BY ORDER OF THE SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE INSTRUCTION 14-411

19 FEBRUARY 2025

Intelligence

ACQUISITION INTELLIGENCE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A2/6OC

Certified by: AF/A2/6O (Col Ariel Batungbacal)

Supersedes: DAFMAN 14-401, 26 MAY 2021

Pages: 30

Department of the Air Force Instruction (DAFI) implements Air Force Policy Directive (AFPD) 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise* and DoDI 5000.86, *Acquisition Intelligence.* This instruction establishes the Acquisition Intelligence guidelines and procedures to the entire DAF, including all civilian employees and uniformed members who perform the intelligence functions that are part of capability development, test, research and development (R&D), the acquisition life cycle, and sustainment. This instruction also supports activities and weapon systems procured under Department of Defense (DoD) 5000 series, in particular DoDD 5000.01 of instructions comprising the Defense Acquisition System. Additionally, this DAFI implements, Department of the Air Force Policy Directive (DAFPD) 10-9, *Lead Command/Lead Agent Designation and Responsibilities for Weapons Systems, Non-Weapon Systems, and Activities*, Defense Intelligence Agency Instruction (DIAI) 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs*, Department of Defense Directive (DoDD) 5205.07 Volume 1, *Special Access Program Security Manual: General Procedures*, and Department of Defense Manual (DoDM) 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*. If there is conflicting guidance between this DAFI and any DoD series or published higher-level guidance, the DoD series or published higher-level guidance takes precedence. This publication applies to all civilian employees and uniformed members of the Regular Air Force, the Air Force Reserve, the Air National Guard, the United States Space Force, and those with a contractual obligation to abide by the terms of DAF publications. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records

Disposition Schedule, which is located in the Air Force Records Information Management System. Submit change recommendations using an DAF Form 847, *Recommendation for Change of Publication* to the Office of Primary Responsibility (OPR). This publication may be supplemented, and all supplements must be coordinated with the OPR prior to certification and approval. Upon publication, Major Commands and Field Commands will ensure copies are provided to the OPR. The authorities to waive wing, unit, delta, or garrison level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the publication OPR for non-tiered compliance items.

1. INTRODUCTION.

1.1. **Purpose.** This instruction outlines directive, overarching processes, and procedures required to deliver and sustain acquisition intelligence. It provides guidance to ensure that intelligence and its related infrastructure are aligned and integrated appropriately within DAF capability development and acquisition life cycle activities.

1.1.1. Acquisition intelligence is the application of intelligence such as foundational military intelligence about adversary threats and planning for intelligence dependency in acquisition projects, programs, and operations. This is not a new intelligence discipline. (See DoDI 5000.86, *Acquisition Intelligence*). It supports capability development, test, R&D, and the acquisition life cycle.

1.1.2. Acquisition intelligence shall be integrated IAW Title 10 U.S.C. § 4211, *Acquisition Strategy*. It is required by DAFI 63-101/20-101 *Integrated Life Cycle Management*, for capability development and the acquisition life cycle.

1.2. **Foundational Terms and Concepts.** This publication uses the following terms:

1.2.1. "Acquisition intelligence" as defined above. It includes support for the six Adaptive Acquisition Framework pathways and all aspects of the definition. These aspects include:

1.2.1.1. Major Commands (MAJCOM), Field Commands (FLDCOM), Direct Reporting Units (DRU), and Field Operating Agency (FOA) execute processes such as intelligence integration, joint-specific, and service-specific capability development.

1.2.1.2. Air Force Materiel Command (AFMC) and Space Systems Command (SSC) are materiel focused commands that execute procurement and sustainment activities.

1.2.2. "Acquisition intelligence analysts" (AIAs) are designated DAF professionals who execute acquisition intelligence activities as their primary duty in MAJCOM, FLDCOM, DRU, FOA, AFMC, SSC, DAF service intelligence centers, and DAF-level staff agencies. AIAs will abide by all intelligence oversite requirements.

