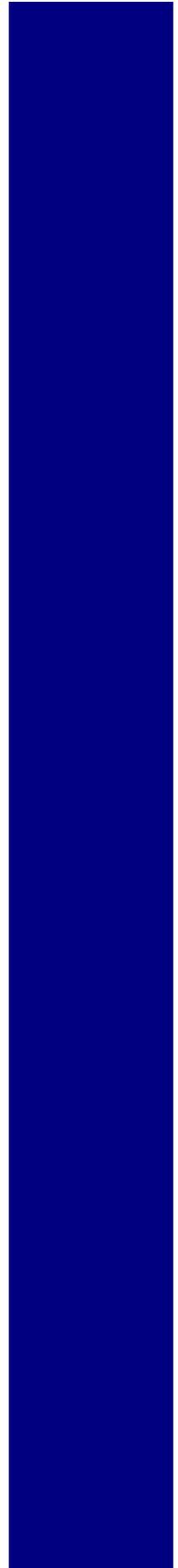


Defense Acquisition Guidebook

Chapter 8 - Intelligence Analysis Support to Acquisition

Production Date: 15 May 2013



DEFENSE ACQUISITION GUIDEBOOK

Chapter 8 - Intelligence Analysis Support to Acquisition

8.0. Introduction

8.1. Threat Intelligence Support

8.2. Signature and other Intelligence Mission Data Support

8.3. Support to the Intelligence Certification Process

8.0. Introduction

8.0.1. Purpose

8.0.2. Contents

8.0.3. Applicability

8.0.4. Acquisition Documents Discussed in Chapter 8

8.0.5. Support from Functional Offices

8.0. Introduction

Intelligence analysis integration is increasingly critical to DoD acquisition programs. Threat intelligence analysis and/or signatures and other Intelligence Mission Data (IMD) are required to inform and enable program capabilities and minimize costs to the government across the entire acquisition process.

Early and incremental involvement and collaboration with the DoD Intelligence Community (DoD IC) will help reduce program risks to schedule, cost, and performance. Early collaboration also increases the likelihood that the delivered system will be fully capable and more survivable against the relevant adversary threats.

Reduced risk to schedule is derived from the early identification of work to be performed by the DoD IC, proper tasking of the DoD IC at the appropriate acquisition milestone through production requirements, identification of capability gaps, costing, and negotiated delivery dates for products.

Reduced risk to cost is derived from the earliest identification of the costs and resource strategies to realize the intelligence support needed to close capability gaps throughout the acquisition life-cycle. Collaboration with the DoD IC assists both the DoD IC and the acquisition communities

in determining the costs to be borne by the DoD IC and the costs to be borne by the program.

Reduced risk to performance is driven by obtaining and inculcating threat analysis information and signature and other IMD from Material Solution Analysis through Full-Rate Production phases.

For Program Protection, Security and Counterintelligence support to acquisition programs see Chapter 13, Program Protection.

8.0.1. Purpose

The purpose of this chapter is to enable the PM to use intelligence information and data to ensure maximum war-fighting capability at the minimum risk to cost and schedule.

8.0.2. Contents

This Chapter is divided into three sections as follows:

Section 8.1 Threat Intelligence Support.

The program may require intelligence analysis of foreign threat capabilities integral to the development of future U.S. military systems and platforms over the life of the program. Identifying projected adversarial threat battlefield capabilities and evolving scientific and technical developments that affect a program or a capability's design or implementation is crucial to successful development, employment, and sustainment processes.

Section 8.2 Signatures and other IMD.

This section explains how PMs can successfully account for signatures and other IMD during system and sensor acquisition for building target models, developing algorithms, optimizing sensor design, and validating sensor functionality. As requirements for smarter, interoperable platforms and systems grow, the need for signatures and other IMD will continue to trend upwards.

Section 8.3 Intelligence Certification.

This section explains how PMs complete the Intelligence Certification and threat validation required by the Joint Staff in support of the [Joint Capabilities Integration and Development System \(JCIDS\)](#) process.

8.0.3. Applicability

This chapter applies to programs that are dependent upon threat intelligence analysis, signatures, and other IMD to enable mission capability in accordance with [DoDD 5000.02](#), and DoDD 5250.01 .

Threat intelligence analysis is provided as Capstone Threat Assessments (CTA), System Threat Assessment Report (STAR) or System Threat Assessment (STA); these are defined and explained in this chapter.

A signature is a distinctive characteristic or set of characteristics that consistently recurs and identifies a piece of equipment, material, activity, individual, or event such as a radio frequency or acoustic characteristics.

