CH 7–1. Purpose
The Defense Acquisition Guidebook (DAG), Chapter 7, provides guidance to Program Managers (PMs) on how to use intelligence information and data to ensure maximum warfighting capability at a minimum risk to cost and schedule.

CH 7–2. Background
Intelligence is a key factor in understanding the current and future threat posed by foreign weapon and information technology system capabilities, and should therefore affect United States (U.S.) weapons and information technology system acquisition decisions. For systems to achieve their intended capabilities, consideration of the threat must be constantly reviewed and considered throughout the life cycle of each system. Threat and intelligence support considerations should affect all decisions from defining requirements and capabilities, through initial concept phases, planning, research, full-scale development, production, test and evaluation, deployment, and system upgrade, all the way through disposal: cradle to grave. Threat analysis and intelligence support requirements inform and enable program capabilities and minimize costs to the government throughout the entire acquisition process.

While the dialogue between the Defense Intelligence Enterprise (DIE) and acquisition community bridges the cultural divide or stovepipes, that same dialogue is no less important between the requirements and intelligence communities. The requirements developer should call on the supporting intelligence SME at the earliest stages of development for assistance in determining if the requirements being developed will involve intelligence support, especially IMD. The determination and statement of the intelligence support requirements, or lack thereof, are recorded and transmitted to the acquisition program manager in each capability document.

CH 7–2.1 Expected Benefits
The integration of intelligence has become increasingly critical to DoD acquisition programs. Threat intelligence analysis and/or intelligence supportability requirements inform the acquisition community and enable weapon system capabilities. They also minimize risk and cost to the government throughout the entire acquisition process.

Early determination of intelligence supportability requirements increases the likelihood that the delivered system will be fully capable and more survivable against the relevant adversary threats. It also reduces risk to acquisition cost, schedule, and performance through the early identification of threat capabilities and the work to be performed by the DIE; it also reduces risk to proper tasking of the DIE at the appropriate acquisition milestone through production requirements, identification of capability gaps, risk considerations, mitigation steps, and negotiated delivery dates for products.

CH 7–3. Business Practice
The importance of determining at the earliest possible time that an acquisition program has intelligence supportability requirements cannot be overstated. As stated earlier, the engagement to determine intelligence support starts with the Sponsor and the supporting intelligence SME.

CH 7–3.1 Intelligence and Requirements
The JCIDS Manual (Appendix I to Encl. D) provides a general description of the nine intelligence support requirement categories to assist the Sponsor and stakeholders in identifying intelligence support requirements and sufficiency or risk of shortfalls in the DIE needed to support a materiel capability solution.
CH 7–3.1.1 Early Intelligence and Requirements Engagement

The JCIDS Manual (paragraph 1.a.(2)) states that it is crucial for the Sponsor to identify intelligence support requirements, particularly IMD dependency, in all capability requirement documents or state there are no such requirements. Therefore, the Sponsor should engage the supporting intelligence SME to assist in determining whether or not a materiel capability solution is IMD-dependent and/or involve other intelligence supportability requirements. The acquisition PM is the beneficiary of this determination and is not responsible for making the determination. If the capability requirement documents identify intelligence supportability requirements, the Sponsor should establish a line of communications among the Sponsor, acquisition PM, and operator, and their respective supporting intelligence SMEs.

CH 7–3.1.2 Advantages of Early Intelligence and Requirements Engagement

The communication between these communities, especially with the supporting intelligence SMEs, should improve efficiency and effectiveness and minimize errors in identifying and requesting adequate intelligence support to acquisition. For example, without greater integration of threat and intelligence within the program structure, the program runs the risk of being out of sync with changes in the threat of record or of a new threat materializing, increases risk during Developmental Operational Test and Evaluation, and ultimately risks system failure when operationally deployed.

CH 7–3.2 Capability Requirements and Intelligence

The Joint Staff provides review, coordination, and certification/endorsement functions in support of the JCIDS process. These functions include intelligence supportability requirements for intelligence certification, and threat validation. All acquisition programs that are expected to operate in a threat environment should be developed in accordance with the most current threat information. The applicable threat information should be continually updated to account for threats throughout the acquisition program’s life cycle. The supporting intelligence SMEs to the Sponsor should be invaluable in incorporating adversarial threat capabilities throughout the JCIDS review process, and will review and validate the threat input within the JCIDS documents.

CH 7–3.2.1 Documents and Intelligence Collaboration

This section addresses the capabilities documents that identify intelligence supportability requirements. It also describes the intelligence certification process regarding intelligence support within an acquisition program.

CH 7–3.2.1.1 JCIDS Documentation

The Sponsor’s supporting intelligence SME should help drive the threat(s) of record in support of JCIDS document development. The supporting intelligence SME should also review all ICDs, CDDs, and CPDs - - as well as Joint ICDs, CDDs, and CPDs, which involve their service equities -- during the JCIDS document-staffing process to ensure that the threat information and the addressing of the nine JCIDS intelligence support categories meet JCIDS requirements. Furthermore, the supporting intelligence SME should assist the Sponsor in identifying key performance parameters, key system attributes, and additional performance attributes that are threat-dependent and require Critical Intelligence Parameters (CIPs) in the threat and capabilities sections of the applicable JCIDS documents. Defense Intelligence Agency (DIA) provides CIP best practices and a development template at the following SIPRNet site: https://intellipedia.intelink.sgov.gov/wiki/Critical_Intelligence_Parameter.