1.2.3. "Programs" are activities related to a materiel system's development and acquisition, and they are elements of the MAJCOM, FLDCOM, DRU, FOA, AFMC and SSC that execute those processes.

1.2.4. "Projects" are R&D activities and special activities that involve the acquisition of capabilities done inside or outside the standard acquisition life cycle.

1.3. **Scope.** This instruction addresses DAF acquisition intelligence roles and responsibilities for specific organizations. It applies to all DAF entities that create or integrate intelligence into capability development, test, R&D, and the acquisition life cycle. It applies regardless of entity type, primary function, authority, or funding source. It applies to all DAF-level headquarters staff agencies, MAJCOM, FLDCOM, DRU, FOA, service intelligence centers, DAF rapid capabilities offices, and rapid acquisition offices/units. This instruction also applies to all development and acquisition pathways and processes, such as service-specific processes, the Joint Capabilities Integration and Development System (JCIDS), Major Capability Acquisition, Middle Tier of Acquisition, Urgent Capability Acquisition, Software Acquisition Programs, Foreign Military Sales, and Special Access Programs.

2. ROLES AND RESPONSIBILITIES.

2.1. **General** .

2.1.1. The entire capability development and Materiel Enterprise is collectively responsible for integrating intelligence into capability development, R&D, test, and the acquisition life cycle. DAF identifies four major areas as critical to the effectiveness of intelligence support to acquisition. The four areas are:

2.1.1.1. Intelligence supportability analysis, to identify, document, and plan for intelligence data and infrastructure necessary to successfully acquire and employ DAF capabilities.

2.1.1.2. Threat support to capability development, R&D, test, and the acquisition life cycle, which integrates intelligence on current and future threats into these processes.

2.1.1.3. ISR interoperability reviews, to ensure the materiel system being developed can integrate with the ISR collection and dissemination ecosystem if the system can collect, disseminate, or must receive intelligence or other relevant battlespace information.

2.1.1.4. Force Development, to ensure AIAs are trained, educated, and receive the experience required to effectively execute the acquisition intelligence mission.

2.2. Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics (SAF/AQ) and Assistant Secretary of the Air Force for Space Acquisition (SAF/SQ) will:

2.2.1. Provide policy and guidance to ensure intelligence integrates throughout capability development, test, R&D, and the acquisition life cycle IAW this instruction.

2.2.2. Ensure the DAF acquisition workforce is organized, trained, and equipped to execute acquisition intelligence activities IAW this instruction.

2.2.3. Set policy and direction for DAF acquisition processes to identify and resolve intelligence dependency shortfalls for intelligence-sensitive programs.

2.2.4. Set policy and guidance for the Materiel Enterprise, including program and test managers, to document and report the following:

2.2.4.1. Determine gaps in the program’s ability to model and outpace future threats.

2.2.4.2. Actions the program will take to rectify or mitigate these gaps during the program life cycle.

2.2.5. Ensure the Materiel Enterprise is integrating digitalized threat representation products, such as threat Modeling & Simulation (M&S) and threat databases.

2.2.6. Collaborate with Service Deputy Chiefs of Staff responsible for Strategy, Plans, Programs, and ISR on integrating intelligence into decision processes. These include program/project documents for capability development, test, and R&D throughout the acquisition life cycle to include intelligence certification.

2.3. Director for Studies and Analysis, Office of the Secretary of the Air Force (SAF/SA) will:

2.3.1. Function as lead for DAF M&S policy and standards.

2.3.2. Function as lead for the DAF M&S Council.

2.3.3. Collaborate with Service Deputy Chiefs and the Defense Intelligence Enterprise.

2.3.4. Establish policy to integrate threat M&S into DAF program/project digital engineering and M&S environments throughout capability development and the acquisition life cycle.

2.3.5. Review and approve priorities of DAF threat M&S requirements.

2.4. **Program Executive Officers (PEOs) and Technology Executive Officers will:**

2.4.1. Provide direction to ensure intelligence integrates into capability development, test, R&D, and the acquisition life cycle.

