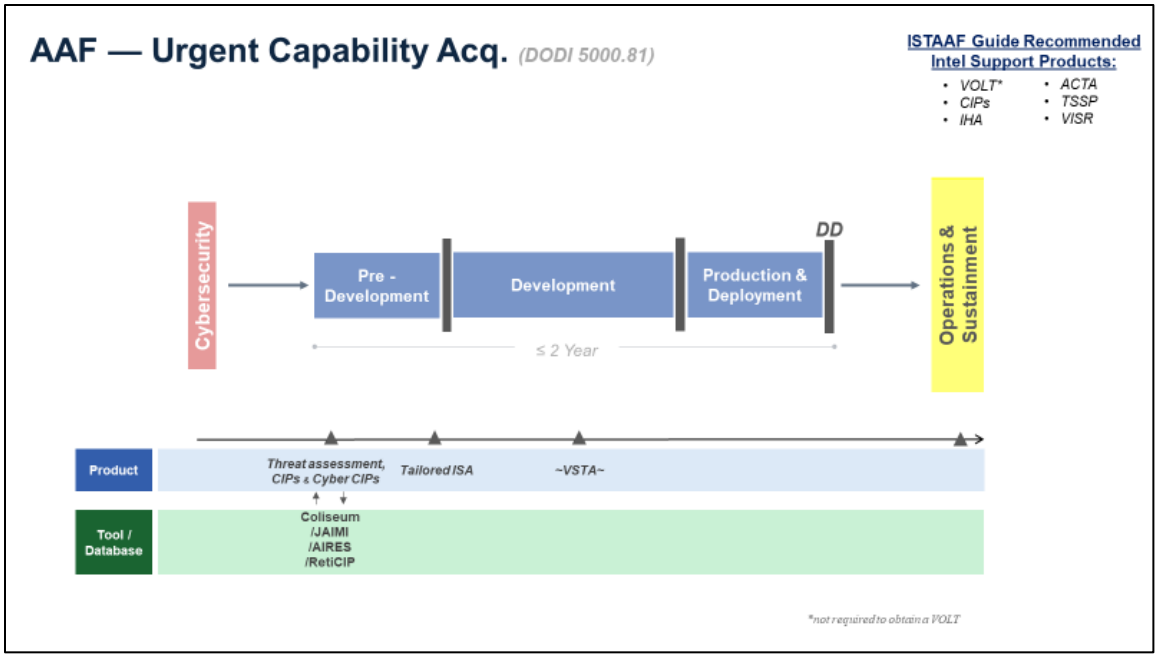


Figure 6: Urgent Capability Acquisition Pathway Intelligence Integration Roadmap

4.4 Software Acquisition

4.4.1 Key Points

- ***Overview:*** *The Software Acquisition Pathway is intended to support the rapid and iterative development/sustainment processes of software programs. Timing of intelligence products should be considered extremely flexible and match the delivery cadence of the SW development process.*
- ***Threat analysis:*** *A threat assessment is not required but is recommended for software programs. Acquisition intelligence professionals should partner with PMs to identify the best format and frequency of the initial assessment and following updates to be approved by the decision authority. If requested, CIPs should be completed during the Planning Phase, and be reviewed regularly. A supply chain risk assessment is recommended to identify and address any concerns with contractors under consideration conducted via the Service's established supply chain risk management process. Specific considerations for a program's cyber resiliency should also be addressed.*
- ***Intelligence supportability:*** *A threat assessment is not required, but a detailed assessment of the program's potential intelligence and IMD requirements should be conducted during the Planning Phase taking care to consider the required volume and frequency once fielded. This can help address some of the Risk Management Framework (RMF) process requirements that an Authorization Official would need to issue an Authority to Operate. A tailored ISA can be created to specify data types and delivery timelines and submit the appropriate requests to the IC organizations responsible for production.*

The Software Acquisition Pathway (SWP) provides program managers a highly tailorable process for "the timely acquisition of custom software capabilities developed for the DoD" (DoDI 5000.87, Section 1.2 (b,c,d)). Programs using this pathway are not subject to JCIDS requirements and are not treated as MDAPs. Balancing acquisition speed with rigor results in no formal milestones for the SWP and allows

intelligence professionals to similarly tailor their efforts to meet the rapid, iterative development process of the SWP (with the approval of the program decision authority). According to DoDI 5000.87, "a risk-based management approach will be an integral part of the program's strategies, processes, designs, infrastructure, development, test, integration, delivery, and operations, … [and will] identify and address risks and execute mitigation actions" (Section 1.2 (i)). Effective threat assessment and analysis of intelligence supportability are key elements to properly addressing program risks and requirements.

Timing of intelligence products, without milestones in the SWP, should be considered extremely flexible and match the delivery cadence of the software development process (https://aaf.dau.edu/aaf/software/). An initial threat assessment should be performed during the Planning Phase and updated at a frequency determined by the PM and their assigned intelligence analyst. Intelligence supportability for the program should also be assessed during the Planning Phase so intelligence data requirements can be documented and assigned to the appropriate production organizations. Not all software acquisition programs will have intelligence data needs, so this may be optional if the decision authority concurs with the determination. For reference, Figure 7 describes the Life Cycle View of the Software Acquisition Pathway.