Initial Capabilities Document (ICD). The initiating DoD Component prepares a concise threat summary and threat rationale. If validated Threat Modules or Validated Online Lifecycle Threat (VOLT) Reports (see Sections 4.1.1 and 4.1.2) are available and address the threat areas affecting 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. If validated Threat Modules or VOLT Reports are available and address the threat areas affecting U.S. capability, these documents should be used as the primary sources for the threat statements.

**Capability Production Document (CPD).** The initiating DoD Component prepares a concise threat summary and threat rationale. If validated Threat Modules or VOLT Reports are available and address the threat areas affecting U.S. capability, these documents should be used as the primary sources for the threat statements.

**CH 7–3.2.1.2 Validated Online Lifecycle Threat (VOLT) and Threat Modules**

Deleted.

**CH 7–3.2.1.3 Intelligence Certification Process**

The Intelligence Certification Process involves the evaluation of threat documentation and the nine JCIDS intelligence support categories with respect to system architecture, security, and intelligence interoperability standards.

The J28 Intelligence Requirements Certification Office (IRCO) acts on behalf of the DJ-2 and the J-2/DDJ28 as the lead intelligence entity within the Joint Staff for intelligence certification of capability requirement documents. It provides intelligence certification of capability requirement documents. See CJCSI_5123.01G (para 2.c.(5), Encl. B) for details on IRCO. The IRCO engages members of the DIE during intelligence certification. The IRCO can be contacted for assistance at (757) 836-7030 or through SIPRNet channels (https://intelshare.intelink.sgov.gov/sites/IRCO/SitePages/Home.aspx).

**CH 7–3.2.2 Advantages of Capability Requirements and Intelligence Collaboration**

The early identification of IMD dependency and/or other intelligence supportability needs in the requirements process will inform identification of potential gaps or shortfalls in intelligence support to an Acquisition Category (ACAT) program, particularly, IMD. This early identification should allow the DIE, PM, and eventually the operator time and flexibility in addressing any recognized gap or shortfall in intelligence support.

**CH 7–4. Additional Planning Considerations**

Threat support and the nine JCIDS intelligence support categories play an increasingly significant role in the successful development of the U.S. capabilities that provide an advantage on the battlefield. This section addresses the capabilities and intelligence documents required by DoDI 5000.02, Encl 1, sec. 3 (Table 2) and their linkages to the Acquisition, Intelligence, and Requirements communities.

**CH 7–4.1 Threat Support**

Threat Intelligence support to the acquisition process provides an understanding of foreign threat capabilities. It should be continually updated to account for upgrades to adversarial capabilities throughout the program to ensure that the technological advantage over adversarial capabilities is maintained. See the graphic in Figure 1.

Figure 1 illustrates the range of support provided by the threat intelligence community over the life of a particular capability shortfall identification process and the resulting system acquisition program. The Defense Intelligence Threat Library (DITL) informs the capability shortfall identification process as well as during the early phases of system acquisition prior to the generation of the VOLT. The Threat Modules in the DITL project foreign capabilities in particular threat areas looking out 20 years.

**Figure 1: Life-Cycle Intelligence Analysis Requirements**
At the beginning of the Material Solution Analysis phase, the Sponsor should contact the supporting intelligence production center (IPC) to support the integration of validated threat information into the technology development approach in the Analysis of Alternatives (AoA). Threat information may come from DIA-validated Threat Modules or other DIA/Service-validated VOLTs that align with the capability mission, concept of operations (CONOPs), and employment timeline.

Once the Sponsor, PM, or other appropriate enabler identifies concepts or prototypes for the materiel solution, the program office or Sponsor should task the supporting IPC for the lead Service to produce a VOLT Report. The program office should work closely with the supporting IPC to provide system-specific characteristics, employment CONOPS, and employment timeline as they evolve. The program office should also work with the Sponsor and VOLT Report validation authority to identify CIPs and ensure that DoD IC production requirements are levied against those CIPs.

**CH 7–4.1.1 Threat Modules**

*DoDI 5000.02, Encl 1, sec. 3* (DITL (Threat Modules) row, Table 2) describes the Threat Modules as regulatory documents that are produced by the DIE and are required to be updated every 2 years, independent of acquisition decision events. Threat Modules serve as the analytical foundation for VOLT Reports and maintain projections of technology and adversary capability trends over the next 20 years.

The Threat Modules are defined as comprehensive, authoritative, and validated assessments of foreign threats, relative to ACAT I-III programs. Modules project the threat environment in a given threat topic out 20 years and constitute the DIE position with respect to those topics. The modules fall under the following
seven categories: Chemical, Biological, Radioactive, and Nuclear; counter sensor; cyberspace; employment/CONOPS; platform/target; sensor; and weapons. The DITL is available on SIPRNet at the following DIA page: https://intellipedia.intelink.sgov.gov/wiki/TLA-3.