2.4.2. Support DAF acquisition intelligence analysts to execute acquisition intelligence activities.

2.4.3. Coordinate with AFMC or SSC A2/S2 senior leadership to designate an intelligence focal point. For example, designate a Director of Intelligence (DOI) to ensure intelligence fully integrates into the decision processes for the acquisition life cycle.

2.4.4. Ensure programs/projects are fully threat-informed, have intelligence supportability (data and infrastructure), conduct Intelligence Health Assessments (IHAs), and have ISR interoperability consistent with this instruction and DAFI 63-101/20-101.

2.4.5. Coordinate with the requirements community to identify requirements, actions and resources needed to ensure programs/projects are developed to outpace future threats.

2.4.6. Ensure programs and projects develop and implement an intelligence integration strategy, plan, or course of action as part of the program's documented acquisition strategy to meet program/project objectives.

2.4.7. Ensure programs and projects include intelligence requirements in Program Protection Plans and Science and Technology Protection Plans consistent with DoDI DoDI5000.83_DAFI63-113, *Technology and Program Protection to Maintain Technological Advantage*. Reference also DoDI 5200.39, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)*, DoDD 5205.07, *Special Access Program Policy*, and DoDI 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs*.

2.4.8. Ensure programs and projects leverage, and if required, integrate, the supply chain focused information collected and analyzed by the Department of Defense Cyber Crime Center (DC3).

2.4.9. Ensure programs and projects identify intelligence requirements and if required submit them through the Community On-Line Intelligence System for End-Users and Managers to the Intelligence Community.

2.5. Deputy Chief of Staff for Personnel (HAF/A1) and Deputy Chief of Space Operations for Human Capital (SF/S1) will:

2.5.1. Professionalize acquisition intelligence by designating AIA billets and acquisition intelligence as a sub-specialty of the Air Force Intelligence career field.

2.5.2. Assist Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6) and Deputy Chief of Space Operations for

Intelligence (SF/S2), as appropriate, by monitoring and managing the DAF workforce awarded the Acquisition Intelligence Special Experience Identifier. Designate AIA billets in the appropriate personnel systems.

2.5.3. Support manpower studies to ensure acquisition intelligence manpower/resources are adequate to perform the mission.

2.6. Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6) and Deputy Chief of Space Operations for Intelligence (SF/S2) will:

2.6.1. Ensure intelligence is integrated into capability development, test, R&D, and the acquisition life cycle IAW this instruction.

2.6.2. Identify, organize, train, and equip Air Staff and Space Staff personnel to execute higher headquarters functions for acquisition intelligence, including policy/strategy development, DAF-level representation, and advocacy IAW this instruction.

2.6.3. Execute acquisition intelligence policy and strategy across the DAF enterprise. Integrate actions with the DAF and DoD entities, to include the Defense Intelligence Enterprise.

2.6.4. Advise the Director of Acquisition Career Management (SAF/AQ) on acquisition intelligence workforce management issues. Assist in executing acquisition workforce responsibilities in respective acquisition functions IAW DAFI 36-2670, *Total Force Development*.

2.6.5. Collaborate with Deputy Chief of Staff for Strategic Plans and Requirements, Deputy Chief of Space Operations for Strategy, Plans, Programs, Requirements, and Analysis on issues related to acquisition intelligence during capability development and document development. Provide intelligence certification IAW JCIDS guidance.

2.6.6. Provide authoritative intelligence in decision making, development, and review processes for capability development, requirements development, planning, and acquisitions.

2.6.7. Represent DAF acquisition intelligence interests to DoD and other agencies.

2.6.8. Collaborate with the DIE and DAF staffs on policy to integrate threat models into DAF M&S.

2.6.8.1. Participate as a member of the DAF M&S Executive Steering Group.

2.6.8.2. Participate as a member of the DAF M&S Council.

2.6.9. Ensure collaboration between the IC and DAF requirements, planning, and acquisition communities to develop and sustain warfighting capabilities.