IMD is DOD intelligence used for programming platform mission systems in development, testing, operations and sustainment including, but not limited to, the following functional areas: Signatures, Electronic Warfare Integrated Reprogramming (EWIR), Order of Battle (OOB), Characteristics & Performance (C&P), and Geospatial Intelligence (GEOINT).

Programs dependent on signature and other IMD are those that require data for programming platform mission systems in development, testing, operations and sustainment to conduct combat identification; Intelligence, Surveillance and Reconnaissance; and targeting using, but not limited to the signatures and IMD as described above.

This Chapter does not apply to acquisitions by the DoD Components that involve a Special Access Program (SAP) created under the authority of [Executive Order 12958](#). The unique nature of SAPs requires compliance with special security procedures of [DoDD 5205.07](#).

8.0.4. Acquisition Documents Discussed in Chapter 8

The acquisition program documents discussed in Chapter 8 are listed below in Table 8.0.4.T1.

Table 8.0.4.T1. Acquisition Documents Discussed in Chapter 8

Document	Prepare	Preparation Reference
Capstone Threat Assessment (CTA)	During capability shortfall identification process. (Maintained by the DoD Intelligence Community throughout the capability development and acquisition lifecycle.)	JCIDS Manual CJCSI 3312.01B DIAI 5000.002

System Threat Assessment Report (STAR) / System Threat Assessment (STA)	Prior to Milestone A, task the supporting intelligence production center.	DoDI 5000.02 E4, Table 3 DIAI 5000.002 Service and Component Intelligence Support to Acquisition policies
MAIS programs and AIS programs on the DOT&E Oversight List regardless of ACT designation are to use the Information Operations Capstone Threat Assessment		
Technology Development Strategy	To support Milestone A decision. Provide summary of the threat assessment in relation to the capabilities or operational concepts the system will support.	DoDI 5000.02 Encl 2 PDUSD AT&L Memo, 20 APR 2011 Document Streamlining Program Strategies and Systems Engineering Plan
Life-cycle Signature Support Plan (LSSP)	When an acquisition program is signature (and other IMD)-dependent.	DoDD 5250.01 DIAI 3115.03

8.0.5. Support from Functional Offices

To properly accomplish activities described in this chapter, the PM needs the cooperation and support of related functional offices. Support to the acquisition community from the intelligence community involves a number of staff organizations and support activities that may be unfamiliar to members of the acquisition community. Table 8.0.5.T1 lists the functional offices that may support the PM in various tasks discussed in Chapter 8. This table identifies (and links to) the sections of Chapter 8 that describe various situations involving these offices. The individual assigned responsibility for coordinating intelligence support within a program office, laboratory, test and evaluation center, or other Research, Development, Test and Evaluation (RDT&E) organization should identify the proper contacts in these organizations prior to initiating program planning.

Table 8.0.5.T1. Functional Offices in Chapter 8

Functional Offices	Chapter 8 References
Intelligence Support Organization <ul style="list-style-type: none"> • Threat Intelligence <ul style="list-style-type: none"> ○ DoD Intelligence Community ○ Capability Development Threat Support Offices ○ System/Material Command Threat Support Offices • Intelligence Mission Data 	8.1 8.2
Intelligence Requirements Certification Office <ul style="list-style-type: none"> • Support to the Intelligence Certification Process <ul style="list-style-type: none"> ○ Joint Staff ○ DoD Intelligence Community 	8.3

8.1. Threat Intelligence Support

8.1.1. Capstone Threat Assessment (CTA)

8.1.2. System Threat Assessment Report (STAR)/System Threat Assessment (STA)

8.1.3. Threat Validation

8.1.4. Support to Operational Test and Evaluation

8.1. Threat Intelligence Support

Threat Intelligence support to the acquisition process provides an understanding of foreign threat capabilities that is integral to the development of future U.S. military systems and platforms. Identifying projected adversarial threat capabilities, to include scientific and technical developments, which may affect a program or a capability’s design or implementation is crucial to a successful development process. Furthermore, the applicable threat information must be continually updated to account for adversarial capabilities throughout the program or capability’s projected acquisition to ensure that technological superiority over adversarial capabilities is maintained. See the graphic in Figure 8.1.F1.