CH 7–4.1.2 VOLT Report

DoDI 5000.02, Encl 1, sec. 3 (VOLT Report row, Table 2) lists the VOLT Report as a regulatory document for ACAT I-III programs. These programs 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 initial operational capability (IOC).

VOLT Reports are required for all other programs unless waived by the Milestone Decision Authority (MDA). Programs on the Director, Operational Test, and Evaluation (DOT&E) Oversight List require a unique, system-specific VOLT Report, unless waived by both the MDA and the DOT&E. DoD Components produce a VOLT Report. DIA validates the VOLT Report for ACAT ID or IAM programs; the DoD Component validates the VOLT Report for ACAT IC or IAC programs and below. For ACAT ID or IAM programs, DIA contact information and the VOLT Report request form are available at the following SIPRNet page: https://intellipedia.intelink.sgov.gov/wiki/TLA-3.

The VOLT Report is defined as the authoritative threat assessment tailored for and normally focused on one specific ACAT I, II or III program and authorized for use in the Defense Acquisition Management process. The VOLT Reports involve the application of threat modules, and are to be written to articulate the relevance of each module to a specific acquisition program or planned capability. At the discretion of the responsible MDA, VOLT Reports can be used in the future to support multiple programs that address like performance attributes, share an employment CONOPs, and have a similar employment timeline.

CH 7–4.1.3 Life-Cycle Mission Data Plan

DoDI 5000.02, Encl 1, sec. 3 (LMDP row, Table 2, Encl. 1) lists the LMDP as a regulatory requirement for all ACAT programs if the system is dependent on IMD. The LMDP is a Milestone A requirement and a Program Executive Officer and Component Acquisition Executive-approved draft update is due for a Development Request for Proposal Release. The DoD Component approves the draft update at Milestone B.

CH 7–4.1.3.1 “V” Process

Figure 2 depicts the five phases of the LMDP process, called the “V” process. In Phase I, the PM, in collaboration with the Sponsor, identifies all known IMD requirements. Phases II-IV involve the DIE lead; the description of these phases is in Section 4.1.3.2 below. In Phase V, the Sponsor determines which shortfalls should be addressed, the appropriate course(s) of action to mitigate risk, and the risk associated with the remaining IMD shortfalls. Supplemental 001, Life-Cycle Mission Data Plan (LMDP) and Intelligence Mission Data (IMD) planning, of this chapter provides details of the LMDP process.

Figure 2: Five Phases of the LMDP Process
CH 7–4.1.3.2 Intelligence input to the “V” Process

Phases II-IV involve intelligence input from the IMD Center (IMDC) and Service IPCs. In Phase II, the IMDC evaluates the submitted LMDP IMD requirements list for sufficiency and determines which IPCs should assess each IMD request. In Phase III, the IPC assesses any gaps associated with each IMD request and estimates the shortfall costs. In Phase IV, the IMDC identifies common IMD requirements across ACAT Programs and Services. The IMDC also analyzes the shortfalls and provides consolidated feedback to the appropriate PM.

CH 7–4.1.4 System Threat Assessment Report (STAR)

Deleted.

CH 7–4.1.5 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 DOT&E or the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), DIA, working with the DIE, should provide additional intelligence support to the operational testing of programs on the annual DOT&E Oversight List. DIA support should include certification that the threat information in the test plan is correct and consistent with existing assessments.
Per DoDI 5000.02, Encl 1, sec. 3 (VOLT Report row, Table 2), programs on the DOT&E Oversight List require a VOLT Report regardless of ACAT designation. Details on the VOLT Report are available at paragraph 4.1.2 of this chapter.

CH 7–4.2 Intelligence Mission Data Support

DoDI 5000.02 (LMDP row, Table 2) lists the LMDP as a regulatory document and is required only if the system is dependent on IMD. DoDD 5250.01 (glossary) defines IMD as DoD intelligence used for programming platform mission systems in development, testing, operations, and sustainment, including, but not limited to, the functional areas of signatures, electronic warfare integrated reprogramming (EWIR), order of battle (OOB), characteristics and performance (C&P), and geospatial intelligence (GEOINT).

CH 7–4.2.1 IMD Functional Areas

The JCIDS Manual (para 2.e., Appendix I, Encl. D) addresses these functional areas as follows:

CH 7–4.2.1.1 Signatures

Signatures are defined as the distinctive characteristics, or sets of characteristics, that consistently recur and identify a piece of equipment, materiel, activity, or event. Signature support is the provision of such data to capability solutions that use signatures in their design, development, testing, training, or operations of sensors, models, or algorithms for the purpose of: combat identification; blue force tracking; targeting; or detecting or identifying activities, events, persons, materiel, or equipment.

CH 7–4.2.1.2 EWIR

EWIR involves assessed, all-source intelligence data on adversary and non-adversary commercial systems, to include technical parametric and performance data, observed electronic intelligence data on foreign emitters from the National Security Agency, and engineering-value/measured data on domestic emitters.

CH 7–4.2.1.3 OOB

OOB is the identification, command structure, strength, and disposition of personnel, equipment, and units of an armed force.

