DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

AFI14-111_AFGM2016-01
20 JUNE 2016

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: AF/A2
1700 Air Force Pentagon
Washington, DC 20330-1700

SUBJECT: Air Force Guidance Memorandum (AFGM) to Air Force Instruction (AFI) 14-111, *Intelligence Support to the Acquisition Life-Cycle*

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately changes AFI 14-111. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with AFI 33-360, *Publications and Forms Management*.

Critical Intelligence Parameters (CIPs). The most recent JCIDS Manual update along with Better Buying Power (BBP) 3.0 initiatives 3.2.2.1/3.2.2.2 and Directive Type Memo signed by USD(AT&L), state that the Service Requirements Sponsors, DoD Component Capability Developers and Intelligence Community representatives will collaboratively establish CIPs for validated capability requirements and acquisition programs. Within the Air Force structure, the Implementing Commands (AFMC and AFSPC) and the Operating Major Command (MAJCOM) representatives will together, as early as possible in the capability's lifecycle, determine which key performance parameters and key system attributes are threat sensitive. The MAJCOMs and Implementing Commands will collaboratively define CIP reporting thresholds for threat-sensitive KPPs and KSAs of a planned capability, and submit these CIPs to the Intelligence Community (IC) via Production Request (PR) through the National Air and Space Intelligence Center (NASIC) (T-0). This process is facilitated by Acquisition Intelligence professionals via Threat Steering & Threat Working Groups (T-1).

Configuration Steering Boards (CSBs). In addition to the BBP requirement for the development of CIPs, the status of CIPs will be briefed during annual AF CSBs (T-1). This is in response to AT&L's direction to "anticipate and plan for responsive and emerging threats." During the CSB, the program managers, with Intelligence Community support (SIPCs, supporting intelligence offices), will brief the CIPs and indicate the program's risks based on where the program is in the lifecycle and how close each CIP is to a breach (T-1). Due to the increased manpower pressed upon the intelligence community to meet the new demand, Acquisition Intelligence personnel should first focus on the ACAT I programs to ensure those programs can provide the appropriate level of positive reporting about threat and CIPs during major Acquisition and Requirements process events.

Intelligence Mission Data (IMD) PR. IMD dependent programs will articulate their program specific IMD requirements to the Intelligence Community via IMD Production Request(s) (T-1). Supporting intelligence offices will work with IMD dependent programs to support development of IMD PRs and submit them to the Intelligence Community for action (T-1). IMD PRs will provide insight to SIPCs of AF needs such that SIPCs can provide costing, availability and production estimates to the AF. Program requirements communicated as part of a multi-program IMD PR should not be duplicated or submitted independently from the multi-program requirement. IMD PRs will be submitted via COLISEUM to NASIC with a courtesy copy to the Intelligence Mission Data Center (IMDC) (T-1). Responses from SIPCs to IMD PRs will be used to support program and Operating Command risk assessments that will then be captured in the LMDP.

Life-cycle Mission Data Plan (LMDP). LMDPs, as an acquisition program plan, will not be used for the purpose of submitting program IMD requirements to the IMDC or SIPCs. This supports program development of the Lifecycle IMD Plan (LMDP) with consideration of intelligence costs, shortfalls/gaps, capability impact, and AF courses of action to mitigate those risks. The AF LMDP template is Attachment 1. The template will be routed through standard acquisition channels for review, following SAF/AQXC's Acquisition Matrix (Attachment 2). We recognize this approach is a slight variation from guidance provided by the IMDC to the Services. It is in the interest of efficiency and effectiveness that the AF process is modified to include an IMD PR that flows separately from the LMDP.

IMD Prioritization. IMD requirements for analysis and production of Order of Battle, Characteristics and Performance, EWIR and Signatures IMD types will be prioritized annually. AF/A2D will oversee the annual IMD prioritization process as executed by NASIC (T-0). MAJCOMs (includes Implementing Commands) will identify IMD priorities for integration into a consolidated AF IMD priorities list. This list will be formalized into a prioritized AF IMD PR for action by Service Intelligence Production Centers (SIPCs).

NASIC Production of System Threat Assessment Reports (STARs) and Validated Online Lifecycle Threat (VOLT). NASIC will produce ACAT ID and IAM STARs or VOLTs for Air Force led programs using DIA validated threat data in accordance with DIAI 5000.002 and the 8 Dec 15 interim guidance to DIAI 5000.002 (T-0). DIA will review and validate all NASIC produced ACAT ID and IAM STARs or VOLTs prior to publication and release. NASIC will produce ACAT IAC/IC/II/III STARs or VOLTs using current published validated, authoritative and official responses to tasked production requirements (T-1). NASIC/CC will provide AF validation, or delegate validation authority, for all NASIC produced ACAT IAC/IC/II/III STARs or VOLTs prior to release (T-1).

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon incorporation by interim change to, or rewrite of AFI 14-111, whichever is earlier.

ROBERT P. OTTO, Lt Gen, USAF
Deputy Chief of Staff, Intelligence,
Surveillance, and Reconnaissance

Attachments:
1. Glossary of References and Supporting Information
2. AF LMDP Template
3. SAF/AQ Acquisition Matrix

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Validated Threat—Current, published threat information that represents the DoD Intelligence Community (IC) coordinated position on an assessed threat. This is the primary source for regulatory system threat assessments in the acquisition process. The threat information must generally be less than 5 years old, meet DIA tradecraft standards, and be approved by DIA for use in system threat assessments.

AF Validated Threat—The AF Validated STAR is the primary source for regulatory system threat assessments in the acquisition process for ACAT IAC/IC/II/III programs. The threat information must generally be less than 5 years old, meet NASIC tradecraft standards, and be approved for use in system threat assessments. Authoritative Threat can be used in conjunction with Validated and Response to Tasked Threats for ACAT IAC, IC, ACAT II and ACAT III STARs.

Authoritative Threat—Current, published threat information that represents the Service Intelligence Production Center (IPC) position on an assessed threat. The threat information must generally be less than 5 years old, meet Service IPC tradecraft standards, and be approved by one or more NASIC Senior Intelligence Analysts (SIA), or other Service IPC equivalent, for use in system threat assessments.

Critical Intelligence Parameter (CIP)—A CIP clearly defines the performance threshold at which a foreign system may compromise mission effectiveness of the U.S system. Military doctrine, tactics, strategy, and expected employment of systems should be considered in the CIP. CIPs should be built around those specific quantity, type, force mix, system capabilities, and technical characteristics or performance thresholds of a particular foreign weapon (for example, radar cross-section, armor type or thickness, or acoustic characteristics) of greatest concern to the U.S. program office and IC. (DIAI 5000.002, Para 4.2.4.2)

Attachment 2

AIR FORCE LIFECYCLE MISSION DATA PLAN TEMPLATE

DEPARTMENT OF THE AIR FORCE

MEMORANDUM FOR: ***PEO***

FROM: *Program Office*

SUBJECT: *(Program Name)* Life Cycle Mission Data Plan (LMDP)

1. (*Program Name*) is preparing for its (*state milestone/decision requiring LMDP*) on (*date*). DoD Directive 5250.01, Management of Intelligence Mission Data (IMD) in DoD Acquisitions requires documentation of Life Cycle Intelligence Mission Data (IMD) requirements in the LMDP. Additionally, AFI 63-101/20-101 requires IMD requirements be reviewed and agreements for production be reaffirmed with the Intelligence Community, via the program's designated intelligence focal point prior to each Milestone Decision.

2. *(Coordinating Intel Office),* in coordination with *(Program Office)*, has determined that the program is IMD dependent.

3. The following identifies specific IMD needs/shortfalls/risks for *(program name)*:

a. **Overview and operational requirements:** To support lifecycle requirements as articulated in its requirements documents, the program is dependent upon the following types of IMD: *(list the types of IMD)*.