Figure 8.1.F1. Depiction of Life-Cycle Intelligence Analysis Requirements

Lifecycle Intelligence Analysis Requirements

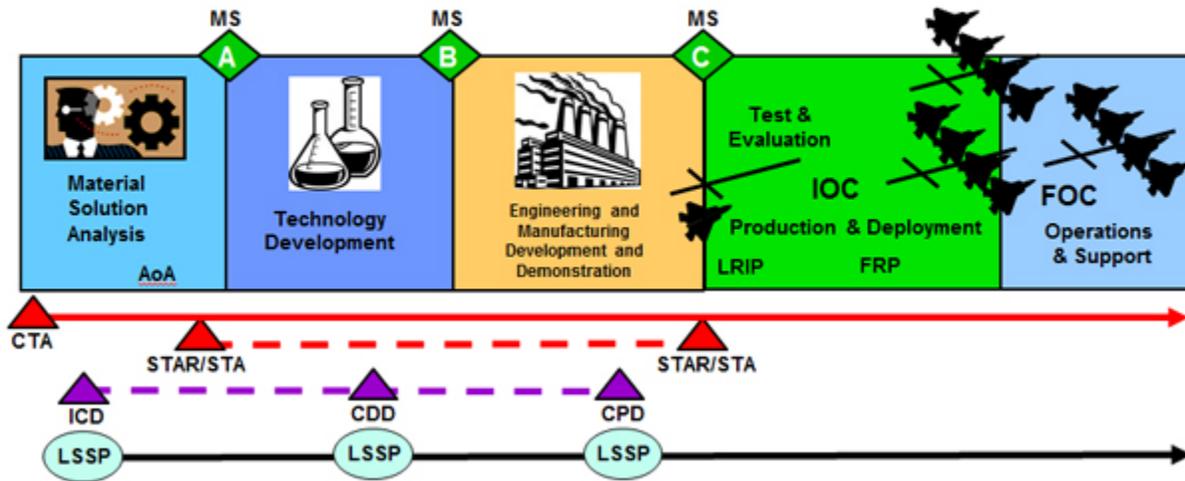


Figure 8.1.F1 illustrates the range of support provided by the threat intelligence community over the life of a particular capability shortfall identification process and resulting system acquisition program. Capstone Threat Assessments (CTA) inform the capability shortfall identification process as well as during early phases of system acquisition prior to the generation of a STAR/STA. The CTAs project foreign capabilities in particular warfare areas looking out 20 years.

At the beginning of the Material Solution Analysis phase, the program office or capability sponsor should contact the appropriate intelligence production center to support integration of validated threat information into the Technology Development Strategy. Threat information may come from DIA-validated Capstone Threat Assessments or other DIA/Service validated STARS/STAs that align with the capability mission, CONOPS, and employment timeline.

Once the capabilities sponsor, program manager or other appropriate enabler identifies concepts or prototypes for the materiel solution, the program office or capability sponsor should task the appropriate intelligence production center for the lead service to produce the System Threat Assessment Report (STAR) for Acquisition Category (ACAT) I/ Major Defense Acquisition Programs (MDAPs) and the System Threat Assessment (STA) for ACAT II programs in accordance with the regulations of that service. The program office needs to work with the producing intelligence center to provide system specific characteristics, employment CONOPS, and employment timeline as they evolve. The program office must also work with the appropriate Service Intelligence Production Center to identify Critical Intelligence Parameters (CIPs) and ensure production requirements are levied against those CIPs.

Analytic Baseline . A systems Analytic Baseline is comprised of DoD-level authoritative policy planning guidance and an intelligence assessment of present trends, patterns and conditions, combined with validated parametric, characteristics/performance and employment data needed

for development, testing, and/or training. When combined with information on appropriate friendly and neutral (Blue/Gray/White*) systems, it represents an extrapolation of the total security environment in which the system is expected to operate. A package comprises a scenario, concept of operations, and integrated data used by the DOD components as a foundation for strategic analyses. Examples of analytical baselines include scenarios and supporting data used for computer assisted war games and theater campaign simulations.

* The three colors reflect three different entities. Blue represents U.S. system data, Gray represents U.S.-produced but foreign-operated system data, and White represents neutrals. When doing long-term analysis, the impact of Blue systems must be taken in light of friendly and neutral systems.

8.1.1. Capstone Threat Assessment (CTA)

CTAs provide the bedrock analytical foundation for threat intelligence support to the defense acquisition process. CTAs, covering major warfare areas, present the DoD Intelligence Community validated position with respect to those warfare areas and will constitute the primary source of threat intelligence for the preparation of Initial Threat Environmental Assessments, STARs/STAs, and threat sections of documents supporting the JCIDS process. In order to effectively support both the capability development and acquisition processes, CTAs are not specific to existing or projected US systems, cover the current threat environment, and, in general, project threats out 20 years from the effective date of the CTA. With the lead intelligence production center, DIA's Defense Warning Office (DIA/DWO) co-chairs the Threat Steering Group (TSG) that produces and reviews the document. CTAs should be updated as determined by the responsible TSG but in any case every 24 months. DIA validates all CTAs.