CH 7–4.2.1.4 C&P

C&P refers to all-source derived assessments of foreign military system capabilities and physical attributes.

CH 7–4.2.1.5 GEOINT

GEOINT provides programs with mapping, charting and geodesy, geospatial information, imagery intelligence, and other GEOINT data, data products, and services to support operations, navigation, terrain visualization, targeting, and the characterization of the physical and manmade environments.

CH 7–4.2.2 Consideration of IMD

The JCIDS Manual (para 2.e.(2), Appendix I, Encl. D) further states that IMD requirements “must be considered” as early as the AoA when one or more of the alternatives under consideration are likely to be dependent on IMD to ensure mission effectiveness. Consideration is to be given for alternatives that are not IMD-dependent or those that can be satisfied by IMD already produced by the DIE. Alternatives requiring additional IMD production by the DIE should only be considered where the value of the additional mission effectiveness exceeds the cost associated with generating and maintaining the additional IMD.
CH 7–4.2.3 Reference Sources on IMD

DoDD 5250.01 and the DIA Intelligence Mission Data SharePoint Site (SIPRNet – http://intelshare.intelink.sgov.gov/sites/imdc/imdppublicshare/default.aspx) provide details on IMD.

CH 7–4.3 Counterintelligence Support

Counterintelligence (CI) support involves the gathering of information and conduct of activities to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

Military Department Counterintelligence Organizations (MDCOs) include the Army's 902nd Military Intelligence Group, Navy Criminal Investigative Service and Air Force Office of Special Investigations.

These MDCOs produce Multi-Discipline CI Threat Assessments (MDCITAs), which focus on the foreign collection threat to critical program information (CPI) in Joint and Service ACAT programs and feed into the process for the identification and selection of measures for the protection of CPI. The MDCITA is a key element of the Program Protection Plan (PPP). These MDCOs also address the Targeting Technology Risk Assessment (TTRA), which is another CI threat assessment focusing on CPI and a milestone requirement. See Section 4.3.2 for details on the TTRA.

The other principle CI product the MDCOs provides to acquisition is the Counterintelligence Support Plan (CISP). The CISP describes the planning for the execution of CI activities for acquisition programs with CPI, to include Cleared Defense Contractors considered essential by an acquisition program manager where CPI is present. An acquisition PM could also request, with justification, a CISP for a program that does not identify CPI. Details on the CISP are available in Chapter 9.

The Defense Security Service coordinates the execution of a DoD Component CISP at cleared defense contractor facilities with CPI, develops and provides training for DoD and defense contractor security personnel regarding CPI protection activities required by (or in) classified contracts and provides unclassified and classified all-source analyses, to include, but not limited to, annual analyses of suspicious contacts and activities occurring with the defense contractor community that could adversely affect the protection of CPI. These reports are disseminated to the defense contractor community and DoD Component heads.

CH 7–4.3.1 Program Protection Plan

DoDI 5000.02, Encl 1, sec. 3 (PPP row, Table 2, Encl. 1) lists the PPP as a regulatory requirement at Milestones A through C. It is a risk-based, comprehensive, living plan to guide efforts to manage the risks to CPI and mission-critical functions and critical components. The full range of security functions and counterintelligence traditionally dominate program protection planning for the protection of CPI and critical components. Details on the PPP are available in Chapter 9.

CH 7–4.3.2 Technology Targeting Risk Assessment (TTRA)

DoDI 5000.02, Encl 1, sec. 3 (TTRA row, Table 2, Encl. 1) lists the TTRA as a Milestone A requirement document for all ACAT I-III programs. It is a country-by-country assessment conducted by the DoD entities within DIE that quantifies risks to CPI and related enabling technologies for weapons systems; advanced technologies or programs; facilities such as laboratories, factories, research and development sites (e.g., test ranges); and military installations. The TTRA evaluates five independent risk factors, each of which contributes to an overall risk factor. The five areas evaluated are: 1) technology competence; 2) national level of interest; 3) risk of technology diversion; 4) ability to assimilate; and, 5) technology protection risk.

The MDCITA, or CI Threat Assessment, is a comprehensive analysis or study that focuses on the foreign intelligence collection threat to the CPI of a DoD ACAT program. It is a key required element of the PPP,
which is the comprehensive plan that describes the integration and synchronization of all measures selected for the protection of CPI.

DoDI 5000.02, Encl 1, sec. 3 (TTRA row, Table 2, Encl. 1) states that the TTRA forms the analytic foundation for the CI assessments (MDCITAs) in the associated PPP. Since the TTRA is a Milestone A only requirement document, if the PM identifies CPI prior to Milestone A, DoDI O-5240.24 (para 3.b, App 1 to Encl 3) states that the “supporting Defense CI Component” will coordinate with the Director, DIA, for the production of the TTRA. Additionally, the instruction further states that the “supporting Defense CI Component” merges the TTRA with the appropriate CI analytical product (MDCITA) and provides the single-source document to the requesting PM. DoDI O-5240.24 is available at the following SIPRNet site: https://www.dtic.mil/whs/directives/corres/pdf/O524024p.pdf.