Standard DoD IMD Databases	Non-DoD/Commercial Databases*

Specific attention to these dependencies can be found in the following: *(Depending upon where the program is in its milestone review cycle, identify the appropriate JCIDS doc: CDD, CPD, etc.)*, dated: *(Below is an example of how the program might add detail to attention already paid to IMD planning within its requirements documents. There is no need to duplicate that documentation. Attention here should be on the connection between Intelligence Mission Data and program requirements.)*

i. Section 6 Development KPPs, KSAs and additional performance attributes
ii. Section 6 Table 6-3 Objective and Threshold Values
iii. Section 9 Intelligence Supportability
iv. Section 9.4 Intelligence Support to Operations
v. Section 9.6 Intelligence Support Shortfalls

b. **System technical requirements, schedule, releasability, availability and cost:**

i. COLISEUM Production Requirements (PRs):

1. *(List PR numbers as submitted to the Intel Community for Signatures, Electronic Warfare Integrated Reprogramming, Order of Battle and Characteristics and Performance. Add classification marking if the PR title is classified and included. Programs may also highlight PRs submitted by other programs that they plan to use to meet their IMD data needs.*
2. *Same as above, etc.*

ii. GEOINT Requirement: (*List GEOINT requirements submitted to National GEOSPATIAL Intelligence Agency for GEOINT products)*

iii. Other documentation: (*Identify the program's IMD planning as it is reflected in other key program management documents such as the System Requirements Document (SRD), Systems Engineering Plan (SEP),the Test and Evaluation master Plan (TEMP), Acquisition Strategy (AS) etc., along with how to access the document(s). Affording access to these planning inputs facilitates Intelligence Community (IC) understanding of the program manager's plan and their ability to ensure relevant support to the program .)*

c. **Risk assessment and courses of action to address IMD shortfalls** (per DODD 5250.01, para 4.f.)*: Program Name* has identified the following gaps in IMD required by the program during its lifecycle. These gaps, and their risks, were assessed by the *program office* in collaboration with the *operational MAJCOM* and the *coordinating Center Intelligence Office(s)* and stated below. Additionally, this plan will be briefly summarized in the program's Acquisition Strategy document, sections 6 (Risk), 8 (Funding/cost), and 12 (LMDP): (reference AS Template v2.3, 4 February 2014), (*include date and means for reviewers to access the AS)*

i. **Statement of IMD gaps**
ii. **Risk and Risk Mitigation Plan**
iii. **Funding/Cost (if any)**
iv. **Recommendation: If the program has dependent systems, such as the ALR-69, contact that program office and request a risk summary. If there are any external risk factors, recommend stating the risk here and how that program office is mitigating it.**

d. **IMD data rights:** *(Identify where IMD data rights are addressed by the program (such as the Acquisition Strategy, SEP, and contract), date, and specific section of the document. Specify how to access the document.)*

e. *** Non-DoD IMD:** (*Program Name*) will not use any non-DoD IC produced IMD throughout its lifecycle -- or -- (*Program Name*) will receive commercially produced IMD from XXX during (*list phases of the Lifecycle*) and a copy of the USD(I) endorsed waiver is attached (see appendix *X*) or a waiver request will be submitted by the Program Office.

4. Other relevant information: *(Describe any other information that is relevant to the IMD dependency that will aid the reviewer in understanding the plan for IMD relevant to the program.)*

5. If you need additional information regarding the *(Program name)* LMDP, please contact *(program office POC info).*

Signature Block for Program Manager

1st Ind, *PEO*

MEMORANDUM FOR // *MDA* // or // FOR RECORD (IF PEO IS MDA, closeout here)

I concur with this plan. // I approve implementation of this plan (*If MDA)*.

Signature Block for PEO
(PEO is the approving authority for LMDPs as delegated by SAF/AQ and outlined in the Air Force LMDP/LMDP Waiver process flow chart)

2nd Ind, *MDA*

MEMORANDUM FOR RECORD

I approve implementation of this plan.

Signature Block for MDA

Cc:
(Implementing MAJCOM/A2)
(Operating MAJCOM/A2)
(Supporting Center Intelligence Office (i.e. AFLCMC/IN, SMC/IN))
SAF/AQR
AF/A2D
  DIA/IMDC (Via HAF/A2D)
  J28 (Via HAF/A2D, DIA/IMDC)

Attachment 3

SAF/AQ ACQUISITION MATRIX

Table A3.1. Document Approval Authority. (AFI 63-101)

	Governance	ACAT IC/IAC							ACAT II					ACAT III				
AS: Approve & Final Signature **A:** Required Approval		AF/TE	AFMC or AFSPC	SAF/FM	SPONSOR	CIO	PEO	MDA	AFMC or AFSPC	SPONSOR	CIO	PEO	MDA	AFMC or AFSPC	SPONSOR	CIO	PEO	MDA
Acquisition Plan	Regulatory						AS					AS						AS
Acquisition Strategy	Regulatory							AS					AS					AS
Acquisition Program Baseline (APB)	Stat./Reg.							AS					AS					AS
Acquisition Decision Memo (ADM)	Regulatory							AS					AS					AS
- Exit Criteria	Regulatory							AS					AS					AS
Affordability Assessment	Regulatory							AS					AS					AS
AoA Study Guidance and Plan	Regulatory							A					A					A
Analysis of Alternatives Report (AoA)	Statutory							A					A					A
Clinger Cohen Act Compliance	Statutory					AS					AS					AS		
Corrosion Prevention Control Plan	Regulatory						AS					AS						AS
Cybersecurity Strategy	Statutory					AS					AS					AS		
Information Support Plan (ISP) (All IT - including NSS)	Regulatory					A		AS			A		AS			A		AS
IUID Implementation Plan	Regulatory						AS					AS						AS
IT & NSS Joint Interoperability Test Cert (All IT - including NSS)	Regulatory					AS					AS					AS		
Life Cycle Sustainment Plan (LCSP)	Regulatory		A					AS	A				AS	A				AS
Life Cycle Mission Data Plan	Regulatory						AS					AS						AS
Materiel Fielding Plan	AF Reg						AS					AS						AS
Orbital Debris Mitigation Risk Report	Regulatory							AS					AS					AS
Post PDR Report Assessment	Regulatory							AS					AS					AS
Post Implementation Review	Stat./Reg.				AS			A		AS			A		AS			A
Prog Env Safety Occ Health Eval (PESHE)	Statutory						AS					AS						AS
Program Protection Plan	Regulatory							AS					AS					AS
Spectrum Supportability Determination	Regulatory					AS					AS					AS		
Spectrum Cert Compliance (DD 1494) - NOTE: This document is approved by the NTIA per DoDI 5000.02	Statutory																	
Systems Engineering Plan (SEP) - NOTE: Final Signature is DASD(SE) for ACAT I Programs	Regulatory						A					AS						AS
Test and Evaluation Master Plan (TEMP)	Regulatory	A						A					AS					AS
Transition Support Plan - NOTE: Final signature is SAF/AQ	AF Reg		A				A		A			A		A			A	
AF MDA MDAPS ONLY																		
2366a Certification	Statutory							AS										
2366b Certification	Statutory							AS										
Beyond LRIP Approval	Statutory							AS										
DoD Component Cost Position	Regulatory			AS														
Independent Cost Estimate	Statutory			AS														
Full Funding Certification Memorandum	Regulatory			AS				AS										
LRIP Production Quantities	Statutory							AS										
Replaced System Sustainment Plan	Statutory						AS											

This table describes approval authority, coordinate documentation with all organizations required to support the implementation of the plan.

This table is not all inclusive, additional documentation and certification requirements should be reviewed for applicability.