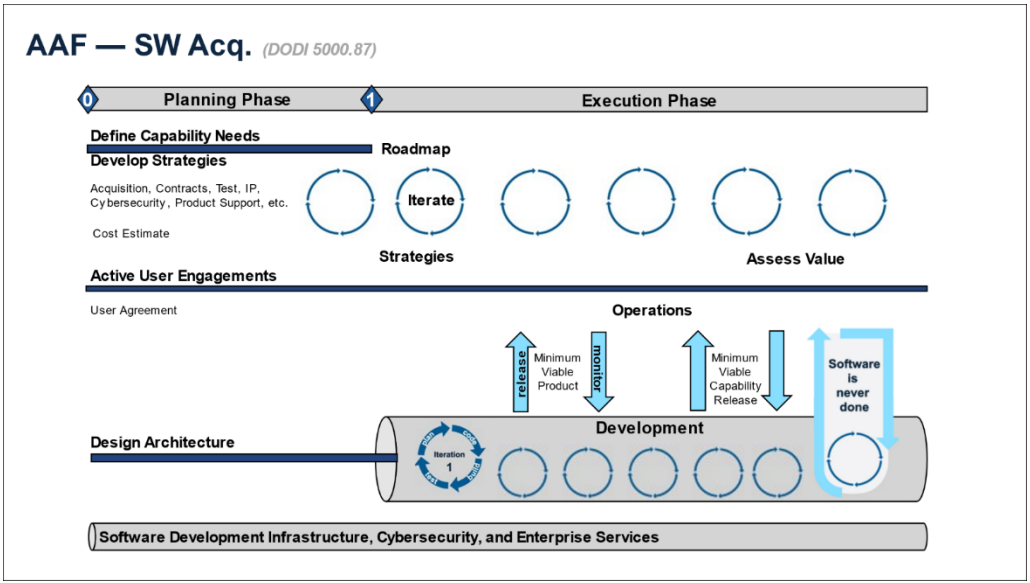


Figure 7: Life Cycle View of Software Acquisition Pathway

4.4.2 Threat Analysis

In accordance with 5000.87, Section 3.3.b (9)(c), programs using the SWP are required to conduct "secure lifecycle management." A tailored threat assessment is the recommended product that will best support SWP programs (a VOLT is not required). The format and frequency of the initial assessment and following updates should be determined as agreed upon by the PM and their acquisition intelligence analyst and approved by the decision authority. Establishing CIPs/Cyber CIPs, if requested, should also be accomplished during the Planning Phase, and should be reviewed on a regular basis. Other intelligence products may be useful for SWP programs, such as the Air Force's ACTA, or a similar evaluation. A TTRA or IHA may also be used to address the threat assessment needs of the program, though they are not required.

4.4.3 Intelligence Supportability

Intelligence data needs and ongoing supportability should be evaluated during the Planning Phase for SWP programs. A detailed assessment of the program's potential intelligence supportability or IMD requirements should be conducted to ensure mission success. A tailored ISA can be created to specify data types and delivery timelines and submit the appropriate requests to the IC organizations responsible for production. Many software programs underestimate the volume or frequency of required updates to their IMD, leading to data delivery challenges once the software is fielded; it is essential that a comprehensive data plan is in place early in the program's life cycle.

Figure 8 (below) presents suggested timing of the various applicable intelligence products and can be modified to best fit a program's needs.

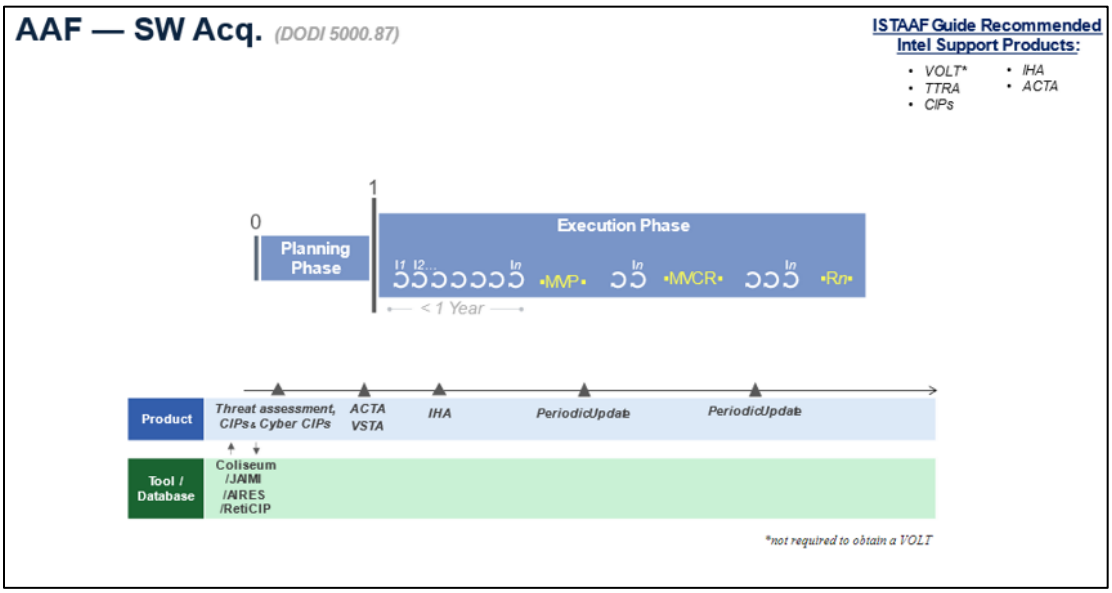


Figure 8: Software Pathway Intelligence Integration Roadmap

4.5 Defense Business Systems (DBS)

4.5.1 Key Points

- ***Overview:*** *The Defense Business Systems Acquisition Pathway strongly emphasizes pursuing existing commercial or government solutions for rapid fielding of capabilities. Acquisition intelligence support is an important part of risk reduction especially in the analysis and planning phases.*
- ***Threat analysis:*** *Tailored threat assessment scope, format, and timing should be agreed upon by the PM and intelligence analyst considering the system's intended use and type of information it needs. Ideally, the assessment will be prepared and reviewed prior to system acquisition. As business systems tend to be software focused, PMs should consider thorough cyber threat analysis as part of the assessment.*
- ***Intelligence supportability:*** *Although the system being acquired is already fully developed, PMs should consider a tailored intelligence supportability analysis to identify any potential IMD needs.*

The intent is to ensure that intelligence data can be provided by the IC and produced with the required cadence.