CH 7–4.4 Intelligence Manpower Support

The JCIDS Manual para 2.a., Appendix I, Encl. D) states that this category is to be addressed if the capability solution will require intelligence personnel for development, testing, training, and/or operation. The PM should address how the existing intelligence manpower resources will meet the capability solution’s intelligence support requirements or whether the capability solution will require additional, dedicated intelligence personnel. Details on the manpower estimate are available in Chapter 5.

CH 7–4.5 Intelligence Resource Support

The JCIDS Manual para 2.b., Appendix I, Encl. D) states that the intelligence resource support category should address whether intelligence funding should be a consideration driven by the IMD dependency and/or the intelligence supportability requirements of the capability solution. Sponsor and PM should devote special attention to the requirement for IMD early in the capability life cycle, including the consideration of resourcing for IMD production prior to Milestone A. The Sponsor and PM should also be aware of intelligence funding which includes two components, the National Intelligence Program (NIP) and Military Intelligence Program (MIP). The NIP includes all programs, projects and activities of the intelligence community. The MIP is devoted to intelligence activity conducted by the military departments and agencies in the DoD that support tactical U.S. military operations.

In the event that the Sponsor and/or PM identifies unique or specialized intelligence supportability requirements for the ACAT program, the Sponsor and/or PM should collaborate with their respective supporting intelligence SMEs to determine or negotiate the source of the funding for such requirements.

CH 7–4.6 Intelligence Planning and Operations Support

The JCIDS Manual para 2.c., Appendix I, Encl. D) states that intelligence planning and operations support requirements involve six interrelated elements in the Joint Intelligence Process, or what is traditionally termed the “intelligence cycle.” These six elements are planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. While not specifically an intelligence requirement, adequate consideration should be given to the requirements of data transport, especially of airborne intelligence and reconnaissance and surveillance platforms -- an area that has experienced tremendous growth over the past decade.

CH 7–4.6.1 Planning and Direction

This category includes the receipt, identification, and prioritization of intelligence requirements; the development of concepts of intelligence operations and architectures; tasking appropriate intelligence elements for the collection of information or the production of finished intelligence; and submitting requests for collection, exploitation, or all-source production support to external, supporting intelligence entities.

Sponsors must address whether mission-planning requirements have been considered and identified, to include manpower, systems, tools, mission-planning data (Red, Gray, Blue, and White), or other non-
materiel requirements of intelligence units, personnel training on systems architecture, and compatibility with current and future Defense Intelligence Information Enterprise architecture.

Joint Publication (JP) 2-01 (Section A) provides additional information on planning and direction.

**CH 7–4.6.2 Collection**

Collection includes those activities related to the acquisition of data needed to satisfy specified requirements. This is managed by collection managers, whose duties include selecting the most-appropriate, available asset(s) and associated processing, exploitation, and dissemination (PED) and then tasking selected asset(s) and associated PED to conduct collection missions.

Collection-management support refers to the personnel, expertise, training, and systems required to ensure that intelligence information requests are submitted through the appropriate channels; that intelligence-collection assets (e.g., Service, national, joint, coalition, and multinational) are effectively employed to collect the required information; and that the collected information is disseminated to the entity that made the original request and to all other end users requiring this information.

The JCIDS Manual (para 2.c.(2), Appendix I to Encl. D), and JP 2-01 (Section B) provide additional details on collection.

**CH 7–4.6.3 Processing and Exploitation**

Data initially received from the sensor arrives in various forms, depending on the nature of the sensing device. Depending on the source, the raw input may be in the form of digitized data, unintelligible voice transmissions, or large digital files containing un-rectified images of the Earth. This collection output is converted by sensor-specific processing measures into visual, auditory, or textual information that is intelligible to humans, and can then be used by intelligence analysts and other consumers. The data conversion may be automated using algorithmic fusion, cuing, data analytics, and automated exploitation. Exploitation entails the further translation and contextualizing of information resulting from collection and initial processing into a product the planner, decision-maker, or intelligence analyst can assimilate cognitively.

The Sponsor should address whether sufficient personnel and resources will be in place for effective processing and exploitation. Whenever possible, the Sponsor should also address required data, coverage, scale, timeliness, formats, accuracy, and resolution level. The Sponsor should then consider whether the intelligence architecture will support the volume of data requiring processing and ensure data is in standard formats to support interoperability. Depending on the specific requirements of Sponsor’s capability solution being supported, you will consider the types of delivery/communications systems required and the volume of information that will be delivered.

The JCIDS Manual (para 2.c.(3), Appendix I to Encl. D), and JP 2-01 (Section C) provide additional information on processing and exploitation.

**CH 7–4.6.4 Analysis and Production**

During analysis and production, intelligence is produced from the information gathered by collection capabilities, and from the refinement and compilation of intelligence received from external organizations. All available processed information is integrated, evaluated, analyzed, and interpreted to create products that will satisfy requesters or users.