2.6.10. Ensures unity of effort for generating, prioritizing, and managing IC requirements submissions among ISR MAJCOM, FLDCOM, DRU, FOA, AFMC, SSC, and other intelligence stakeholder communities.

2.6.11. Oversee DAF intelligence supportability/interoperability by identifying shortfalls, risks, and issues in production, planning, and joint processes, to include resource planning shortfalls in the Planning, Programming, Budget and Execution processes.

2.6.12. Manage intelligence requirements, provide substantive intelligence support, oversee acquisition intelligence support, and provide oversight for all SAPs IAW AFPD 16-7, *Special Access Programs*.

2.6.13. Coordinate on command and subordinate unit supplements, guides, and manuals that result from this instruction.

2.6.14. Establish ISR-specific guidance and standards to manage acquisition intelligence data during the acquisition life cycle.

2.7. Deputy Chief of Staff for Strategic Plans and Requirements, and Deputy Chief of Space Operations for Strategy, Plans, Programs, Requirements, and Analysis will:

2.7.1. Set policy and guidance for the capability development enterprise to integrate intelligence into capability development activities.

2.7.2. Coordinate with Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6) and Deputy Chief of Space Operations for Intelligence (SF/S2) to do the following:

2.7.2.1. Participate in the development and review of requirements, planning, capability development, and acquisition decisions/documents (DAF and Joint).

2.7.2.2. Adequately address intelligence interests and concepts of operations and have appropriate intelligence content.

2.8. DAF Service Intelligence Centers (SICs) NASIC and NSIC will:

2.8.1. Ensure intelligence products are timely and tailored for capability development, test, R&D, and the acquisition life cycle IAW IC and DoD-assigned production responsibilities and IAW DAF requirements/priorities. (T-2)

2.8.2. Identify, train, and equip unit members to integrate intelligence into capability development, R&D, test, and the acquisition life cycle. (T-2)

2.8.2.1. Produce/integrate intelligence products into DAF capability development, R&D, test, and the acquisition life cycle IAW IC and DoD-assigned production responsibilities and IAW DAF requirements/priorities. (T-2)

2.8.2.1.1. SICs will:

2.8.2.1.1.1. Produce timely, accurate, and relevant threat forecasts, roadmaps, assessments (except counterintelligence assessment), technical intelligence, threat modules and scenarios to keep programs/projects threat-informed and enable them to make timely adjustment that outpace evolving threats. (T-2)

2.8.2.1.1.2. Make intelligence products easily discoverable and accessible across security classification levels as required, to include technical intelligence products. Ensure products and data easily integrate with customer digital ecosystems to the maximum extent possible. (T-2)

2.8.3. Engage MAJCOM, FLDCOM, DRU, FOA and AFMC or SSC (materiel-focused commands), including program/project offices and capability development offices, to establish and maintain robust and ongoing dialogue (formal and informal) and partnerships (formal and informal) regarding intelligence that supports the program/project. (T-2)

2.8.3.1. Support formal partnerships between SIC and non-SIC entities IAW established DAF frameworks and DAF and IC governance to develop technical intelligence if/when the IC cannot meet prioritized technical intelligence requirements. (T-2)

2.8.3.1.1. SICs will, IAW DoDI 5000.61, *DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)* and Defense Intelligence Enterprise Management guidance:

2.8.3.1.1.1. Validate non-US forces and capabilities technical intelligence developed by SICs or formal partnership with SICs based on IC assigned production responsibilities. (T-2)

2.8.3.1.1.2. Create frameworks, create governance, and coordinate with the Defense Modeling and Simulation Intelligence Analysis Committee to facilitate the application of quality and tradecraft standards for M&S production covered under formal partnerships. (T-2)