Table 8.1.1.T1. Listing of Capstone Threat Assessments

WARFARE AREA	PRIMARY PRODUCTION OFFICE OR CENTER
Air Warfare	National Air and Space Intelligence Center (NASIC)
Chemical, Biological and Radiological Defense	Defense Intelligence Agency (DIA)
Information Operations	DIA/Joint Information Operations Threat Working Group
Land Warfare	National Ground Intelligence Center (NGIC)
Missile Defense	Defense Intelligence Agency (DIA)
Naval Warfare	Office of Naval Intelligence (ONI)
Space Warfare	National Air and Space Intelligence Center (NASIC)

The Capstone Threat Assessments can be found at the JWICS or SIPRNET websites of the primary production office or center.

For more information contact DIAs Defense Warning Office at:

JWICS email - dise541@dodiiis.ic.gov

SIPRNET Email jeffery.vales@dse.dia.smil.mil

Commercial 434-956-2170

DSN 521

8.1.2. System Threat Assessment Report (STAR)/System Threat Assessment (STA)

The Defense Intelligence Agency (DIA) provides validation for System Threat Assessment Reports (STARs), prepared by the appropriate Service, to support Acquisition Category (ACAT) ID/ Major Defense Acquisition Programs (MDAPs). Appropriate Defense Intelligence organization(s), identified by the component headquarter intelligence organizations, prepare the STAR. The assessment should be kept current and validated throughout the acquisition process. DoD Instruction 5000.02 requires that MDAPs have a validated STAR in place at Milestones B and C (and at program initiation for shipbuilding programs). The assessment should be system specific, to the degree that the system definition is available at the time the assessment is being prepared, and should address projected adversary capabilities at system initial operating capability (IOC) and at IOC plus 10 years. DIA will co-chair the TSGs for ACAT ID STARs with the producing command or center. STARs for ACAT IC MDAPs and STAs for ACAT II non-MDAPs are prepared and validated by the lead service in accordance with service regulations. DIA Instruction 5000.002 describes the required STAR elements and format.

Critical Intelligence Parameters (CIPs) are established and examined through the joint and collaborative efforts of the intelligence, capability sponsor, and acquisition management community to aid in developing intelligence production requirements to support an acquisition program. CIPs are those key performance thresholds of foreign threat systems, which, if exceeded could compromise the mission effectiveness of the U.S. system in development. Adversary military doctrine, tactics, strategy, and expected employment of systems should be considered in the CIPs. Program specific CIPs, and their associated production requirements, are a key part of a STAR and will be required for validation. The inclusion of CIPs is also encouraged for STAs. If a CIP is breached, the responsible intelligence production center will notify the program office and DIA/DWO in accordance with DIA Instruction 5000.002. DIA/DWO will notify the appropriate organizations in the Office of the Secretary of Defense.

At the discretion of the responsible TSG, STARs/STAs can be used to support multiple programs which address like performance attributes, share an employment CONOPs, and have a similar employment timeline. Individual system descriptions and CIPs are still required to support the generation of the STAR.

Major Automated Information System (MAIS) programs use the Joint Information Operations Working Group and DIA-validated Information Operations (IO) Capstone Threat Assessment or service produced System Threat Assessment Report. DIA will validate service produced ACAT IAM STARS when the IO CTA is not used. Non-MAIS programs are encouraged to use the IO Capstone Threat Assessment or service produced System Threat Assessment Report as their threat baseline. MAIS programs still need to provide system descriptions, as well as the CIPs and production requirements that are specific to their program's needs.

8.1.3. Threat Validation

As noted above, for Major Defense Acquisition Programs (MDAPs) subject to Defense Acquisition Board review, the Defense Intelligence Agency (DIA) validates System Threat Assessment Reports (STARS) for Acquisition Category (ACAT) ID/ Major Defense Acquisition Programs (MDAPs). STARS for ACAT IC MDAPs and System Threat Assessments for ACAT II programs are validated by the appropriate service. DIA validation assesses the appropriateness and completeness of the intelligence, consistency with existing intelligence positions, and the use of accepted analytic tradecraft in developing the assessments. Working with its partners in the DOD intelligence community and, as needed, in the larger intelligence community, validation is intended to ensure that all relevant data is considered and appropriately used by author(s) of the assessment.