***BY ORDER OF THE
SECRETARY OF THE AIR FORCE***

AIR FORCE INSTRUCTION 14-111

18 MAY 2012

Incorporating Change 1, 16 June 2014

Intelligence

INTELLIGENCE SUPPORT TO THE ACQUISITION LIFE-CYCLE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-Publishing.af.mil for downloading and ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A2DP

Certified by: AF/A2D
(Brig Gen Mark W. Westergren)

Supersedes: AFI 14-111, 10 January 2005

Pages: 23

This publication implements Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations*, and is consistent with Department of Defense Instruction (DoDI) 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense,* AFPD 10-9 *Lead Command Designation and Responsibilities for Weapons Systems*, AFPD 16-7, *Special Access Programs*, AFPD 63-1, *Acquisition and Sustainment Life Cycle Management*, AFPD 99-1, *Test and Evaluation Process*, and AFPD 90-11, *Strategic Planning System,* and guidance portion in Department of Defense Directive (DoDD) 5250.01, *Management of Intelligence Mission Data (IMD) Within the DoD*. This publication must be used in conjunction with Air Force Instruction (AFI) 10-601, *Operational Capability Requirements Development*, AFI 14-132, *Air Force Geospatial Intelligence (GEOINT)*, AFI 14-201, *Intelligence Production and Applications,* AFI 14-205, *Geospatial Information and Services*, *Operational Capability Requirements Development,* AFI 63-101, *Acquisition and Sustainment Life Cycle Management,* AFI 63-114, *Quick Reaction Capability Process,* AFI 99-103, *Capabilities-Based Test and Evaluation*, AFI 99-114, *Foreign Materiel Program*. This publication applies to Regular Component, Air Force Reserve (AFR), Air National Guard (ANG), and Department of the Air Force (AF) Civilians. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). Submit change recommendations using an AF Form 847, *Recommendation for Change of Publication* to the Office of Primary Responsibility (OPR). This publication may be supplemented, but all supplements must be coordinated with the Office of Primary Responsibility (OPR) prior to certification and approval. Upon publication, MAJCOMS will ensure copies are provided to the OPR. Compliance waiver requests must be submitted through the chain of command to the appropriate tier waiver approval authority, all other waivers will be submitted to the publication OPR.

SUMMARY OF CHANGES

This interim change identifies tiered waiver authorities for unit level compliance items to depict the assessed risk of non-compliance and updates the certifying official. A margin bar (|) indicates newly revised material.

1. ACQUISITION INTELLIGENCE

1.1. **Purpose.** Successful development of weapons systems, new operational concepts, and innovative combat techniques depends upon rapid, precise, accurate, and detailed intelligence, along with the infrastructure needed to provide it. Three key processes in the Department of Defense (DoD) must work in concert to deliver the capabilities required by the warfighter: The requirements process, the acquisition process and the Planning, Programming, Budget and Execution (PPBE) process. Acquisition intelligence activities span all three processes, as well as additional processes that are unique to the Intelligence Community (IC). Intelligence Supportability Analysis (ISA) is the process by which AF intelligence, acquisition and operations analysts identify, document and plan for requirements, needs and supporting intelligence infrastructure necessary to successfully acquire and employ AF capabilities, thereby ensuring intelligence supportability. ISA is required throughout a program's life cycle, and should be considered for all programs and initiatives. This publication outlines processes and provides guidance to ensure intelligence and its related infrastructure are aligned and integrated appropriately within AF acquisition-related activities.

1.2. **Objective.** To support effective research, development, fielding, employment, sustainment and improvement of AF capabilities by identifying intelligence requirements, resolving/mitigating deficiencies, integrating intelligence, and providing needed intelligence data and infrastructure in a timely and secure manner.

1.3. **Tenets.** Effective acquisition intelligence support is:

1.3.1. Relevant, providing meaningful support that enables programs to optimize capabilities.

1.3.2. Iterative, providing timely intelligence inputs to the materiel effort along acquisition timelines in an evolving fashion dictated by materiel development and sustainment needs.

1.3.3. Tailored, focusing products and processes to meet the needs of the users while reducing extraneous information.

1.3.4. Collaborative. Requiring partnership across acquisition, intelligence, counterintelligence, and requirements communities in order to identify and resolve intelligence issues related to new and evolving programs.

2. ROLES AND RESPONSIBILITIES

2.1. **General**

2.1.1. USAF Intelligence Offices are the primary interface to the National Intelligence Community and will partner with the IC to provide intelligence products and services, and to identify and resolve the intelligence needs of AF programs.

2.1.2. Authoritative threat intelligence information will be used by AF programs when validated intelligence information is not required. The National Air and Space Intelligence Center (NASIC) and other DoD/Service intelligence production centers provide authoritative threat intelligence information suitable for program use.

2.2. **Administrative Assistant to the Secretary of the Air Force (SAF/AA)** Serves as the Senior Security Official for the AF with oversight and policy authority for all AF SAPs.

2.3. **Assistant Secretary of the Air Force for Acquisition (SAF/AQ):** Sets policy and direction for AF acquisition processes to ensure intelligence dependencies, shortfalls and requisite courses of action are identified to resolve shortfalls for intelligence-sensitive programs.

2.4. **Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance (AF/A2):**

2.4.1. Sets policy and direction for AF intelligence processes to ensure intelligence products and services are integrated across the full acquisition life cycle. This includes research, development, acquisition, test, modernization and sustainment activities.

2.4.2. Provides oversight of the processes and procedures governing derived intelligence requirements.

2.4.3. Participates in the development of, and reviews requirements, planning, and acquisition documents and ensures they adequately address intelligence interests and have appropriate intelligence content.

2.4.4. Collaborates with AF/A3/5 and SAF/AQ to provide intelligence support during development of new requirements and program documents.

2.4.5. Represents AF ISR interests with respect to DoD and other agency activities impacting AF acquisition intelligence programs.

2.4.6. Collaborates with Intelligence Agencies and across AF staffs to establish policies for threat Modeling & Simulation (M&S) efforts.

2.4.7. Establishes workforce standards for acquisition intelligence competencies to include initial certification and recurring training, as appropriate. Approval authority for Major Command (MAJCOM) requests for waivers to acquisition intelligence certification requirements.

2.4.8. Advises the Director of Acquisition Career Management on acquisition intelligence workforce management issues, and assists in execution of acquisition workforce responsibilities in respective acquisition functions IAW AFI 36-2640, *Executing Total Force Development*.

2.4.9. Ensures collaboration between the IC and AF requirements, planning and acquisition communities in the development and sustainment of warfighting capabilities.

2.4.10. Provides intelligence certification recommendation as part of Joint Capabilities Integration and Development System (JCIDS) coordination and leverages acquisition intelligence inputs such as Independent Intelligence Assessment (IIA) to develop certification recommendations.

2.4.11. IAW AFPD 16-7, advocates intelligence requirements, provides substantive intelligence support, oversees acquisition intelligence support and provides intelligence oversight for all SAPs.

2.5. **Deputy Chief of Staff, Operations, Plans and Requirements (AF/A3/5):**

2.5.1. Ensures intelligence dependencies are described within applicable JCIDS documents per Joint Staff guidance and addressed within the AF Requirements Oversight 144 Council requirements approval process.

2.5.2. Collaborates with AF/A2 for intelligence support on issues concerning system performance, system survivability and validation of operational survivability requirements as well as on Planning and direction, Collection, Processing and exploitation, Analysis and production, and Dissemination (PCPAD) architectures and supportability.

2.5.3. Ensures that AF/A2 participates in the development and review of requirements, planning, and acquisition documents to ensure they adequately address intelligence interests, concept of operations (CONOPS), and have appropriate intelligence content.

2.5.4. Coordinates JCIDS documents with AF/A2 for intelligence certification recommendation prior to forwarding for Joint Staff intelligence certification.

2.5.5. As lead for AF M&S policy and standards, collaborates with AF/A2 and NASIC to establish policy for threat M&S efforts, to include those performed in support of program-based requirements development and simulation-based support activities throughout the life cycle.