Intelligence products are generally placed in one of eight production categories: 1) warning; 2) current; 3) general military; 4) target 5) science and technology 6) CI; 7) identity intelligence and, 8) estimative intelligence. The categories are distinguished from each other primarily by the purpose for which the intelligence was produced.
The Sponsor should address the necessary or desired product format, production timeline; and necessary update requirements that will be available and have been requested to support their capability solutions. Consider whether sufficient personnel and resources will be in place for effective analysis and production.

The JCIDS Manual (para 2.c.(4), Appendix I to Encl. D), and JP 2-01 (Section C) provide additional information on analysis and production.

**CH 7–4.6.5 Dissemination and Integration**

This category involves the timely distribution of critical information and finished intelligence, readily accessible by the user, to the appropriate consumer. The movement toward a net-centric environment has reduced the technical challenges related to information dissemination. Nevertheless, intelligence infrastructure (such as intelligence networks, systems, and software) and intelligence resources -- such as funded programs or manpower -- remain critical (and necessary) components of information delivery.

This category should encompass the specific requirements of the capability solution being supported, which may include: timeliness and means of delivery; interoperability of delivery/communications systems; format of information delivered; and information/product storage location, capacity, and accessibility.

The JCIDS Manual (para 2.c.(5), Appendix I to Encl. D), and JP 2-01 (Section C) provide additional information on dissemination and integration.

**CH 7–4.6.6 Evaluation and Feedback**

Evaluation and feedback occur continuously throughout the intelligence process, and as an assessment of the intelligence process as a whole. Intelligence personnel at all levels, as well as users of intelligence, should assess the execution of the intelligence tasks being performed to identify deficiencies within the intelligence process and to determine if intelligence requirements are being satisfied. The goal of evaluation and feedback is to identify issues as early as possible to minimize information gaps and to mitigate capability shortfalls.

When possible, this category should address capability solution requirements for means, formats, information needs, and periodicity of assessments to support decisions about reprioritization of intelligence requirements, shifts in collection emphasis, changes to analytic levels of effort, reallocation of available intelligence assets, training of intelligence personnel, and the development of new intelligence capabilities.

The JCIDS Manual (para 2.c.(6), Appendix I to Encl. D), and JP 2-01 (Section C) provides additional information on evaluation and feedback.

**CH 7–4.7 Targeting Support**

The JCIDS Manual (para 2.d., Appendix I, Encl. D) describes targeting as the process of selecting and prioritizing targets and matching the appropriate response to them, considering commander’s guidance and objectives, planning requirements at all warfare levels, and operational requirements and capabilities. Intelligence targeting support shortfalls may detrimentally affect the capability solution’s successful development, on-time delivery schedule, and, ultimately, its operational status.

This targeting support category should address requirements for support to target development, mission planning, precise positioning, bomb damage assessment, munitions effects assessment, weaponrying, the anticipated volume of targets to be managed and the numbers of target folders to be produced, and associated targets or aim points to plan for during mission planning.
CH 7–4.8 Warning Support

The JCIDS Manual (para 2.f., Appendix I, Encl. D) characterizes warning support as a traditional intelligence mission of “Indications and Warning” – identifying and defining a potential threat and then monitoring it. However, in terms of intelligence support to acquisition, warning support should focus on the information that enables that system capability to remain scientifically and technologically superior to developing or projected adversary capabilities. This support depends on the identification of CIPs by the Requirements Developer and PM, in collaboration with their support intelligence SME. A CIP represents a threat capability or threshold and changes to which could critically impact the effectiveness and survivability of a proposed system (CIP breach).

The JCIDS Manual (para 2.c.(3)(c), Encl. B) states that when a Service IPC monitoring CIPs determines that an approved CIP has been breached, notification of the breach will be made to appropriate offices in DoD, and the program office(s) and Functional Capabilities Board(s) impacted by the breach. Additionally, the matrix support intelligence SME should establish a continuous line of communications with the respective Service IPC to ensure that the program receives appropriate notification of a CIP breach affecting its system capability.

CH 7–4.9 Space Intelligence Support

The JCIDS Manual (para 2.g., Appendix I, Encl. D) states that space intelligence support involves requirements for space-based capability solutions; other capability solutions relying on space-derived capabilities; and platforms that perform space control or space support. This category also includes intelligence information, infrastructure, or resources that provide space-specific intelligence analysis on foreign space capabilities.

The space intelligence support category should also address requirements for space intelligence coverage, whether periodic or persistent; timeliness; security; form of support necessary; and accuracy.

CH 7–4.10 Intelligence Training Support

Historically, some acquisition programs have required specific support in terms of specialized training conducted by intelligence SMEs during part or all of an ACAT program’s life cycle.

Such specialized training requirements may include training additional personnel in existing training programs and/or in a new, unique training program that will be developed to support the ACAT program. In either case, the requirement for specific training to support part or all of an ACAT program’s life cycle should be identified as early as possible in the acquisition process. For non-MDAPs, the PM should ensure that a close coordination relationship exists with the program matrix support intelligence SME, as well as with the requirements developer and requirements support intelligence expert. This close relationship should foster the early identification of any unique or specialized intelligence training requirement throughout the ACAT program’s life cycle.