DIA validates threat information contained in [Joint Capabilities Integration and Development System](#) documents as described in the [JCIDS Manual](#) . When requested by the appropriate authority, DIA may also validate other threat information not contained in the STAR but needed for program development.

8.1.4. Support to Operational Test and Evaluation

The [Test and Evaluation Master Plan](#) should define specific intelligence requirements to support program operational test and evaluation. When requested by the appropriate authority in the offices of the Director, Operational Test and Evaluation (DOT&E) or the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), DIA, working with the Department of Defense Intelligence Community (DoD IC), will provide additional intelligence support to the operational testing of programs on the annual DOT&E Oversight List. DIA support will not include the validation of specific testing scenarios or the validation of "Blue" (see paragraph 8.1) surrogate systems or platforms, but can include certification that the threat information in the test plan is correct and consistent with existing assessments.

Per [DoD Instruction 5000.02](#) certain programs on the DOT&E Oversight List are to be considered as MDAPs for testing and evaluation purposes and will require a System Threat Assessment Report regardless of Acquisition Category designation.

8.2. Signature and other Intelligence Mission Data Support

8.2.1. Signature and other Intelligence Mission Data support in the Technology

[Development Strategy \(TDS\)](#)

[8.2.2. Distributed DoD Signatures and other Intelligence Mission Data Pool and Standards](#)

[8.2.3. Intelligence Mission Data \(IMD\) Support](#)

[8.2.3.1. Materiel Solution Analysis Phase to Milestone A](#)

[8.2.3.2. Technology Development Phase to Milestone B](#)

[8.2.3.3. Engineering & Manufacturing Phase to Milestone C](#)

[8.2.3.4. Low-Rate Initial Production to Full-rate Production/Full Deployment Decision Review \(FRP-DR\) to Disposal](#)

[8.2.4. Life-cycle Signature Support Plan \(LSSP\) Assessment](#)

8.2. Signature and other Intelligence Mission Data Support

The first step for managers involved with acquisition efforts and programs is to identify any requirement for intelligence analysis related to enabling mission capability. The data derived from this analysis and needed by acquisition programs is commonly referred to as signatures and other IMD. See definitions at Section 8.0.3. Applicability .

Further, Services have liaisons with expertise in both intelligence and acquisitions. These professionals know how to interface with the DoD IC and are typically part of the acquisition team (or are accessible to the team).

[DoD Directive 5250.01](#), Management of Signature Support Within the Department of Defense, establishes the Signatures Support Program (SSP) (previously known as the National Signatures Program (NSP)) to manage and execute the DoD Signature Support Mission (SSM). Signatures are essential for building target models, developing algorithms, optimizing sensor design, and validating sensor functionality. The PM should account for signatures during system and sensor acquisition.

The PM documents detailed signature requirements in a [Life-cycle Signature Support Plan \(LSSP\)](#) (per DoD Directive 5250.01) and defines overall signature support requirements and compliance with signature standards in the Capability Development Document and Capability Production Document (per [CJCS Instruction 3312.01](#), "Joint Military Intelligence Requirements Certification"). Under CJCS Instruction 3312.01, the SSP uses the LSSP to assess the ability of the signatures community to support a program's signature requirements.

8.2.1. Signature and other Intelligence Mission Data support in the Technology Development Strategy (TDS)

[DoD Directive 5250.01](#) requires that signature support requirements and funding be incorporated

into a program's acquisition strategy. Per PDUSD AT&L Memo, 20 APR 2011 Document Streamlining Program Strategies and Systems Engineering Plan, the TDS should provide a table that indicates the program life-cycle signature support requirements. Life-cycle signature support funding requirements will be reflected in the TDS program funding summary. [[Technology Development Strategy Memo](#)] If required signatures are not already available in the distributed national signatures pool, the program will need to plan and budget for development of these signatures. Stating in the TDS that a program is signature dependent and will identify requirements in a Life-cycle Signature Support Plan ensures that the Program Office has considered signature development resource needs in the program planning and budgeting process.

8.2.2. Distributed DoD Signatures and other Intelligence Mission Data Pool and Standards

DoD Directive 5250.01 requires that all signatures provided for the DoD be made available through a distributed DoD signature pool and adhere to established standards. Whether developed by a government signature center or by a contractor, if the signatures and other IMD are made available through a distributed pool, they can be shared to prevent duplication of work and cost across the DoD.

An essential element to make this possible is the use of standards to ensure common meta-data tags and processing methods are used. This in turn ensures the signatures will be discoverable in the distributed pool and that the signatures will be usable for multiple customer's including acquisition programs and operational systems.