2.6. **MAJCOM/Field Operating Agency (FOA):**

2.6.1. Identify ISR subject matter experts (SMEs) (to include acquisition intelligence specialists) and process owners to support requirements development High-Performance Team (HPT) processes. (T-2)

2.6.2. Ensure timely, complete, sufficient, and accurate intelligence analysis, information and support is provided to and integrated within capabilities-based planning and requirements development processes and life cycle PPBE documentation. (T-2)

2.6.3. Provide initial certification of personnel as acquisition intelligence specialists based upon the following minimum requirements: (1) completion of Defense Acquisition University courses ACQ 101, *Fundamentals of Systems Acquisition Management* and

RQM 110, *Core Concepts for Requirements Management,* (2) completion of the Acquisition Intelligence Formal Training Unit, (3) one year experience in a designated acquisition intelligence position. Submit requests for waivers to initial certification requirements to MAJCOM/FOA A2. (T-2)

2.6.4. Collaborate with AF/A2 to designate positions as acquisition intelligence positions. (T-2)

2.6.5. Participate in acquisition intelligence activities as follows:

2.6.5.1. Assist in the MAJCOM/FOA development of strategic plans and other acquisition-related documents, studies and analyses, ensuring ISR requirements and constraints are addressed. (T-2)

2.6.5.2. Participate in identification of intelligence support requirements for intelligence-sensitive acquisition programs. (T-2)

2.6.5.3. Draft and coordinate intelligence content for JCIDS and other requirements, acquisition and program planning documents for completeness, supportability, impact, and threat content. (T-2)

2.6.5.4. Coordinate analysis of requirements to identify ISR-related deficiencies and guide efforts to resolve those deficiencies. (T-2)

2.6.5.5. Participate in acquisition intelligence forums, as appropriate (e.g., Intelligence Support Working Group (ISWG), Threat Steering Group (TSG), etc.) to support derivation of intelligence requirements, intelligence costing, assessment of data shortfalls, and development of courses of action to address shortfalls. (T-2)

2.6.5.6. Coordinate with implementing command A2 to determine acquisition intelligence lifecycle support required for intelligence-sensitive materiel requirements (rapid reaction, modernization and sustainment, acquisition etc.). (T-2)

2.6.5.7. Submit requirements for and/or assist in the justification of requirements for modifications to fielded programs, based on emerging threats or technologies that jeopardize the mission effectiveness or survivability of the system. (T-2)

2.7. **Program Executive Officers (PEOs), Technology Executive Officer, Designated Acquisition Officials (DAOs) and PMs.**

2.7.1. In collaboration with implementing command designated intelligence focal points, ensure programs within their responsibility receive appropriate acquisition intelligence support IAW AFI 14-111 and AFI 63-101.

2.7.2. Determine Program Protection Plan (PPP) intelligence requirements IAW DoDI 5200.39. (T-0)

2.8. **Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA). In addition to FOA responsibilities, AFISRA also:**

2.8.1. Through NASIC, provide air, space and cyber intelligence assessments, products and services for a wide range of needs. (T-3)

2.8.1.1. Ensure NASIC chairs and/or attend TSGs. (T-3)

2.8.1.2. NASIC, as lead AF agency for production of Capstone Threat Assessments (CTAs), System Threat Assessments (STAs) and System Threat Assessment Reports (STARs), validate all intelligence production requirements (PR) and broker/monitor status of such requirements for satisfaction through the Defense Intelligence Analysis Program (DIAP). NASIC is the AF validation authority for Acquisition Category (ACAT) IC and ACAT II authoritative threat documents. NASIC is also responsible for applying the analysis of other national, DoD agencies/organizations, or allied intelligence services, as needed, to meet the need of the USAF force modernization and acquisition communities. (T-3)

2.8.1.3. Identify data production capabilities and shortfalls impacting acquisition programs. Identify associated operational impacts to support risk assessments and course of action development. (T-2)

2.8.1.4. Collaborate with AF/A2 and AF/A3/5, to establish standards for threat M&S efforts, to include those performed in support of program/capability-based requirements development and simulation-based support activities throughout the life cycle. (T-3)

2.8.1.5. Review threat and life-cycle intelligence mission data plans/documents/studies/ assessments prior to milestone (MS) reviews, as required. Ensure threat and intelligence mission data information meet DoD and AF standards. (T-2)

2.8.1.6. Monitor Critical Intelligence Parameters and provide appropriate notification in case of a breach. (T-2)

2.9. **Implementing Command (Air Force Material Command (AFMC), Air Force Space Command (AFSPC)):**

2.9.1. Ensure ready forces and capabilities (to include tools) to execute their acquisition intelligence mission. (T-2)

2.9.1.1. Collaborate with AF/A2 to establish workforce training standards for acquisition intelligence competencies, to include initial certification and recurring training, as appropriate. (T-2)

2.9.1.2. Lead development of curricula for Acquisition Intelligence Formal Training Unit. (T-2)

2.9.1.3. Provide initial certification of personnel as acquisition intelligence specialists based upon the following minimum requirements: (1) completion of Defense Acquisition University courses ACQ 101, Fundaments of Systems Acquisition Management and RQM 110, Core Concepts for Requirements Management (2) completion of the Acquisition Intelligence Formal Training Unit (3) one year experience in a designated acquisition intelligence position. (T-2)

2.9.1.4. Maintains and updates, the Acquisition Intelligence Guidebook (AIG), as required. The guidebook serves as a reference on intelligence tasks throughout the life cycle of an acquisition program or project and is available from AFMC/A2X. (T-3)

2.9.2. Ensure timely, complete, sufficient, and accurate intelligence analysis, information and support are provided to and integrated into acquisition and sustainment processes. (T-2)

2.9.3. In collaboration with the lead command A2 and programs, performs objective assessments of intelligence impacts associated with intelligence-sensitive programs from both an impact to acquisition and impact to operational employment perspective. (T-2)

2.9.3.1. Documents identify impact in IIA and provide that information to AF/A2 to support intelligence certification recommendations as well as other Headquarters AF and DoD level planning and requirements activities. (T-2)

2.9.4. Oversee and manage the conduct of acquisition intelligence, as follows:

2.9.4.1. Determine intelligence sensitivity of programs and advise program offices and MAJCOMs/FOAs (for new programs) of corresponding levels of support required to execute acquisition intelligence responsibilities. This information supports development of acquisition program baselines that account for program office intelligence workload. (T-1)

2.9.4.2. Oversee and review completion of ISA for programs to include documentation of intelligence requirements, deficiencies, and proposed solutions. This must be accomplished for programs in all phases including technology development, acquisition, test and sustainment. (T-2)

2.9.4.3. Work with PEOs/DAOs to identify requirements for acquisition intelligence related program facilities, personnel and resources. (T-2)

2.9.4.4. Identify and submit intelligence PRs to initiate IC production processes. (T-1)

2.9.4.5. Obtain expertise and cost data from intelligence agencies, as necessary. Work with acquisition counterparts (program manager (PM), Technology Lead, etc.) and MAJCOMs/FOAs to ensure intelligence costs are included in life cycle cost estimates and program budgets. (T-3)

2.9.4.6. Provide intelligence input to command attestation/certification of acquisition requirements feasibility. (T-2)

2.9.4.7. Provide intelligence analytical support to capabilities-based planning activities, as required. (T-2)

2.9.4.8. Perform Cross-Program Analysis (CPA) of program derived intelligence requirements to ensure consolidation of common deficiencies and facilitate development of multi-program solutions. Provide resulting derived requirements to appropriate MAJCOMs/FOAs for resolution via established AF requirements processes as well as to IC agencies for resolution via established intelligence PRs processes. (T-3)

2.9.4.9. Ensure acquisition intelligence specialists participate in force modernization forums (such as AF capabilities planning forums, TSGs, HPTs, Capability Material Teams, ISWGs, etc.). (T-2)

2.9.4.10. Coordinate transition of intelligence requirements, responsibilities and resources as programs transition between research sites, centers or other IC organizations. Draft Intelligence Annex to Transition Support Plans. (T-3)

2.9.5. Facilitate Threat Working Groups (TWGs) to identify emerging weapons and technologies that may threaten acquisition programs or the long-term viability (mission effectiveness and survivability) of AF weapon systems in sustainment. Assist, as necessary, with justification for threat-driven modifications to weapon systems, in coordination with program offices and lead command A2 personnel. (T-2)