The DBS pathway is used to "acquire information systems that support DoD business operations" (DoDI 5000.02, Section 4.2.e (1)). This pathway "may also be used to acquire non-developmental, software intensive programs that are not business systems" (DoDI 5000.02, Section 4.2.e (1)(b)). By pursuing existing commercial and government solutions that require minimal customization, the DoD can implement the systems quickly to achieve successful mission outcomes. Part of the risk reduction effort during the acquisition process should include tailored acquisition intelligence assessments, executed during the Solution Analysis or Functional Requirements and Acquisition Planning phases. Figure 9 below illustrates the DBS Pathway (https://aaf.dau.edu/aaf/dbs/).

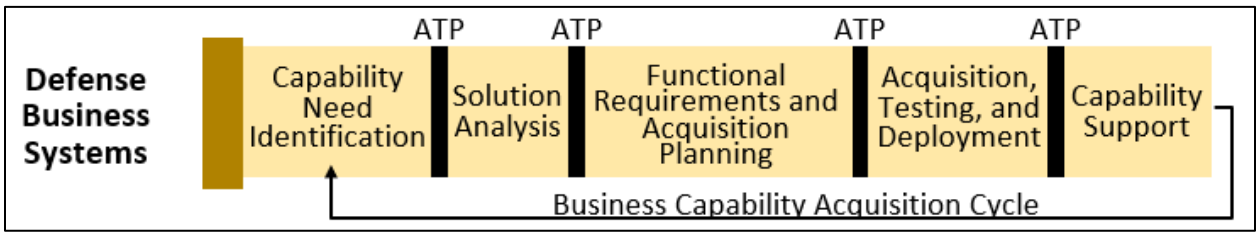


Figure 9: Life Cycle View of the Defense Business Systems Pathway

According to DoDI 5000.75, Section 4.1.a (1), "tailoring should be considered throughout the life cycle from both the functional and acquisition perspective, to include program strategies and oversight, program information, acquisition phase content, and the timing and scope of decision reviews and decision levels." This includes consideration of risk factors, allowing PMs to shape their intelligence threat analysis and supportability requirements.

4.5.2 Threat Analysis

The timing of an initial tailored threat analysis should be discussed and agreed upon by the PM and their assigned acquisition intelligence professional. Ideally, the assessment will be prepared and reviewed prior to the acquisition/purchase of the business system being considered (before entering the Acquisition, Testing, and Deployment phase), so that any threats identified can be properly understood and mitigated. The scope of the assessment may vary widely, depending on what the system's intended use may be, and what types of information it may require. Creation of CIPs should also be considered at this point, as well as a supply chain risk assessment. DoD business systems tend to be software-centric programs; therefore, PMs may want to conduct a more thorough cyber threat analysis in addition to their general threat assessment. Updates to any of the threat products can be conducted during the Capability Support phase to ensure the ongoing security of the business system in use.

4.5.3 Intelligence Supportability

DBS pathway programs should also conduct a tailored intelligence supportability analysis to identify any potential IMD needs, even though the system being acquired is already fully developed. This analysis can be conducted during the same phases as the threat assessment, to ensure that intelligence data can be provided/produced with the required cadence as described in the acquisition plan. The intent is to prevent acquisition of a system that needs data that the IC can't provide. Figure 10 (below) presents suggested timing of the various applicable intelligence products for the DBS pathway, providing tailored flexibility to program managers.

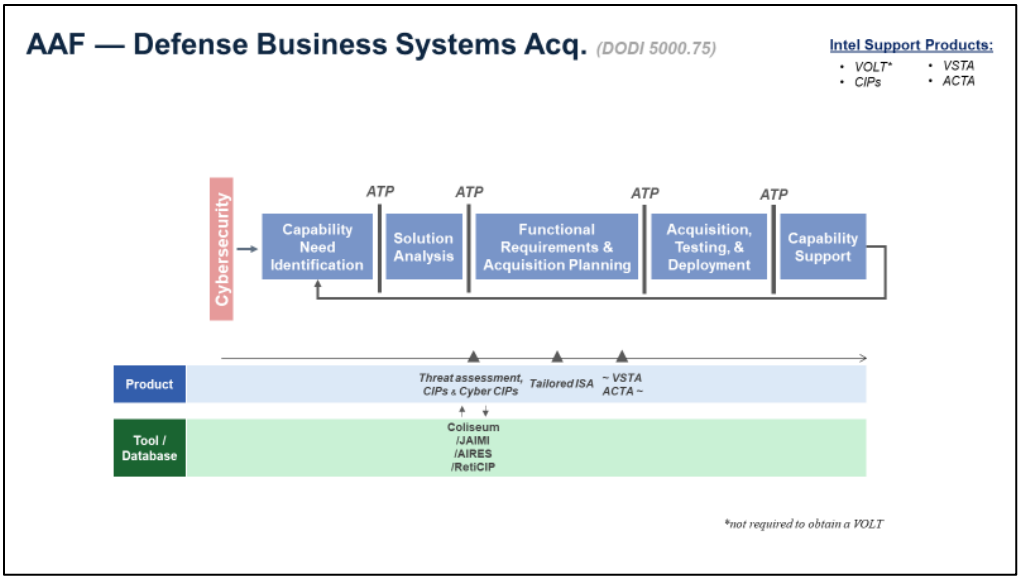


Figure 10: Defense Business Systems Pathway Intelligence Integration Roadmap

4.6 Acquisition of Services

4.6.1 Key Points

- ***Overview:*** *The Acquisition of Services (or Services Acquisition [SA]) pathway covers a wide range of services including construction, transportation, research and development, and logistics. Acquisition intelligence support is less defined than other pathways and requirements are addressed by OUSD(I&S) in coordination with OUSD(A&S).*
- ***Threat analysis:*** *Risk management responsibility is assigned to the Functional Services Manager (FSM) who can determine the appropriate threat assessment approach for their program in conjunction with their intelligence analyst. A supply chain risk assessment is recommended to identify and address any concerns with contractors under consideration conducted via the Service's established supply chain risk management process.*
- ***Intelligence supportability:*** *It is unlikely that an SA program has IMD requirements. If necessary, a tailored intelligence supportability analysis can be performed, prior to Phase 6 "Execute Strategy."*

The SA pathway "is intended to identify the required services, research the potential contractors, contract for the services, and manage performance" (https://aaf.dau.edu/aaf/services/). These services can cover a wide range of capabilities "including knowledge-based, construction, electronics and communications, equipment, facilities, product support, logistics, medical, research and development, and transportation services" (DoDI 5000.02, Section 4.2.f (1)). Figure 11 (below) illustrates phases of the SA pathway.