2.8.4. Establish and execute unit procedures for critical intelligence parameters (CIP) monitoring and breach forecasting IAW DoDI 5000.86 and the JCIDS Manual, to include: 1) continuous monitoring, which is resource dependent; 2) periodic, comprehensive reviews/updates; 3) CIP breach forecast notifications as able, such as issuing warnings before a breach to enable programs to adjust and stay ahead of the threat; and 4) CIP breach notifications. (T-2)

2.8.5. Develop forward-looking production plans that anticipate future critical DAF intel needs. (T-2)

2.8.6. Participate in production gap prioritization and risk management. (T-2)

2.8.7. Participate in the DAF M&S Council and subordinate working groups. (T-2)

2.9. MAJCOMs, FLDCOM, Direct Reporting Unit (DRU), and Field Operating Agency (FOA) Commanders will:

2.9.1. Ensure intelligence integrates into every phase of capability development, test, R&D, and the acquisition life cycle IAW this instruction. (T-2)

2.9.2. Identify, train, and equip ISR subject matter experts, AIAs, and process owners to integrate intelligence into all requirements and capability development processes. (T-2)

2.9.3. Coordinate with AFMC or SSC (materiel-focused commands) to determine intelligence sensitivity for programs/projects. Advise program offices and MAJCOMs, FLDCOM, DRU, FOA (for new programs) on levels of support required to execute acquisition intelligence responsibilities. (T-2)

2.9.3.1. Ensure the transfer of acquisition intelligence responsibility from MAJCOM, FLDCOM, DRU, FOA to AFMC or SSC occurs upon PEO acceptance of the program. Coordinate with AFMC or SSC intelligence to determine acquisition intelligence life cycle support required for intelligence-sensitive programs/projects. (T-2)

2.9.3.2. Integrate future threat assessments during requirements determination and capability development, fielding, support, and sustainment. Determine necessary intelligence support, data dependencies, and infrastructure to address the threats. (T-2)

2.9.3.3. Coordinate with AFMC or SSC, service intelligence centers, and other IC agencies as required to develop CIPs IAW with command guidance. (T-2)

2.9.3.4. Ensure timely, complete, sufficient, and accurate acquisition intelligence is provided and integrated with capabilities-based planning, requirements development processes, and life cycle Planning, Programming, Budgeting, and Execution processes and forums. (T-2)

2.9.3.5. Ensure strategic plans and other capability development and acquisition-related documents, studies, and analyses integrate and fully address ISR requirements and constraints. (T-2)

2.9.3.6. Submit requirements and assist in the justification of new requirements for modifications to fielded programs based on emerging threats or technologies that jeopardize mission effectiveness or capability survival. (T-2)

2.9.4. Participate in the requirements framework to identify and generate requirements, and advocate for mission systems, operational needs, models, simulations, and capability requirements development that support DAF processes. (T-2)

2.9.4.1. Identify and manage risks that result from requirements production planning shortfalls, to include resource planning shortfalls in Planning, Programming, Budgeting, and Execution processes. (T-2)

2.9.4.2. Coordinate with the Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6) or Deputy Chief of Space Operations for Intelligence (SF/S2) (their staffs), as appropriate to identify risks and issues for presentation and engagement in joint technical intelligence requirements processes. (T-2)

2.9.5. Draft and coordinate the intelligence content for DAF, JCIDS, and other capability development, requirements, acquisition, and program planning processes and related documents. Ensure completeness of intelligence supportability, impact, and threat content. (T-2)

2.9.5.1. For program intelligence certification, coordinate with the Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6) on capability development, requirements, acquisition, and program planning processes and related documents (DAF and JCIDS). Ensure completeness of intelligence supportability, impact, and threat content. (T-2)

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

2.9.6. Identify and submit intelligence requirements to initiate intelligence collection and production that supports programs throughout the program lifecycle.