2.9.6. Recommend approval/disapproval to AF/A2 of program requests for waivers to required intelligence planning and threat documentation (e.g. STAR, intelligence mission data or signature support plans, etc.). (T-3)

2.9.7. Ensure weapon systems in the Operations and Support phase receive threat assessments as needed throughout their lifecycle, to support in-service upgrades relevant to adversaries, reprogramming, and capability advancements. (T-2)

2.9.8. Review information provided via AF Form 1067, Modification Proposals, IAW AFI 63-131, Modification Program Management, for systems in sustainment. Determine whether the identified deficiencies/suggested modifications are intelligence sensitive and require intelligence support. (T-2)

2.10. **Air Force Operational Test and Evaluation Center (AFOTEC):**

2.10.1. Ensure that Operational Test and Evaluation (OT&E) program threat/target lists and OT&E threat environments are adequately addressed. Ensure appropriate intelligence is used to support test planning and the development of the threat/target/environment (TTE) portions of AFOTEC documents. (T-1)

2.10.2. Participate in STAR TSG, CTA and other acquisition intelligence forums, as appropriate. (T-1)

2.10.3. Coordinate with operating and implementing commands to identify and document total intelligence support requirements for OT&E. Ensure validated threat and ISA are included in Test and Evaluation Master Plans (TEMPs), and Operational Test Plans. (T-1)

2.10.4. Work with MAJCOM/FOA and direct report unit intelligence offices and IC organizations to ensure development of appropriate OT&E threat lists/scenarios to support Initial Operational Test and Evaluation. (T-1)

2.11. **Air Education and Training Command:**

2.11.1. In addition to responsibilities outlined for MAJCOMs/FOAs, design, develop, and instruct acquisition intelligence training courses at the direction of the AF Career Field Manager (CFM). (T-3)

2.11.2. Incorporate acquisition intelligence concepts and materials into acquisition and intelligence training programs at the direction of the appropriate AF CFM. (T-3)

2.12. **Air Force Office of Special Investigations (AFOSI)**

2.12.1. AFOSI will provide input to program protection planners in concert with MAJCOM senior intelligence officers (SIOs) IAW DoDI O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA).* (T-0)

2.12.2. Operating or implementing command SIOs will identify counter-intelligence topics, vulnerabilities and opportunities to AFOSI command representative as required. (T-3)

3. IMPLEMENTATION CONCEPTS

3.1. **Acquisition Intelligence Process Requirements.** The following conditions are necessary for intelligence support to be effectively integrated within acquisition life cycle processes:

3.1.1. Common access to and understanding of a program and its intelligence needs, across the intelligence, operations, planning, requirements, research, acquisition and sustainment communities.

3.1.2. Integration of acquisition intelligence stakeholders into assessment, analysis, planning, programming, and decision activities to provide data for cost, schedule and performance tradeoffs.

3.1.3. Tailoring of acquisition intelligence processes to each program. Ensuring they are executed as early as possible in the life cycle, and repeated, as necessary, during the life cycle. As requirements become more defined, more details about intelligence supportability and potential shortfalls can be derived.

3.1.4. The Operations and Support (O&S) phase of a weapon system usually lasts for decades and will encounter evolving theats throughout its life cycle. Warfighters depend on appropriate threat assessments to ensure weapon systems remain mission effective and survivable. Consistent processes during the O&S phase should support needed in-service upgrades relevant to adversaries, including “reprogramming” and capability advancements.

3.2. **Process.** Acquisition intelligence includes the following intelligence considerations for which process checklists and product formats are specified in the AIG:

3.2.1. Intelligence Sensitivity. The first step in the acquisition intelligence process is determination of intelligence sensitivity of the program by the implementing command A2 or delegate. Programs are considered to be intelligence-sensitive if they require intelligence data during development or to perform their mission, require the direct support of intelligence personnel or influence intelligence data at any point in the PCPAD cycle. Criteria and checklists for determining intelligence sensitivity are documented in the AIG. This assessment aids early development of rough-order-of-magnitude estimates for intelligence support to and risk management of the program.

3.2.2. Intelligence Supportability Analysis: ISA is the process by which AF intelligence, acquisition and operations analysts identify, document and plan for requirements, needs and supporting intelligence infrastructure necessary to successfully acquire and employ AF capabilities, thereby ensuring intelligence supportability. It is an iterative, collaborative process that provides tailored support to intelligence sensitive efforts within the Integrated Defense Acquisition, Technology and Logistics Life Cycle Management System. ISA should begin as early as possible and continue throughout the system life cycle; it is to be used for all initiatives, not only ISR programs. It must provide robust support during analysis of alternatives (AoA), system design, production and sustainment and will not end until the final transition/disposal of the capability.

3.2.2.1. ISA results in the identification of derived intelligence requirements (DIRs) and deficiencies, along with associated impacts to both acquisition and operational capability if the required intelligence is not provided. Examples of DIRs include: threat data, geospatial information, PCPAD requirements and issues related to Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF). These analytic activities must be documented, tracked and reported.

3.2.2.2. Results of ISA form the foundation for intelligence input to requirements and acquisition documents such as Initial Capabilities Documents (ICDs), Capability Development Documents (CDDs), TEMPs, Life Cycle Mission Data Plans (LMDPs), System Requirements Documents, etc., as outlined in applicable acquisition guidance (see Attachment 1).

3.2.2.3. Identified deficiencies are documented and submitted via established IC PRs and AF ISR Capability Planning & Analysis processes for resolution.

3.2.3. Documentation. ISA results must be documented throughout the process in a manner that facilitates intelligence input to established requirements systems and required acquisition documents (LCMP, CDD, COLISEUM, etc.) Documentation should be readily available and routinely updated to support acquisition events including, but not limited to: Acquisition Strategy Panels (ASPs), ICDs, CDDs, AF Requirements Boards, and AF Requirements Oversight Council meetings.

3.2.4. Deficiency Resolution. Once intelligence needs, shortfalls, and associated costs/benefits/risks have been assessed, the PM and acquisition intelligence specialists will develop and implement a plan or course of action in a secure and cost-effective manner, in time to meet approved or adjusted MS within the program timeline. The plan or course of action and its supporting information shall be periodically reviewed throughout the life cycle of the program and updated as needed, IAW DoD, Defense Intelligence Agency (DIA), Joint and AF guidance.

3.2.5. Intelligence Health Assessment (IHA). The IHA is an assessment of the status of a program’s intelligence supportability. IHA factors will be evaluated and incorporated into a program’s overall risk assessment.

3.2.6. Independent Intelligence Assessment (IIA). IIA are objective assessments of capability impact driven by intelligence dependencies that are associated with intelligence-sensitive programs. The IIA is a higher headquarters assessment of impact to acquisition and impact to operations based upon the results of intelligence supportability analysis, CPA and IC responses to acquisition community intelligence requirements.

3.2.7. Cross-Program Analysis (CPA). CPA is the examination of programs and derived intelligence requirements to identify commonality and achieve synergies via common solutions. The linkage of documented requirements/shortfalls with multiple customer sets serves to strengthen AF requirements and/or gain efficiencies in meeting these requirements, which can be forwarded to the IC and/or the AF corporate structures for action. CPA can also identify system or program integration issues.

3.2.8. Intelligence Certification. To be accomplished IAW Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3312.01A *Joint Military Intelligence Requirements Certification*.

3.3. **Primary Collaborative Activities.** The primary means for executing acquisition intelligence are described below. Program teams should tailor the breadth and depth of application of the acquisition intelligence processes to the complexities and needs of their specific effort, commensurate with its point in the life cycle.

3.3.1. Intelligence Support Working Group (ISWG). The ISWG brings together functional representatives from the intelligence, operations and acquisition communities to conduct and document ISA and to assess their collaborative ability to ensure that a program can be adequately supported at a level that will enable mission success. An ISWG is a useful construct to develop intelligence inputs to an AoA.