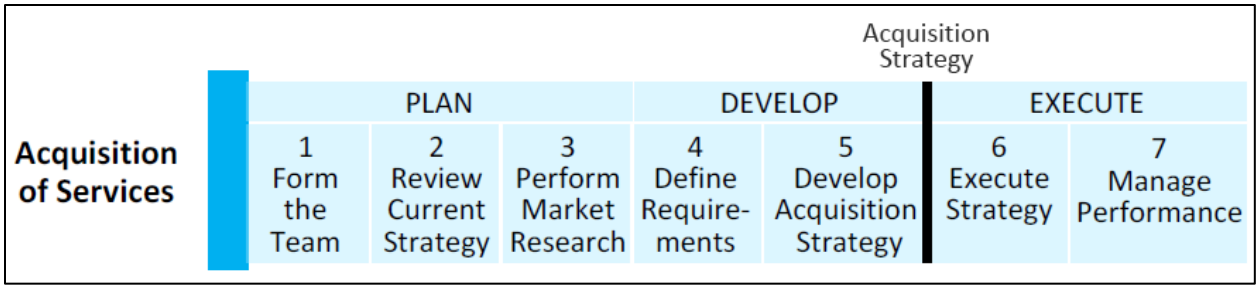


Figure 11: Life Cycle View of the Services Acquisition Pathway

OUSD (I&S) "coordinates with OUSD(A&S) to ensure that security implications are addressed throughout the acquisition of services process in accordance with DoD security policy" (DoDI 5000.74, Section 2.6). Additionally, risk management responsibility is assigned to the FSM as described in DoDI 5000.74, Sections 3.4.b (4) and 3.4.d.

4.6.2 Threat Analysis

Using streamlined documentation for the Services Acquisition Strategy (DoDI 5000.74, Section 4.4.c), the FSM can determine the appropriate threat assessment approach for their program in conjunction with their intelligence analyst. A tailored threat assessment may not be necessary for most services acquisitions, but a supply chain risk assessment is recommended to identify and address any concerns with contractors under consideration for the program. Any assessments should be completed prior to Phase 6 "Execute Strategy" and can begin as early as Phase 2 "Review Current Strategy" (since this is when program risk identification starts for the SA pathway).

4.6.3 Intelligence Supportability

It is unlikely that there will be IMD requirements for an SA program, but this should be considered by the FSM to ensure there aren't any intelligence data needs. If necessary, a tailored intelligence supportability analysis can be performed, prior to Phase 6 "Execute Strategy." Figure 12 (below) presents suggested timing of the applicable intelligence products for the SA pathway.