The Signatures Support Program provides single access point connectivity to the distributed pool through web-pages on JWICS (<http://ssp.dodis.ic.gov/>), SIPRNet (<http://dt.dia.smil.mil/ssp>), and NIPRNet (site under development). (**NOTE:** These sites cannot be accessed via the Internet or Non-secured Internet Protocol Router Network.) Current signature standards are also available at these web-sites.

8.2.3. Intelligence Mission Data (IMD) Support

DoD Directive 5250.01, Management of Signature Support Within the Department of Defense, requires all signature-dependent technology and acquisition programs and efforts to submit a [Life-cycle Signature Support Plan \(LSSP\)](#) throughout their respective lifecycle. An LSSP is intended to facilitate collaboration and agreement between the acquisition, requirements and intelligence communities regarding signatures, also known as Intelligence Mission Data (IMD), which is DoD intelligence used for programming platform mission systems in development, testing, operations, and sustainment including, but not limited to the following functional areas: Intelligence Signatures, Electronic Warfare Integrated Reprogramming (EWIR), Order of Battle (OOB), Characteristics and Performance (C&P), and Geospatial Intelligence (GEOINT).

Technology initiatives and weapons systems design, development, test, evaluation, operation and sustainment increasingly rely on signatures and other Intelligence Mission Data to meet expected capability. The identification of required data type, conditions, fidelity, precision, etc., often evolves as the technology and systems mature. Additionally, the intelligence community must

constantly respond to these requirements in an ever changing environment as threats, targets, and systems evolve over time. For these reasons developing an LSSP must be initiated early in a programs lifecycle to establish an effective and efficient flow of communication and actions to ensure timely support for IMD requirements.

The LSSP defines specific technology and program IMD requirements. The [DAU LSSP webpage](#) provides an LSSP template, instructions for LSSP completion, an LSSP Signature Requirements Table template, and an example Contract Data Requirements List form for procuring signature data. The [LSSP Template](#) provides an outline and guidance that standardizes communication between the technology or program offices and the intelligence community. The LSSP should contain as much detail as possible to inform intelligence community production and collection decisions. Therefore, increasing detail should be provided in each update and submission of the LSSP. Content considerations for an LSSP by phase and milestone can be found below.

8.2.3.1. Materiel Solution Analysis Phase to Milestone A

In accordance with DAG Chapter 2, a programs strategy document (Technology Development Strategy (TDS)) should identify the (a) systems and subsystems of the program that require intelligence mission data necessary to deliver the intended capabilities; and (b) IMD funding requirements as appropriate. The TDS should refer to the programs LSSP for a listing of the actual IMD requirements and additional detail.

Since final material solutions are yet to be approved prior to Milestone A, specific system configuration and detailed signature requirements are generally not known. However, based on the intended operational mission, the program should identify the IMD type(s) (e.g. Radar, Thermal, Acoustic, EWIR, GEOINT etc.) the domain (e.g. Space, Air, Land, Naval, Missile Defense, etc.), data fidelity (e.g. queuing quality), and possibly sub-categories within a domain (e.g. for Air: Fighter Aircraft) for each subsystem that requires the data. To the level that specific requirements are known, they should be stated.

IMD requirements and related implications to design, performance, and test & evaluation, will be accounted for and considered throughout the Materiel Solution Analysis Phase. Relevant questions to consider and actions to take during this phase include:

Questions:

- Has the program been identified for Foreign Military Sales (FMS)? If yes, then how will this effect design, development, testing, disclosure and releasability of IMD-dependent components?
- For each proposed material solution identified during the Analysis of Alternatives (AoA) process, will the solution require the detection and identification of an activity, event, person, material, or equipment? If yes, then for each proposed detection or identification method (radar, EO/IR, acoustic, chemical, etc.), assess the technical feasibility of acquiring IMD within cost and schedule constraints. Consider the quality of available IMD, the ICs capability to deliver IMD and whether the IMD needs to be collected,

processed and/or developed.

Actions:

- During development of the preliminary system specification, identify which system functions will likely drive the need for IMD, either directly or through derived requirements.
- During development of mission and functional threads, identify potential IMD requirements for inclusion in the LSSP.
- During development of Test and Evaluation strategies and plans, identify IMD requirements based on the need to verify and validate detection and identification functionality. Characterize associated technical risk in the [Test and Evaluation Strategy](#) . Estimate IMD delivery requirements to meet projected test schedules.