3.3.1.1. ISWG Participants. The ISWG is established by the program manager and is typically chaired or co-chaired by an implementing command designated intelligence focal point. ISWGs are composed of the following major interest groups: Implementing command program and intelligence offices; lead command requirements and intelligence offices; operational users; system engineers, developers and testers; and intelligence providers (IC representatives, intelligence production center points of contact, intelligence support managers, etc.).

3.3.2. TWGs are working-level integrated product teams (WIPTs) that address threat issues and ensure consistent threat support to acquisition programs throughout their life cycles. They are typically chaired by the program's designated intelligence focal point. TWGs are appropriate forums for addressing TTE issues for all programs. TWGs are typically composed of operational users, intelligence representatives, counterintelligence representatives, systems developers, and system testers.

3.3.3. Cost Analysis Working Group (CAWG). The CAWG is comprised of representatives from operating and implementing command organizations with expertise in cost analysis and works closely with the Air Force Cost Analysis Agency to develop the system life cycle cost estimate. Intelligence cost estimators participate in the CAWG for intelligence sensitive programs.

3.3.4. Threat Steering Group (TSG). The TSG's primary purpose is to produce a STAR or STA IAW DoD 5000-series guidance and DIA Instruction (DIAI) 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs*. **Note:** DIAI 5000.002 is available on SIPRNET at: **http://diateams.dse.dia.smil.mil/sites/Issuances/default.aspx**.

3.3.4.1. TSG membership typically includes representatives from: intelligence staffs of the implementing and operating commands, intelligence staffs of the service and Unified Commands, staff of the program manager; SAF/AQ; DIA (ACAT 1D programs); NASIC; AFOTEC; Operations, Plans and Requirements staffs from the implementing and operating commands, as appropriate.

3.3.4.2. IAW DIAI 5000.002, product centers provide NASIC and the TSG a system description that describe the system in sufficient detail to assess which threats could jeopardize the proposed system's ability to perform its mission. To accurately assess the threat, it is necessary that the system description include mission profiles for all missions foreseen for the system. The program office is responsible for providing the system description. The description must be current.

3.3.5. AoA is an evaluation of the performance, operational effectiveness, operational suitability, and estimated costs of alternative systems to meet a mission capability. The analysis assesses the advantages and disadvantages of alternatives versus the baseline capability, including the sensitivity of each alternative in the available tradespace. Acquisition intelligence has a role in all of the AoA working groups (WG). An ISWG is a useful construct to develop intelligence inputs to an AoA.

3.3.5.1. Threats and Scenarios Working Group (TSWG). The TSWG is responsible for identifying and providing the scenario(s) to be used during an AoA to assess the military utility and operational effectiveness of solutions being considered for possible AF acquisition to meet a valid requirement. Additionally, the TSWG provides threat performance and characteristic information from intelligence sources to enable the AoAs Effectiveness Analysis Working Group (EAWG) to simulate potential threats to mission effectiveness. The TSWG will be staffed primarily with MAJCOM intelligence professionals and SMEs. Members support the TSWG by providing relevant intelligence information to sustain TSWG decisions. The TSWG is the forum tasked to track, anticipate, and mitigate issues potentially impacting the identification, selection and recommendation of scenarios to the AoA WIPT. Other members may be added on an ad hoc basis to resolve issues, as they arise.

3.3.5.2. Technology and Alternatives Working Group (TAWG). The TAWG acts as the interface with alternative providers, crafting the requirements request, receiving alternative data, and resolving questions between the providers and the rest of the AoA WGs. The acquisition intelligence specialist's role as a TAWG member is to ensure the requirements information request specifically asks for ISR capability enabler assumptions to include external infrastructure needs, these include inputs from the acquisition intelligence costs analyst detailing what data is required to frame the ISR infrastructure costing analysis report.

3.3.5.3. Operating Concept WG. The acquisition intelligence specialist's role is to review the CONOPS from an intelligence perspective to ensure intelligence supportability issues/needs are noted.

3.3.5.4. Effectiveness Analysis Working Group. The acquisition intelligence specialist participates in the creation of the analysis assumptions from the perspective of valid intelligence supportability.

3.3.5.5. Cost Analysis Working Group. Acquisition intelligence cost analysts, in coordination with, members of the other working groups, support the AoA by providing cost data on intelligence support-related activities external to the proposed solutions/alternatives (i.e. DOTMLPF).

3.3.6. Other Supported Venues. Other acquisition-related forums that can require intelligence support include Acquisition Strategy Panels, Systems Security Working Groups, HPTs, Integrated Test Teams, Interoperability WGs, and unique WGs established by programs/capabilities/initiatives/projects.

LARRY D. JAMES, Lt Gen, USAF
Deputy Chief of Staff, Intelligence, Surveillance,
and Reconnaissance

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 10-9, *Lead Command Designation and Responsibilities for Weapons Systems,* 8 March 2007

AFPD 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations,* 2 April 2004

AFPD 16-7, *Special Access Program,* 19 February 2014

AFPD 63-1, *Acquisition and Sustainment Life Cycle Management*, 3 April 2009

AFPD 90-11, *Strategic Planning System*, 26 March 2009

AFPD 99-1, *Test and Evaluation Process*, 22 July 1993

AFI 10-601, *Operational Capability Requirements Development*, 6 November 2013

AFI 14-201, *Intelligence Production and Applications,* 1 December 2002

AFI 14-205, *Geospatial Information and Services*, 5 May 2010

AFI 16-701, *Military Personnel Exchange Program (MPEP)*, 2 February 2006

AFI 33-360, *Publications and Forms Management*, 25 September 2013

AFI 36-2640, *Executing Total Force Development*, 16 December 2008

AFI 63-101, *Acquisition and Sustainment Life Cycle Management*, 20 June 2013

AFI 63-114, Quick Reaction Capability Process, 4 January 2011

AFI 63-131, *Modification Program Management*, 19 March 2013

AFI 63-1201, *Life Cycle Systems Engineering*, 23 July 2007

AFI 99-103, *Capabilities-Based Test and Evaluation*, 16 October 2013

AFI 99-114, *Foreign Materiel Program*, 25 October 2002

AFMAN 33-363, *Management of Records*, 1 March 2008

DoDI 5000.02, *Operation of the Defense Acquisition System*, November 25, 2013

DoDI 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*, July 16, 2008

DoDI O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)*, June 8, 2011

DoDD 5250.01, *Management of Intelligence Mission Data (IMD) Within the DoD*, January 22, 2013

CJCSI 3170.01G, *Joint Capabilities Integration and Development System; Chairman of the Joint Chiefs of Staff Manual for the Operation of the Joint Capabilities Integration and Development System*, March 1, 2009

CJCSI 3312.01A, *Joint Military Intelligence Requirements Certification*, February 23, 2007

DIAI 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs* January 19, 2005

AIG, *Acquisition Intelligence Guidebook*

Adopted Forms

AF Form 847, *Recommendation for Change of Publication,* 22 September 2009

AF Form 1067, *Modification Proposals,* 1 November 1999

Abbreviations and Acronyms

ACAT—Acquisition Category

AF—United States Air Force

AFI—Air Force Instruction

AFISRA—Air Force Intelligence, Surveillance and Reconnaissance Agency

AFMC—Air Force Materiel Command

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFOTEC—Air Force Operational Test and Evaluation Center

AFPD—Air Force Policy Directive

AFSPC—Air Force Space Command

AIG—Acquisition Intelligence Guidebook

AoA—Analysis of Alternatives

ASP—Acquisition Strategy Panel

AT&L—Acquisition, Technology and Logistics

CAWG—Cost Analysis Working Group

CDD—Capability Development Document

CFM—Career Field Manager

CI—Counterintelligence

CIA—Central Intelligence Agency

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CONOPS—Concept of Operations

CPA—Cross-Program Analysis

CPD—Capability Production Document

CTA—Capstone Threat Assessment

DAO—Designated Acquisition Official

DIA—Defense Intelligence Agency

DIAI—Defense Intelligence Agency Instruction

DIAP—Defense Intelligence Analysis Program

DIR—Derived Intelligence Requirements

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DOTMLPF—Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities