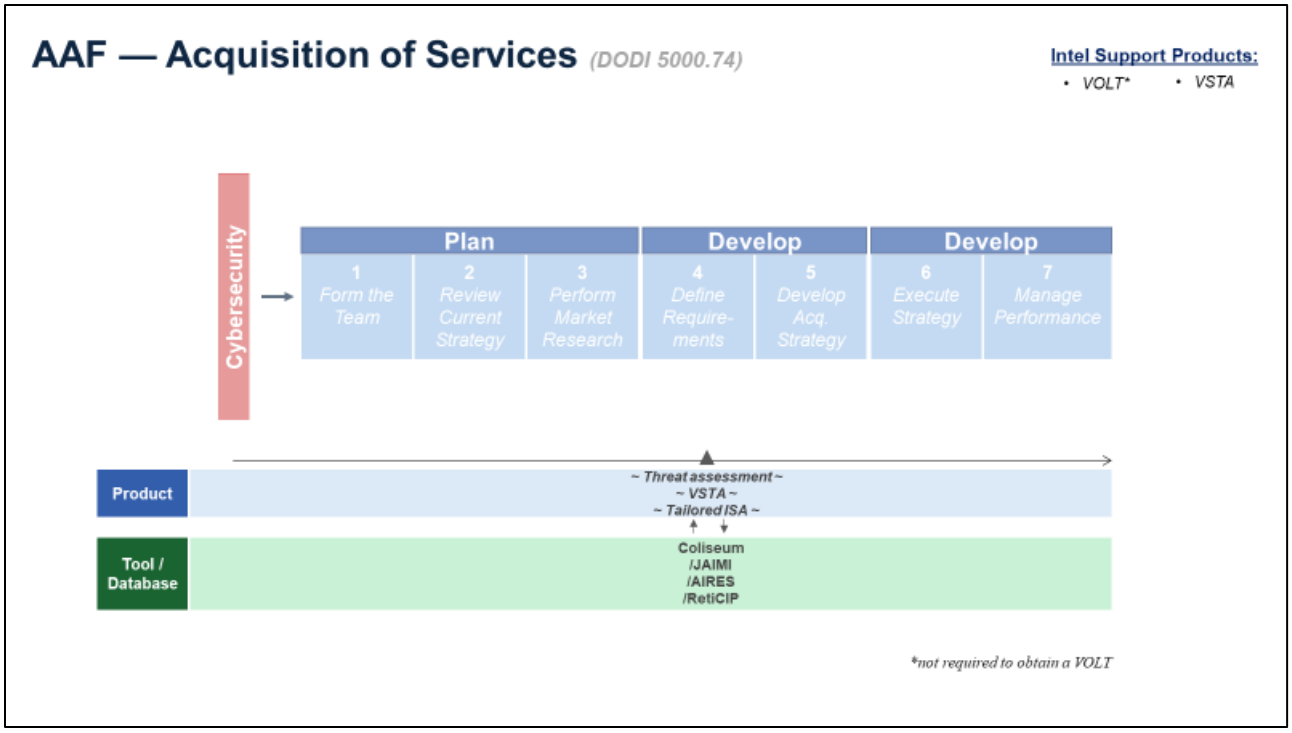


Figure 12: Services Acquisition Pathway Intelligence Integration Roadmap

5.0 INTELLIGENCE SUPPORT PROCESS OVERVIEW

The AAF supports the DAS with the objective of delivering effective, suitable, survivable, sustainable, and affordable solutions to the end user in a timely manner. To achieve those objectives, MDAs, other Decision Authorities (DAs), and PMs have broad authority to plan and manage their programs consistent with sound business practice. The AAF acquisition pathways provide opportunities for MDAs/DAs and PMs to develop acquisition strategies and employ acquisition processes that match the characteristics of the capability being acquired (DoDI 5000.02, Section 1.3).

As the AAF's intent is to provide a more tailorable and process-oriented approach to acquisition, intelligence support to the AAF should be similarly adaptive. Instead of focusing on delivering specific products throughout the acquisition life cycle, acquisition intelligence activities should instead focus on the intent of a program's intelligence requirements, threat information, and intelligence data.

The products described in this guide can be valuable; however, the value is not in product delivery completion but in the information that it provides. It is, therefore, important that program managers and acquisition intelligence professionals understand the type and fidelity of information needed at different points throughout the acquisition life cycle rather than just the product delivery schedule.

This guide captures Service best practices with respect to satisfying the intent of the need for intelligence. At a high level, this is divided into two areas: threat information and intelligence supportability. Threat information can include the identification and capabilities of adversaries. Intelligence supportability information helps determine the intelligence requirements necessary to support an acquisition program. This section outlines the information needed in each AAF pathway and methods for tailoring products to satisfy the requirements.

Table 3: Acquisition Intelligence Information Matrix

AAF PATHWAY	GENERAL THREAT ASSESSMENT	INTELLIGENCE DEPENDENCY ANALYSIS	TECHNOLOGY RISK ASSESSMENT*	INTELLIGENCE HEALTH ASSESSMENT *(USAF)*	CYBER THREAT ANALYSIS	SUPPLY CHAIN RISK ASSESSMENT	CRITICAL INTELLIGENCE PARAMETERS
Urgent Capability Acquisition	Tailored Product	Tailored Product				Vendor Susceptibility to Targeting Assessment (VSTA, *USAF*), Supply Chain Threat Assessment (SCTA), or similar	CIPs
Middle Tier Acquisition	VOLT/ Tailored Product	Tailored Product	Tailored Product	IHA *(USAF)*	Tailored Product	VSTA *(USAF)*, SCTA, or similar	CIPs
Major Capability Acquisition	VOLT/ Tailored Product	LMDP, ISA	TTRA *(Army)*	IHA *(USAF)*	ACTA *(USAF)*	VSTA *(USAF)*, SCTA, or similar	CIPs
Software Acquisition	Tailored Product	Tailored Product	Tailored Product	IHA *(USAF)*	Tailored Product	VSTA *(USAF)*, SCTA, or similar	CIPs
Defense Business Systems					Tailored Product	VSTA *(USAF)*, SCTA , or similar	
Acquisition of Services						VSTA *(USAF)*, SCTA, or similar	

**not to be confused with TTRA*

6.0 ACQUISITION INTELLIGENCE BEST PRACTICES

The AAF drives more acquisition flexibility for programs 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 to enhance national security. The AAF helps PMs respond to the Acquisition Agility Act of Fiscal Year (FY) 2017 (part of the National Defense Authorization Act of FY2017) and the focus on a more "agile" 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.

Acquisition intelligence support to agile acquisition is predicated on clear and thorough communication within the PMO. Acquisition intelligence professionals 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 acquisition intelligence professionals ensure responsive threat reporting throughout the acquisition life cycle.

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 from to find the best fit for their program's

acquisition type. The acquisition intelligence analyst should work with the PM to identify which threat products are most beneficial to their program.

Another best practice is the use of Threat Steering Groups (TSGs). TSGs are essential for assessing intelligence threats, as they coordinate and validate intelligence support requirements. Comprised of cross-community experts, TSGs ensure timely and consistent support for capability development initiatives. Threat reporting, whether via VOLT or other tailored intelligence products, all benefit from well executed TSGs.

NOTE: The VOLT is required for Major Capability Acquisitions and programs on the Director Operational Test & Oversight (DOT&E) oversight list unless waived by the MDA. These products may be valuable to Middle Tier and Urgent Capability Pathways if the DIE is able to produce one. If a non ACAT 1D program needs intelligence support, the acquisition intelligence professionals should leverage existing DIE products, create their own tailored intelligence products, and/or collaborate with IC subject matter experts to ensure the program office is threat informed. If intelligence doesn't exist or is not at a fidelity a program office can use, an AIA should request intelligence support through a production requirement via COLISEUM.

PMs should partner with their acquisition intelligence professionals early in the acquisition life cycle. Involving them in key meetings and getting their input throughout the process can inform decision making and improve the outcomes. Acquisition intelligence professionals should proactively research the available tools and reports. They should also study the programs and identify likely threats while engaging with the PM, CE, Test and Evaluation (T&E), users, and other stakeholders.