Chapter 7 Supplement—Life-Cycle Mission Data Plan

CH 7-S–1. Overview

Modern weapon systems are inherently dependent on a variety of scientific and technical intelligence products throughout every stage of their life-cycle. Intelligence Mission Data (IMD) provides essential data for building system models, developing algorithms, optimizing sensor design, system testing and evaluation (T&E), and validating sensor functionality. Therefore, it is important for systems to consider IMD as a potential cost, schedule or performance risk and initiate IMD planning as early as possible in the acquisition process. Ideally, IMD considerations will inform technology transition decisions and development planning efforts in advance of entrance into the Joint Capabilities Integration and Development System process and Defense Acquisition System.
The Defense Intelligence Enterprise (DIE) resources are known to be limited in ability to support the full range of existing IMD requirements; therefore, programs will gain greater insight into their potential IMD risk if they define their requirements with sufficient detail to receive a DIE assessment of availability and data cost. Systems that are designed to fully leverage what is already available or is planned to be available from the DIE will carry less risk from IMD shortfalls.

**DoDD 5250.01** establishes direction for life-cycle IMD planning to include, but not limited to, the following functional areas: Signatures, Electronic Warfare Integrated Reprogramming (EWIR), Order of Battle (OOB), Characteristics and Performance (C&P), and Geospatial Intelligence (GEOINT). Notably, it creates the Intelligence Mission Data Center (IMDC) as a resource to support IMD efforts DoD-wide.

**DoDD 5250.01** and **DoDI 5000.02, Encl 1, sec. 3** (LMDP row, Table 2, Enclosure 1) require all IMD-dependent technology and acquisition programs and efforts to submit an LMDP throughout their respective life-cycle. The LMDP facilitates collaboration and coordination between the acquisition, requirements and intelligence communities for how the system will be supported with IMD across its life-cycle. Supporting intelligence offices assist programs with the development of LMDPs, coordination with IMD producers and resolving issues associated with IMD. They also facilitate assistance from the IMDC.

**CH 7-S–1.1. Purpose**

The purpose of this supplement is to describe the process for the development of the LMDP.

**CH 7-S–1.2. Summary of the Supplement**

This supplement depicts the step-by-step process related to the addressing of the IMD requirements in support of the development of the LMDP. Since the LMDP is IMD dependent, this supplement provides questions to be addressed and actions to be taken at each milestone and at various phases of the life cycle of the acquisition program.

**CH 7-S–2. LMDP Process**

The life-cycle mission data planning process follows the systems engineering "V" process to define, assess and manage IMD needs, timelines, gaps and risks. This collaborative planning process enables programs along with the requirements community to identify how the system will be supported by the DIE with IMD necessary to meet acquisition program development and test timelines as well as the full range of support necessary to conduct operations and sustainment. The results of this planning process are captured in the system’s LMDP.

Supporting intelligence offices guide programs in specific formats/processes for LMDP development, coordination and approval within each Service. Additionally, IMDC recommended formats for the LMDP can be found on the IMDC SharePoint sites and Defense Acquisition University’s website. The IMDC has developed a tool, the “IMD Management, Analysis and Reporting System (IMARS)” to facilitate the identification, assessment and analysis of IMD requirements.

The following steps and acquisition phase aligned questions can assist a program with identifying IMD requirements and incorporating IMD planning into program execution:

- The first step in the LMDP development process is the systems engineering level analysis of system attributes to derive of IMD requirements. This analysis should be conducted by program office systems engineers in collaboration with intelligence personnel who can trace attributes to relevant intelligence products and services. Once IMD data dependencies are identified, supporting intelligence offices can facilitate their submission to the Service Intelligence Production Centers (IPCs) and IMDC for review and feedback.
- Once these organizations have received a system’s list of IMD requirements, Service IPCs review their IMD holdings against the required IMD based upon specific data accuracy/fidelity needs. Where gaps are found, the IPCs use a Cost Assessment and Program Evaluation or CAPE
compliant costing methodology to articulate costs for closing data gaps.

- The IMDC facilitates provision of Service IPC costing and availability assessments to the supporting intelligence office and the program along with insights into other programs with similar gaps.

Programs, along with requirements sponsors can then apply acquisition and operational risk assessment methodologies and determine appropriate courses of action that address identified IMD gaps and aid in prioritization of their IMD requirements. This supports identification of relative IMD priorities and risk mitigation for use in IMD planning.

**CH 7-S–2.1. Materiel Solution Analysis Phase to Milestone (MS) A**

A program’s strategy document (Acquisition Strategy (AS)) is an appropriate place to identify the (a) systems and subsystems of the program that require IMD necessary to deliver the intended capabilities; and (b) IMD funding requirements as appropriate.

Since final material solutions are yet to be approved prior to MS A, specific system configuration and detailed IMD requirements are generally not known. However, based on the intended operational mission, the program should identify the likely IMD type(s) (e.g. Radar, Thermal, Acoustic, Electronic Warfare Integrated Reprogramming (EWIR), Geospatial Intelligence (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 can be identified.