DS&TI—Designated Science and Technology Information

EAWG—Effectiveness Analysis Working Group

FBI—Federal Bureau of Investigations

FOA—Field Operating Agency

GEOINT—Geospatial Intelligence

HPT—High Performance Team

IAW—In Accordance With

IC—Intelligence Community

ICD—Initial Capabilities Document

IIA—Independent Intelligence Assessment

IHA—Intelligence Health Assessment

IMD—Intelligence Mission Data

IOC—Initial Operational Capability

ISA—Intelligence Supportability Analysis

ISR—Intelligence, Surveillance, and Reconnaissance

ISWG—Intelligence Support Working Group

JCIDS—Joint Capabilities Integration and Development System

KSA—Key System Attribute

LMDP—Life Cycle Mission Data Plan

MAJCOM—Major Command

MCIA—Marine Corps Intelligence Activity

MDAP—Major Defense Acquisition Program

MS—Milestone

MSIC—Missile and Space Intelligence Center

M&S—Modeling & Simulation

NASIC—National Air and Space Intelligence Center

NGA—National Geospatial-Intelligence Agency

NGIC—National Ground Intelligence Center

NRO—National Reconnaissance Office

NSA—National Security Agency

OPR—Office of Primary Responsibility

OT&E—Operational Test and Evaluation

O&M—Operation and Maintenance

O&S—Operations and Sustainment

PCPAD—Planning and direction, Collection, Processing and exploitation, Analysis and production, and Dissemination

PEO—Program Executive Officer

PM—Program Manager

PMD—Program Management Directive

PPBE—Planning, Programming, Budgeting, and Execution System

PPP—Program Protection Plan

PR—Production Requirement

SAF/AQ—Assistant Secretary of the Air Force for Acquisition

SIO—Senior Intelligence Officer

SME—Subject Matter Expert

STA—System Threat Assessment

STAR—System Threat Assessment Report

T-0—Tier 0

T-1—Tier 1

T-2—Tier 2

T-3—Tier 3

TAWG—Technology and Alternatives Working Group

TEMP—Test and Evaluation Master Plan

TPP—Technology Protection Plan or Planning

TSG—Threat Steering Group

TSWG—Threats and Scenarios Working Group

TTE—Threat, Target, Environment

TWG—Threat Working Group

USAF—United States Air Force

USD (AT&L)—Under Secretary of Defense for Acquisition, Technology and Logistics

WG—Working Group

WIPT—Working Level Integrated Product Team

Terms

Acquisition Intelligence Specialist—Personnel certified in acquisition intelligence.

Analysis of Alternatives (AoA)—The evaluation of the operational effectiveness and estimated costs of alternative materiel systems to meet a mission need. The analysis assesses the advantages and disadvantages of alternatives being considered to satisfy requirements, to include the sensitivity of each alternative to possible changes in key assumptions or variables. The AoA assists decision-makers in selecting the most cost-effective materiel alternative to satisfy a mission need.

Authoritative—An intelligence product that has been published/posted under the auspices of the Defense Intelligence Analysis Program (DIAP). It has been produced by the intelligence element recognized in the DIAP as the authority for that kind of information, vetted and adjudicated within that element, and is based on reliable and trusted analysis tools and processes.

Capability—The combined capacity of personnel, materiel, equipment, and information in measured quantities, under specified conditions, that, acting together in a prescribed set of activities, can be used to achieve a desired output.

Capability Development Document (CDD)—A document that captures the information necessary to develop a proposed program, normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable and technically mature capability. The CDD is validated and approved before MS B.

Capability Production Document (CPD)—A document that addresses the production elements specific to a single increment of an acquisition program. The CPD is validated and approved before MS C.

Capstone Threat Assessment (CTA)—The DoD Intelligence Community's official assessment of the principal threat systems and capabilities within a category of warfare (e.g., air, Space, Cyber, Naval Warfare, etc.) that a potential adversary might reasonably bring to bear in an attempt to defeat or degrade U.S. weapon systems. CTAs project the threat environment in a given warfare area out to 20 years, and constitute the validated, DoD IC position with respect to those warfare areas.

Critical Intelligence Parameter (CIP)—A factor which clearly defines the threshold at which the performance of a foreign system/capability could compromise the program / mission effectiveness of the US system. If a CIP is breached (i.e., a foreign system has met the CIP threshold) materiel and/or non-materiel (DOTMLPF) changes must be considered, the program will likely require additional time and funds to adjust (“re-baseline”), and spiral/increment thresholds, objectives, KPPs, KSAs, etc. may require adjustment.

Cross-Program Analysis (CPA)—CPA is an analytical effort designed to "look across" all intelligence-sensitive programs and the related intelligence shortfalls. The primary objective of CPA is to identify and consolidate like deficiencies. Synergies between programs and cost savings are realized when solutions are identified that support multiple programs. The results of CPA guide identification and development of solutions to the documented deficiencies. An additional aspect of CPA is to identify system or program integration issues.

Defense Intelligence Analysis Program (DIAP)—DIA centrally manages defense intelligence analysis and production using a distributed analytical process known as the DIAP. This program integrates general military intelligence and scientific and technical intelligence production conducted at DIA, Combatant Commands, and Service intelligence centers. The DIAP allows DIA to focus all-source defense intelligence analysis efforts on compelling issues for defense customers while limiting duplication of effort.

Derived Intelligence Requirements——Intelligence requirements that are implied from higher-level requirements, such as Key Performance Parameters (KPPs) and Key Systems Attribute (KSA).

Geospatial Intelligence—The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information, also called GEOINT.

Implementing Command—The command or agency designated by the AF Acquisition Executive to manage an acquisition program. The intelligence support to the manager of an acquisition program usually resides with the Product Center/Logistics Center/Lab Research Site Intelligence Division/Branch.

Initial Capabilities Document (ICD)—Documents the need for a materiel approach to a specific capability gap derived from an initial analysis of materiel approaches executed by the operational user and, as required, an independent analysis of materiel alternatives. It guides initial program activities and supports MS A.

Intelligence Community (IC)—The federation of executive branch agencies and organizations that conduct foreign and/or counter-intelligence activities necessary for conduct of foreign relations and protection of national security. IC members include the Service intelligence organizations (NGIC, ONI, NASIC, MCIA, and Service intelligence staff/support units), NSA, CIA, FBI, DIA (including MSIC and AFMIC), NRO, and NGA, as well as the intelligence components of the US Coast Guard, Department of Energy, Department of Homeland Security, Department of State, Department of Commerce, and Department of Treasury. **Note:** Counterintelligence (CI) is an organizational and functional part of the Intelligence Community, but is usually "compartmented" from foreign intelligence offices and/or functions in order to protect sensitive personal and law enforcement information IAW federal law and Intelligence Oversight guidance. While this AFI focuses on support from the (foreign) intelligence components of the IC, representatives from the CI components can be requested to support acquisition intelligence processes, if needed. The Air Force Office of Special Investigations (AFOSI) is the primary USAF CI organization, a FOA that identifies, investigates and neutralizes criminal, terrorist, and espionage threats to the personnel and resources of USAF and DoD.

Intelligence Costing—–An integral part of the ISA is the estimation of costs associated with the Intelligence resources required to support the acquisition programs. The lack of understanding of these costs can result in scheduling delays, costly work-arounds, and unplanned adjustments to Operations and Maintenance (O&M) budgets.

Intelligence Estimate—An appraisal of available intelligence relating to a specific situation or condition, with a view to determining the courses of action open to an enemy or potential enemy and the probable order of adoption of such courses of action.

Intelligence Mission Data (IMD)—DoD intelligence used for programming platform mission systems in development, testing, operations, and sustainment including, but not limited to, the following functional areas: signatures, EWIR, OB, C&P, and GEOINT.

Intelligence Requirement—The need for a product, function, infrastructure, or service provided by the Intelligence Community (IC) that is integral to a program at a point within its life cycle. Intelligence requirements can come from any part of the DOTMLPF construct. Program intelligence requirements should be documented to support both current and future acquisition and intelligence requirements. Documentation should include information on the availability of the needed IC capabilities. Requirements which cannot be met with current IC capabilities are identified as gaps, shortfalls or deficiencies.