COORDINATION WITH COUNTERINTELLIGENCE

The ISTAAF Guide focuses on intelligence, but intelligence and counterintelligence work hand-in-hand to support program manager needs. For additional information on counterintelligence processes and products, to include SCRM, refer to the Technology and Program Protection Guidebook.

APPENDIX 1: INTELLIGENCE SUPPORT PRODUCTS

This appendix describes both DoD and Service intelligence support products. These products serve as practical examples and are intended to provide ideas for augmenting existing products or developing tailored products.

A-1-1 Tailored Threat Assessment

In this document, the concept of tailored threat assessments or tailored products is mentioned frequently. This does not refer to a specific product but rather the broader concept of an assessment designed for a specific program by the PM and acquisition intelligence professionals, with the approval of the MDA and documented in the Acquisition Decision Memorandum (ADM). The process allows flexibility to determine the most suitable approach for the program's specific requirements.

A-1-2 Validated On-Line Lifecycle Threats (VOLTs)

The VOLT is the authoritative threat assessment tailored for one or more programs as applicable. VOLTs include threat modules and can include additional tailoring to articulate the relevance of each module to a specific acquisition program or planned capability. Acquisition intelligence professionals can request combined VOLTs to serve multiple ACAT I-III programs, but MCAs and programs on the DOT&E Oversight List require a unique, system-specific VOLT. VOLT development starts with the establishment of a Threat Steering Group composed of the program office representatives, DIA/Service Intelligence Production Center representatives, DevOps Test representatives, DOT&E representatives (if under DOT&E oversight) and the program's acquisition intelligence analyst. The goal is to identify the program's KPPs, critical components/functions, and relevant threats, including a review or addition of CIPs. Exemplars of VOLTs are available on SIPRNet at https://threatlibrary.d-se.dia.smil.mil/VOLTs/ or JWICS at https://threatlibrary.dodiis.ic.gov/VOLTs/.

Key Points:

- Intelligence Production Centers (IPCs) produce VOLTs and DIA validates those produced for ACAT ID or IAM programs.
- VOLTs can be used to support multiple programs with similar performance attributes, or those that share an employment concept of operations and have a similar employment timeline.
- DOT&E has authority to request a VOLT or VOLT update through COLISEUM for any program on the DOT&E Oversight List.
- 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.gov/wiki/TLA-3_Contacts.

A-1-3 Critical Intelligence Parameters (CIPs)

A CIP is a defined threat capability or technology development threshold that, if attained (breached) may impede the lethality, survivability, or sustainability of U.S. defense acquisition systems. CIPs therefore receive focused intelligence analysis and reporting that informs revisions to requirements, incremental upgrades, or potentially new acquisition programs to ensure capabilities remain

technologically competitive on the modern battlefield. Acquisition intelligence professionals 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 the Defense Intelligence Threat Library, which is the authoritative source for CIPs and CIP statuses. Users can browse and subscribe to CIPs in the Threat Library to receive notifications of CIP updates. Examples of CIPs are available at the following SIPRNet site:

https://intellipedia.intelink.sgov.gov/wiki/Critical_Intelligence_Parameter#.28U.29_cip_examples.

The Joint Acquisition Intelligence for Mission Integration (JAIMI) tool provides users with assistance creating parametric based CIPs via a "CIP wizard" tool with a machine-to-machine connection to MEPED.

Key Points:

- CIPs submitted to IPCs are associated with the program 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.
- CIPs are considered “near breached” when the DIE assesses that the CIP likely will be breached in the next five years.
- CIPs serve as indications & warning to provide 5-year head start on S&T investments and program upgrades.

A-1-4 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 Department’s supporting Defense CI Component produces the TTRA. DIA validates the TTRA for ACAT ID and ACAT IAM programs while the Military Department’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 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.

A-1-5 Intelligence Health Assessments (IHAs) - *USAF*

IHAs evaluate the six JCIDS categories to ensure intelligence support for a system is documented. The PM uses the results of an IHA to identify and document intelligence 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.

AID's JAIMI tool provides users with a step-by-step workflow to create and manage IHAs that includes an exportable risk matrix to support decision briefings.

A-1-6 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 include:

- 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.
- GEOINT data that provides mapping and locating data.
- EWIR data that identifies and counteract enemy radar and detection.
- Threat models (TMAP) and Threat Technical Data Packages (T2DP).

Acquisition intelligence professionals 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, threat models, and GEOINT products. AIRES is a valuable resource in this process.

A program's LMDP is updated before each milestone decision to enable updated availability assessments and associated 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. DIA's Validated IMD Supportability Report (VISR)

is the assessment of LMDPs in support of the IMD producers and the acquisition process, as facilitated and coordinated by DIA/TLA-3. Intelligence Mission Data Center (IMDC). The IMDC ties IMD requirements and any shortfalls to their associated KPPs/KSAs. The VISR provides a technical evaluation of the enterprise's ability to support IMD demands throughout a weapon system's life cycle. 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; it 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:

- If a program uses intelligence mission data, they will need an LMDP.
- The LMDP requirement begins at MS-A and is updated in accordance with designated life cycle events.
- For questions on identifying priorities and requirements for establishing an LMDP, contact DIA's IMDC at: IMDC_LMDP_Support@dia.smil.mil.
- A Program Executive Officer and Component Acquisition Executive-approved draft LMDP is due for a development 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 and leverage AIRES in this process. 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 acquisition intelligence professionals 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.

A-1-7 Threat Test Support Package (TTSP) – *USA*

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 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. The JAIMI tool provides users with a step-by-step workflow to create and manage TTSPs. Users can browse existing TTSPs or walk through the process of creating a new TTSP in JAIMI. JAIMI supports business analytics behind the demand signal for threat representations to drive surrogate developments, foreign materiel acquisition, and production of threat models.