IMD requirements and related implications to design, performance, and T&E, are best 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 affect 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, electro-optical/infrared (EO/IR), acoustic, chemical, etc.), assess the technical feasibility of acquiring IMD within cost and schedule constraints. Consider the quality of available IMD, the capability of the DIE to deliver IMD and whether the IMD needs to be collected, processed and/or developed.

**Actions:**

- Consider IMD during development of the preliminary system specification, system functions that will likely drive the need for IMD, either directly or through derived requirements.
- Consider potential IMD requirements during development of mission and functional threads.

Consider IMD requirements during development of T&E strategies and plans based on the need to verify and validate detection and identification functionality. Characterize associated technical risk in the T&E Strategy. Estimate IMD delivery requirements to meet projected test schedules so that the program can articulate to the DIE their need dates for specified IMD.

**CH 7-S–2.2. Technology Development Phase to MS B**

As a program approaches MS B, the LMDDP can be expanded to include mission or capability specific details to support program development. For example, as the design matures, additional details should emerge about the design of the sensors and the algorithms. The LMDDP might also identify any IMD-based models and earlier submissions for IMD submitted to a Service IPC (National Air and Space
Intelligence Center, National Ground Intelligence Center, Office of Naval Intelligence, Missile and Space Intelligence Center, 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 MS A, refine and add details for the MS B LMDP during development of the Systems Performance Specification and the Allocated Baseline. Submit any new or refined IMD requirements to the Service IPCs and IMDC for costing and availability assessment and then update the LMDP with results of that assessment. Relative questions to consider and actions to take during this phase include:

Questions:

- Has the program been identified for FMS? If yes, then how will this affect design, development, testing, disclosure and releasability of IMD-dependent components?
- For each proposed detection/identification method (radar, 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 MS B?
- Which IMD-dependent performance requirements need to be verified through T&E?
- 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 program’s spectrum requirements taken into account bandwidth needed for IMD updates during system operations and sustainment?
- Should any IMD data sets be considered as Government Furnished Equipment 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 key performance parameters/key system attributes.
- Define system level functional and performance requirements derived from items such as: Concept of Operations (CONOPS), system-level performance metrics, mission threads/use cases, and usage environment. Document results and requirements in the System Requirements Document, LMDP, and Systems Engineering Plan (SEP) as appropriate.

Assess IMD requirements and schedule relative to Director, Operational T&E needs. Document results in the LMDP and by reference in the T&E Master Plan.

**CH 7-S–2.3. Engineering and Manufacturing Phase to MS C**

This LMDP will be an update to the previous LMDP. The purpose is to add any new IMD considerations resulting from design maturity or changes in the CONOPS. It should include expected IMD data flows for system employment in an operational environment. The LMDP 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 DIE. 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 at MS B, refine and add details for the MS C LMDP during development of the System Functional Specifications and the Initial Product Baseline. Relevant questions to consider and actions to take during this phase include:

Questions:

- Has the program been identified for FMS? If yes, then how will this affect 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 planned for in the LMDP and AS, at the level of quality needed?
- Which IMD requirements need to be verified in Follow-on T&E (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 LMDP and by reference in the updated TEMP.

**CH 7-S–2.4. Low-Rate Initial Production to Full-Rate Production/Full Deployment Decision Review to Disposal**

In preparation for initial operational capability, an LMDP 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 LMDP 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 for operational missions.

This LMDP should take into consideration relevant Combatant Command or operating unit 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 authorized by the Designated Disclosure Authority?
- Have IMD support requirements been addressed in the Operations and Support Phase?
- Does the current CONOPS for the system drive new or updated IMD requirements? Have these new/updated IMD requirements been handed off to the operational requirements prioritization processes?
- If the operational system has an IMD reprogramming process, is the reprogramming system and organization ready for operations?

Actions
• Coordinate the LMDP with the requirements sponsor.
• Confirm operations of the IMD reprogramming process.

CH 7–Version and Revision History
The table below tracks chapter changes. It indicates the current version number and date published, and provides a brief description of the content.

<table>
<thead>
<tr>
<th>Version #</th>
<th>Revision Date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2/1/17</td>
<td>Chapter 7 administrative changes</td>
</tr>
<tr>
<td>1</td>
<td>4/27/17</td>
<td>Chapter 7 administratively updated to coincide with DoDI 5000.02, CH 2, primarily establishing the VOLT and Threat Modules, and replacing the ITEA, CTA and STAR.</td>
</tr>
<tr>
<td>2</td>
<td>6/8/17</td>
<td>Chapter 7 link in paragraph 7-3.2.1.3 corrected and administrative changes made for clarification.</td>
</tr>
<tr>
<td>3</td>
<td>6/26/17</td>
<td>Chapter 7 SIPRNet links in paragraphs 7-3.2.1.3 and 7-4.2.3 corrected and inserted SIPRNet links in paragraphs 7-4.1, 7-4.1.1, 7-4.1.2, and 7-4.3.2. Inserted clarifying updates to paragraphs regarding CIPs in capability documents, TTRA, intelligence manpower, CIPs in warning support, and intelligence resources. Added information on Defense Security Service role in CI support and descriptions of National Intelligence Program and Military Intelligence Program funding.</td>
</tr>
</tbody>
</table>