Intelligence-sensitive—Any program/initiative that produces, consumes, processes, or influences intelligence information, thereby requiring threat or intelligence infrastructure support. If it is likely that, in the future, the program would produce, consume, process, or influence intelligence information, it should be considered intelligence-sensitive.

Intelligence Supportability—Refers to the availability, suitability and sufficiency of intelligence support required by a program. CJCSI 3312 Par. 4.c(2)(b).

Intelligence Supportability Analysis (ISA)—–Intelligence personnel partner with acquisition and operations stakeholders, and with other SMEs, to help derive/resolve the intelligence requirements by tailoring and utilizing the acquisition intelligence processes described in this AFI. In addition, IAW CJCSI 3312.01, the AF must review the intelligence support and intelligence-related operational requirements specified in (or derived from) JCIDS and other acquisition documents for completeness, supportability, and impact. For the purposes of this AFI, these intelligence certification activities are also included under the "ISA" term. ISA was formerly known as intelligence infrastructure analysis.

Intelligence Support Working Group (ISWG)—The ISWG is an enduring and continuously functioning group that brings together functional representatives from the intelligence, operations and acquisition communities to conduct and document ISA and to assess their collaborative ability to ensure that a program can be adequately supported at a level that will enable mission success.

Intelligence, Surveillance, and Reconnaissance (ISR)—Term referring to the activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.

JCIDS Documents (ICD, CDD, CPD)—–IAW CJCSI 3170.01 and the JCIDS Manual, DIA validates the threat and intelligence supportability information in all JROC Interest, JCB Interest, and Joint Integration ICDs, CDDs and CPDs through the intelligence certification process (ref. CJCSI 3312.01). For programs with Joint Information or Independent JPDs, which DIA does not review or validate, DoD Components can utilize DIA-validated threat reference information and/or data contained in DoD Service validated and authoritative intelligence products for their JCIDS documents.

Life Cycle—The span of time associated with a technology, concept, system, subsystem, capability, initiative or end-item that begins with the conception and initial development of the requirement, continues through development, acquisition, fielding, sustainment, until the time it is either consumed in use or disposed of as being excess to all known materiel requirements.

Life Cycle Mission Data Plan (LMDP)—A management plan that is applied throughout the life of a intelligence mission data-dependent acquisition that bases programmatic decisions on the availability of data over the life of a mission data-dependent acquisition.

Major Defense Acquisition Program (MDAP)—A DoD acquisition program that is not a highly sensitive classified program and: (1) That is designated by the USD(AT&L) as a MDAP; or (2) That is estimated to require an eventual total expenditure for research, development, test, and evaluation, including all planned increments, of more than $365 million (based on fiscal year 2000 constant dollars) or an eventual total expenditure for procurement, including all planned increments, of more than $2.19 billion (based on fiscal year 2000 constant dollars).

Milestone (MS)—Major decision point that separates the phases of an acquisition program under the DoDI 5000.02, *Operation of the Defense Acquisition System,* acquisition management framework. These include: MS A—Technology Development Phase approval; MS B—Engineering and Manufacturing Development Phase approval (normally the initiation of an acquisition program); and MS C—Production and Deployment Phase approval.

Planning, Programming, Budgeting, and Execution System (PPBE)—A cyclic process containing four distinct but interrelated phases: Planning—Produces a fiscal forecast, planning guidance, and program guidance; Programming—Creates the AF portion of the DoD's Future Years Defense Program (FYDP) by defining and examining alternative forces and weapons and support systems; Budgeting—Formulates and controls resource requirements, allocation, and use; and Execution—Measures and validates the performance of the planning, programming, and budgeting phases.

Program—For clarity throughout this publication, a program, project, technology demonstration, research effort, development planning activity, quick reaction capability, study, concept, initiative, system, modification, sustainment effort or upgrade involving intelligence support during research, development, acquisition, test, modernization, or sustainment will be implied by and referred to by the word “program.”

Program Management Directive (PMD)—The official AF document used to direct acquisition responsibilities to the appropriate major commands, agencies, program executive office, or designated acquisition commander. All acquisition programs require PMDs. PMDs initiate and terminate actions, cite funding sources, and assign responsibilities and tasks to appropriate commands and agencies.

Program Protection Plan or Planning (PPP)—The Program Protection Plan is the program manager's single source document used to coordinate and integrate all protection efforts designed to protect critical information and resources, and to prevent inadvertent disclosure of leading edge technology to foreign interests. Program Protection Planning is a comprehensive effort that encompasses all security, technology transfer, intelligence, and counterintelligence processes through the integration of embedded system security processes, security manpower, equipment, and facilities.

Requirements Strategy—A plan or document that maps the details necessary for developing a requirements document, and describes the resources and communities necessary to support the process.

Special Access Program (SAP)—A program established by the head of a department or agency whom the President has designated in the Federal Register as an original SECRET or TOP SECRET classification authority, which has additional "need to know" access controls beyond those controls normally required for access to information classified as CONFIDENTIAL, SECRET or TOP SECRET. SAPs are established only when the program is required by statute or upon a specific finding that: (1) the vulnerability of, or threat to, specific information is exceptional; and (2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

System Threat Assessment Report (STAR)—Official assessment of the principal threat systems and capabilities that a potential adversary might reasonably be expected to employ in an attempt to defeat or degrade a specific US weapon system when it is deployed. The STAR includes descriptions of the operational threat environment, target attributes, system-specific threats (for the time period of IOC to IOC+10 years), and emergent technologies. STARs are developed for ACAT Level 1D, 1C, and ACAT II programs, and for all programs on DOT&E Oversight List. For those AF programs, STARs are required for Milestones (MS) B and C IAW DoDI 5000.02. AF policy: STARs must be current at the time each MS decision is made. STARs typically expire 24 months from the date of publication.

Technology Protection Plan or Planning (TPP)—Similar to the PPP developed in the acquisition cycle, a TPP is developed by research organizations to identify critical information and resources that require increased protection. The TPP identifies the threats to a technology and prescribes necessary countermeasures to ensure the technology is adequately protected from compromise. TPPs will likely focus on those critical technologies, information, capabilities, and demonstrations, referred to as designated science and technology information (DS&TI), that have a more defined transition path to an activity ready to assume program management responsibility (usually an acquisition program or other DoD government agency or organization) or that have strong potential for transition based on the underlying value/advancement of warfighter capability. DS&TI will be protected via a TPP or, in the case of a technology insertion Advanced Technology Demonstration, within the auspices of an existing Program Protection Plan (PPP). The overall objective of AFRL-generated technology protection planning is to protect identified DS&TI that will transition into a weapons system platform or program to ensure the AF can acquire, field, and operate quality weapons and support systems, which have not been compromised and will meet mission requirements.

Tier 0 (T-0)—Determined by respective non-AF authority (e.g., Congress, White House, OSD, JS). The requirement is external to AF. Requests for waivers must be processed through command channels to publication OPR for consideration. (AFI 33-360)

Tier 1 (T-1)—Non-compliance puts Airmen, commanders or the AF strongly at risk of mission or program failure, death, injury, legal jeopardy or unacceptable fraud, waste or abuse. T-1 waiver requests may be granted at the MAJCOM/CC level, but may not be delegated lower than MAJCOM Director, with the concurrence of the publication's approving official. (AFI 33-360)

Tier 2 (T-2)—Non-compliance has the potential to create moderate risk of mission or program degradation or failure, injury, legal jeopardy or unacceptable fraud, waste or abuse. Waivers may be granted at the MAJCOM/CC level, but may not be delegated lower than MAJCOM Director. (AFI 33-360)

Tier 3 (T-3)—Non-compliance has a relatively remote potential to create risk of mission or program degradation or failure, injury, legal jeopardy or unacceptable fraud, waste or abuse. Waivers may be granted at the Wing/DRU/FOA/CC level. (AFI 33-360)