A-1-8 Adversary Cyber Threat Assessments (ACTAs) - *USAF*

ACTAs are produced by acquisition intelligence professionals supporting the program office; however, ACTAs can be bolstered by an IPC when a PR is submitted in COLISEUM with specific questions. ACTAs are not considered 'finished intelligence' products from an IPC but may suffice when formal intelligence threat products are not available. Many PMs will accept an acquisition intelligence 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., 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 or authority to test. 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 Air Force Life Cycle Management Center's Acquisition Intelligence 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%20Ex-emplar.pptx.

A-1-9 References

The references cited in this table focus on acquisition and intelligence issuances that provide additional information to the PM and the acquisition intelligence professionals 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 Defense Acquisition System
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 5000.89, Test and Evaluation
DoD Instruction 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers
DoD Manual 5000.78, Rapid Acquisition Authority (RAA)
DoD Guidebook, Technology and Program Protection Guidebook
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
DIA Standard 5000.1, Defense Intelligence Threat Support to Acquisition
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 71-9, Warfighting Capabilities Determination
Army Regulation 73-1, Test and Evaluation Policy
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 5000.2G, 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

APPENDIX 2: ADDITIONAL RESOURCES

A-2-1 Intelligence Sites and Systems to Benefit Acquisition Intelligence

The following websites and systems will benefit acquisition intelligence professionals in the performance of their duties.

Joint Acquisition Intelligence for Mission Integration (JAIMI): JAIMI is an OSD A&S/AID developed tool designed to be the end-to-end digital ecosystem for DoD acquisition intelligence and program manager personnel. It is a web-based application, available on SIPRNet and JWICS, that leverages data and software to help U.S. platforms stay ahead of advancing threats in a long-term, strategic competition. JAIMI includes features for tracking and managing intelligence support to acquisition including a resources page with links and best practices, dataset of acquisition programs appended with intelligence support metadata, file management, activity tracking, CIP creation workflow, IHA creation workflow, TTSP Workflow, and analytics dashboards.

DIA Intelligence Threat Library (DITL): The DITL is an OSD directed and DIA managed tool designed to be the end-to-end digital ecosystem for DoD acquisition intelligence supporting the requirements, acquisition, and test communities. It hosts in a single location foundational, tailored, and critical acquisition intelligence to increase discoverability and prevent the formation of discrete information silos to maximize effective and efficient use of resources and minimize duplication. Key resources hosted in the DITL include Threat Modules, VOLTs, and CIPs. The DITL includes machine-to-machine connections to MEPED to enable creation of digital threat tables on specific topics, dynamic display of authoritative threat data and analysis, subscription services that provide instantaneous automated notifications of desired threat updates, and feedback tools to drive improvements to foundational and tailored threat assessments. The DITL also provides insight into critical threat topics and analytic tasking that can inform and drive improvements to acquisition intelligence enterprise management. Current VOLTs can be found on SIPRNet at https://threatlibrary.dse.dia.smil.mil/volts and on 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.

Defense Acquisition Visibility Environment (DAVE): DAVE is an authoritative source for Program Information for major programs. It provides access to accurate, authoritative, and reliable data to support acquisition oversight, insight, analysis, and decision making. Capabilities include the Acquisition Information Repository, Acquisition Visibility Data Framework, cost and funding charts, data sets and data opportunities visualization, program submissions, Reference Environment for the Business of Acquisition, and the Selected Acquisition Report (SAR)/Machine-assisted Analytic Rapid Repository System (MAR) Catalog (https://dave.acq.osd.mil/login).

Acquisition Intelligence Requirements Enterprise System (AIRES): AIRES is a web-based application that is the authoritative source of Intelligence Mission Data (IMD) and Modeling and Simulation (M&S) requirements across services, programs, and Intelligence Production Centers (IPCs). AIRES automates

many of the responsibilities directed by DODD 5250, CJCSI 5123, CJCSI 3318, DODI 5000.86, etc., and Service instructions. AIRES supports the Joint Staff's Priorities and Risk Management Framework (PRMF), as well as DOD 5250's Life Cycle Mission Data Plan (LMDP). AIRES is DOD's sole repository to collect IMD and M&S requirements, prioritize requirements, determine IMD and M&S gaps, schedule, and track IMD and M&S production, and provide data analytics.

Office of Naval Intelligence Repository for Characterization of the Adversary/Engineering Level Characterization of the Adversary: 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: 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 acquisition intelligence 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 intelligence 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 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://lni.cia.ic.gov.

A-2-2 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 Acquisition Intelligence Division for inclusion in future versions of this guidance.

Army/G2 iSTART: Virtual and in-person training event for the Army acquisition intelligence workforce and those interested in the intelligence support to acquisition mission area. It is open to all Services and other customers/stakeholders.

AF Life Cycle Management Center/Intelligence Directorate Intelligence Formal Training Unit: Virtual and in person training event several times during the year for AF's acquisition intelligence workforce.

DAU ACQ 110 Fundamentals of Acquisition Intelligence: This course provides a joint, service-level overview of acquisition intelligence that addresses timely and effective communication between the intelligence, requirements, and acquisition communities throughout the acquisition life cycle.

DAU CACQ 010 Foundational Acquisition Intelligence Credential: This credential provides a joint, department-level foundational understanding of the knowledge and skills required to perform the role of the acquisition intelligence analyst. This credential focuses on the timely and effective communication

between the intelligence, requirements, and acquisition communities throughout the acquisition lifecycle.

A-2-3 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 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 intelligence mission data sufficiency analysis efforts throughout the DoD. Led by Secretary of the Air Force, Administrative Assistant's Concepts, Development, and Management Office, the JIC ensures timely execution of funds, synchronizes intelligence support for model creation, monitors simulations, and reports outcomes to OUSD. Additional information can be found on NIPR at https://intelshare.intelink.gov/sites/jic/ or on SIPR at https://intelshare.intelink.sgov.gov/sites/jic/

Chief Modeling and Simulation Office 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 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.