8.2.3.2. Technology Development Phase to Milestone B

As a program approaches Milestone B (MS B), the LSSP must include mission or capability specific details and IMD requirements to support program development. For example, as the design matures, additional details should emerge about the design of the sensors and the algorithms. The LSSP should also identify any IMD-based models and intelligence production requirements (PRs) already submitted to a Service Intelligence Production Center (NASIC, NGIC, ONI, MSIC, etc.), other IMD production efforts (e.g. lab, warfare research center, or other agency, organization, etc.), and planned IMD collection events that the program will conduct.

Based on initial IMD requirements defined for Milestone A, refine and add details for the MS B LSSP during development of the Systems Performance Specification and the Allocated Baseline. Relative questions to consider and actions to take during this phase include:

Questions:

- Has the program been identified for Foreign Military Sales (FMS)? If yes, then how will this effect design, development, testing, disclosure and releasability of IMD-dependent components?
- For each proposed detection/identification method (radar, Electro Optical/Infra-Red (EO/IR), acoustic, chemical, etc.), does the required IMD (signature, EWIR, GEOINT, OOB, C&P) already exist (at the estimated quality needed) or will it need to be processed, produced, or collected?
- Is the required detection/identification technology sufficiently mature (Technology Readiness Level 6 or higher) to proceed into end-item design or Milestone B?
- Which IMD-dependent performance requirements need to be verified through test and evaluation?
- Does the program have IMD requirements derived from Modeling and Simulation activities?
- Can the estimated IMD processing, production, collection be completed within required cost and schedule?

- Do the detection/identification algorithms or processes need to be designed to accommodate IMD updates?
- Is there potential for the detection/identification hardware and software to perform IMD collection and provide updates to IMD databases? If yes, has a design study been conducted to assess feasibility and cost/benefit analysis?
- Have significant IMD-dependent functions been included in the proposed exit criteria for the Engineering & Manufacturing Development (EMD) Phase?
- Has the programs spectrum requirements taken into account bandwidth needed for IMD updates during system operations and sustainment?
- Should any IMD data sets be considered as GFE for the EMD Contract?

Actions:

- During the functional allocation process, conduct sensitivity analyses on IMD level of quality (e.g. resolution, frequency range, etc.) to assess quality of available data versus required quality to meet performance KPPs/KPAs.
- Define system level functional and performance requirements derived from items such as: Concept of Operations, system-level performance metrics, mission threads/use cases, and usage environment. Document results and requirements in the System Requirements Document (SRD), LSSP, and Systems Engineering Plan (SEP) as appropriate.
- Assess IMD requirements and schedule relative to DOT&E needs. Document results in the LSSP and by reference in the [Test and Evaluation Master Plan \(TEMP\)](#) .

8.2.3.3. Engineering & Manufacturing Phase to Milestone C

This LSSP will be an update to the previous LSSP. The purpose is to add any new IMD requirements resulting from design maturity or changes in the Concept of Operations (CONOP). It should identify the expected IMD production support and concept necessary for system employment in an operational environment. The LSSP should include information on IMD data existing within the program (modeling and simulation or measured physical parameters) for sensor or algorithm development or for testing purposes, and; information on the existence of any blue IMD collected to support the program. Additionally, the IMD production concept must be defined and coordinated with the intelligence community. At a minimum this should include the identification of organizations for the production of IMD, addressing responsible entities for adversary commercial systems, and US systems (blue). This information is required to ensure that this form of IMD is available through the DoD data sources.

Based on IMD requirements defined in the Milestone B LSSP, refine and add details for the MS C LSSP during development of the System Functional Spec and the Initial Product Baseline. Relevant questions to consider and actions to take during this phase include:

Questions:

- Has the program been identified for Foreign Military Sales (FMS)? If yes, then how will this effect design, development, testing, disclosure and releasability of IMD-dependent components?

- For each proposed detection/identification method (radar, EO/IR, acoustic, chemical, etc.), has IMD (signature, EWIR, GEOINT, OOB, C&P) required for system operations and sustainment been accounted for in the LSSP and Acquisition Plan, at the level of quality needed?
- Which IMD requirements need to be verified in [Follow-on test and evaluation \(FOT&E\)](#)?

Actions:

- Determine IMD-related schedule events (need date from Intelligence Production Center, algorithm or sensor critical test-related dates, etc.) for inclusion in the System Technical Schedule within the SEP.
- Assess IMD-related functions for inclusion in Risk Management assessments in the SEP.
- Assess IMD requirements and schedule relative to FOT&E needs. Document results in the LSSP and by reference in the updated [TEMP](#).