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

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)

U.S. Marine Corps:

U.S. Space Force:

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

APPENDIX 3: DIGITAL ENGINEERING

As the Department moves to Digital Engineering, the Defense Intelligence Enterprise must transform its policy, processes, and tools to accommodate working in a digital construct. Digital engineering is an integrated digital approach using authoritative sources of system data and models as a continuum throughout the development and life of a system. Digital engineering updates traditional systems engineering practices to take advantage of computational technology, modeling, analytics, and data sciences. For more information see the Department of Defense Digital Engineering Strategy: https://ac.cto.mil/digital_engineering/.

Figure 13 - The Army's XM 30 is an example of a program leveraging digital engineering

As evidenced across the Services and industry, digital engineering is a necessary practice to support acquisition in an environment of increasing global challenges and dynamic threat environments. Scientific and Technical Intelligence, as a key enabler of U.S. weapon system development, requires modernization to the ways in which it is created and delivered in order to fully support modern DoD and Service model-based systems engineering (MBSE).

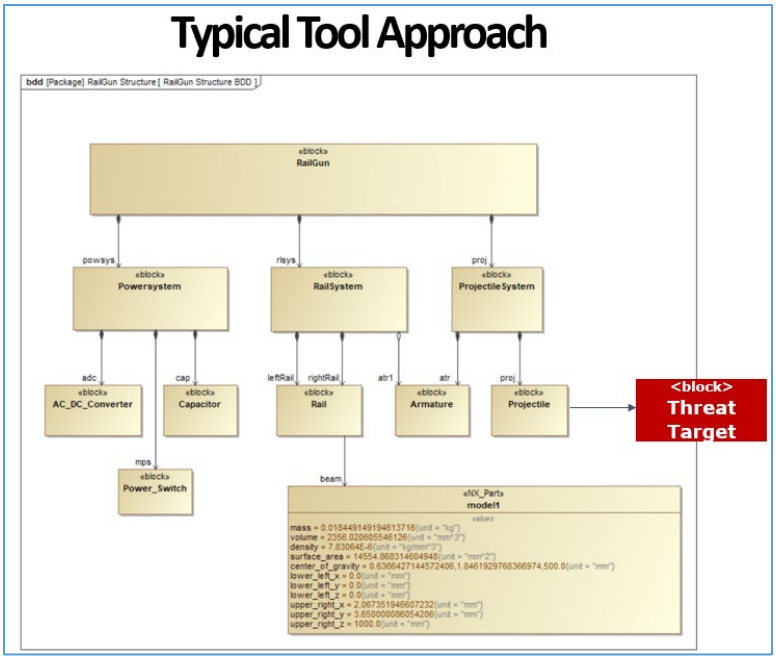


Figure 14: System Model Block Diagram

Digitizing threat models, simulations, and data in an externally facing, persistent, and machine-readable manner sets the foundation to support MBSE, ensuring currency of technical and engineering content about the threat throughout the acquisition lifecycle, continuously informing engineering and trade space decisions. To support this transition, our Acquisition Intelligence workforce must become familiar with talking in Systems Modeling Language. DAU course CLE 084 “Models, Simulations, and Digital Engineering” is a great foundational course that will introduce you to the concepts and terminology.

APPENDIX 4: ABBREVIATIONS AND ACRONYMS

Term	Definition
AAF	Adaptive Acquisition Framework
ACAT	Acquisition Category
ACTA	Adversary Cyber Threat Assessments
ADM	Acquisition Decision Memorandum
AID	Acquisition Intelligence Division
AISWG	The Acquisition Intelligence Support Working Group
AoA	Analysis of Alternatives
C&P	Characteristics and Performance
CIP	Critical Intelligence Parameter
CPI	Critical Program Information
DA	Decision Authority
DAS	Defense Acquisition System
DBS	Defense Business Systems
DIE	Defense Intelligence Enterprise
DITL	Defense Intelligence Threat Library
DOT&E	Director, Operational Test and Evaluation
EWIR	Electronic Warfare Integrated Reprogramming
FSM	Functional Services Manager
FY	Fiscal Year
GEOINT	Geospatial Intelligence
IC	Intelligence Community
ICD	Intelligence Community Directive

Term	Definition
IHA	Intelligence Health Assessment
IMD	Intelligence Mission Data
IMD SWG	Intelligence Mission Data Standing Working Group
IMDC	Intelligence Mission Data Center
ISA	Intelligence Supportability Assessments
ISTAAF	Intelligence Support to the Adaptive Acquisition Framework
JAIMI	Joint Acquisition Intelligence for Mission Integration
JCIDS	Joint Capabilities Integration and Development System
JIC	Joint Integration Cell
JWICS	Joint Worldwide Intelligence Communications System
KPP	Key Performance Parameter
LMDP	Lifecycle Mission Data Plan
LNI	Library of National Intelligence
MAR	Machine-Assisted Analytic Rapid Repository System
MBSE	Model-Based Systems Engineering
MCA	Major Capability Acquisition
MDAP	Major Defense Acquisition Programs
MDCITA	Multi-Disciplined Counterintelligence Threat Assessment
MTA	Middle Tier Acquisition
NDS	National Defense Strategy
OUSD (A&S)	Under Secretary of Defense for Acquisition and Sustainment
PPP	Program Protection Plan
PR	Production Requirement
PRMF	Priorities and Risk Management Framework

Term	Definition
RDA	Research, Development, and Acquisition
RMF	Risk Management Framework
SA	Services Acquisition
SIPRNet	Secure Internet Protocol Router Network
SWP	Software Acquisition Pathway
T&E	Test and Evaluation
TSDB	Threat System Database
TTRA	Technology Targeting Risk Assessments
TTSP	Threat Test Support Packages
UCA	Urgent Capability Acquisition
VISR	Validated IMD Supportability Report
VOLT	Validated Online Lifecycle Threat