8.2.3.4. Low-Rate Initial Production to Full-rate Production/Full Deployment Decision Review (FRP-DR) to Disposal

In preparation for IOC, an LSSP update is required to ensure congruence with the Final Production Baseline and to fully account for required operational signatures based on the latest threat assessments and CONOPS for the system. This LSSP also needs to fully account for IMD sustainment plans including identification of processes and data sources which are essential for system operations, such as: IMD production processes; IMD databases; IMD verification and validation for operational use; processes and systems which support development and dissemination of IMD data loads for operational missions.

This LSSP requires COCOM coordination and identification of COCOM processes for updating and fulfilling IMD requirements during operation and sustainment of the system. Relevant questions to consider and actions to take during this phase include:

Questions

- For FMS versions of the system, have IMD-dependent components been verified for release and approved by the Designated Disclosure Authority?
- Have IMD support requirements been included in the Life-cycle Sustainment Plan and the Product Support Package?
- Does the current CONOPS for the system drive new or updated IMD requirements? Have these new/updated IMD requirements been handed off to the COCOM requirements prioritization process?
- If the operational system has an IMD reprogramming process, is the reprogramming system and organization ready for operations?

Actions

- Coordinate the LSSP with the systems COCOM.

- Confirm operations of the IMD reprogramming process.

8.2.4. Life-cycle Signature Support Plan (LSSP) Assessment

Each [LSSP](#) is assessed to identify existing signature holdings, requirements, standards, collection events, technologies and associated cost estimates relative to the program. As a result, a custom assessment is provided to the PM to use in planning signature collection, development, and processing to ensure signatures and other IMD are available in time to meet system design and delivery schedules .

[8.3. Support to the Intelligence Certification Process](#)

8.3. Support to the Intelligence Certification Process

The Joint Staff provides review, coordination, and certification/endorsement functions in support of the [Joint Capabilities Integration and Development System \(JCIDS\)](#) process. These functions include intelligence supportability for intelligence certification and threat validation. All acquisition programs or capabilities that are expected to operate in a threat environment must be developed in accordance with the most current threat information. Per [CJCS Instruction 3312.01](#) , the applicable threat information must be continually updated to account for threats throughout the program or capability's projected acquisition life cycle. DIA's Defense Warning Office (DIA/DWO) will assist sponsors with incorporating adversarial threat capabilities throughout the JCIDS review process, and will review and validate the threat input within the JCIDS documents. Threat sections should not include non-adversarial, natural events as threats to capabilities or systems.

[Initial Capabilities Document \(ICD\)](#) . The initiating DOD Component prepares a concise threat summary and threat rationale, working with DIA/DWO as needed. If validated Capstone Threat Assessments (CTAs) or System Threat Assessment Reports (STARs)/System Threat Assessments (STAs) are available and address the threat areas affecting the U.S. capability, these documents should be used as the primary sources for the threat statements. The ICDs reference the threat documents used to support the analysis.

[Capability Development Document \(CDD\)](#) . The initiating DOD Component prepares a concise threat summary and threat rationale, working with DIA/DWO as needed. If validated CTAs or STARs/STAs are available and address the threat areas affecting the U.S. capability, these documents should be used as the primary sources for the threat statements. Programs designated as ACAT-ID MDAPs, or programs with the potential to be so designated, must use DIA-validated threat references.

[Capability Production Document \(CPD\)](#) . The initiating DOD Component prepares a concise threat summary and threat rationale, working with DIA/DWO as needed. If validated CTAs or STARs/STAs are available and address the threat areas affecting the U.S. capability, these documents should be used as the primary sources for the threat statements. Programs designated as ACAT ID MDAPs, or programs with the potential to be so designated, must use DIA-

validated threat references.

Information Support Plan (ISP). Per DoDI 4630.8 and CJCSI 3312.01B, DIA/DWO reviews program generated ISPs during the Intelligence Certification process. A threat summary or section is not required in the ISP format; however, if used should reference the current and applicable CTA or STAR/STA.

Additional Criteria . The certification also evaluates intelligence-related systems with respect to open system architecture, security, and intelligence interoperability standards. (J-6 Interoperability certification is conducted in a separate, but related process, and is documented in [CJCS Instruction 6212.01](#) .)

Those personnel with a SIPRNET terminal can access the specific procedures and criteria for the Intelligence Certification on the Intelligence Requirements Certification Office homepage (under "Certification Process"). By telephone, additional information may be obtained by calling the Intelligence Requirements Certification Office at 703-571-9543 (Mr. Vernon Wilson) or 703-571-9541 (Mr. Dana Smith).