2.9.7. Coordinate with AFOTEC intelligence offices and Defense Intelligence Enterprise organizations to ensure development of appropriate threat lists/scenarios that support initial operational test and evaluation (OT&E). (T-2)

2.9.8. Provide tailored, command-specific guidance on threat analysis collaboration methods, forums, and best practices IAW this instruction. Participate in acquisition

intelligence forums as appropriate to support intelligence requirements, resourcing, assessment of data shortfalls, and development of courses of action to address shortfalls. (T-2)

2.9.9. Work with Acquisition Intelligence Analyst Certification Program (AIACP) program manager to identify AIA positions for coding and ensure AIAs are certified IAW the program requirements. (T-2)

2.10. Air Force Materiel Command or Space Systems Command will:

2.10.1. Ensure intelligence integrates into every phase of capability development, test, R&D, and the acquisition life cycle (e.g., analysis of alternatives, capability requirements documents, market research, acquisition strategies, plans, requests for proposals/other transaction authority, contracts, milestones).

2.10.2. Ensure programs/projects are threat-informed, have intelligence supportability (data and infrastructure), and have interoperability with weapons systems IAW DAFI 63-101/20-101 and AFI 61-101. (T-2)

2.10.3. Ensure each program's documented acquisition strategy includes intelligence. (T-2)

2.10.4. Coordinate with requirements owner to determine program/project intelligence sensitivity (if not already completed) and its impact to the acquisition life cycle and operational employment. (T-2)

2.10.5. Ensure intelligence requirements are developed and documented in coordination with the requirements owners. (T-2)

2.10.6. Identify, organize, train, and equip DAF professionals to execute acquisition intelligence activities including the provision of facilities, personnel, intelligence supportability, intelligence sensitivity analysis, intelligence requirements, and program intelligence certification IAW AIACP and command policy. Ensure AIA are tracked, certified IAW certification requirements. (T-2)

2.10.7. Ensure intelligence fully integrates into the decision processes for the acquisition life cycle. Oversee and review Intelligence Supportability Analysis (ISA) (T-2)

2.10.8. Ensure each program's documented acquisition strategy includes an intelligence integration strategy, plan, or course of action to meet program/project objectives in a cost-effective manner. (T-2)

2.10.9. Make program threat analysis products and data easily discoverable and accessible across security classification levels. Include the ability to easily integrate products with customer digital ecosystems to the maximum extent possible. (T-2)

2.10.10. Coordinate with MAJCOM, FLDCOM, DRU, FOA, service intelligence centers, and IC as required to develop new CIPs IAW with command guidance. Help existing CIPs to mature during capability development and the acquisition life cycle as they evolve based upon program maturation. (T-2)

2.10.11. Identify and submit intelligence requirements to initiate intelligence collection and production that support programs throughout the lifecycle. (T-2)

2.10.12. Coordinate transition of intelligence requirements, responsibilities, and resources as programs transition between research sites, centers, or other organizations. (T-2)

2.10.13. Collaborate with IC on threat forecasting to identify impacts on acquisition programs or long-term viability (mission effectiveness and survivability) of DAF weapon systems in the sustainment phase. Coordinate with MAJCOM, FLDCOM, DRU, FOA and SICs to develop justification for threat-driven modifications to the program. (T-2)

2.10.14. Ensure programs/projects receive threat intelligence as needed throughout their life cycle to support in-service upgrades relevant to adversaries, reprogramming, and capability advancements. (T-2)

2.10.15. Review information provided via AF Form 1067, *Modification Proposals* IAW DAFI 63-101/20-101 for systems in sustainment. Determine whether the identified deficiencies/suggested modifications are intelligence sensitive and require intelligence support. (T-2)

2.10.16. Draft/coordinate the intelligence content of acquisition and program planning documents. Ensure completeness of intelligence supportability, impact, and threat content. (T-2)

2.10.16.1. Identify and submit intelligence requirements to initiate intelligence collection and production that support programs throughout the lifecycle. (T-2)

2.10.16.2. Coordinate requirements analysis to identify deficiencies, and guide efforts to resolve those deficiencies. (T-2)

2.10.16.3. Provide intelligence health assessments to support acquisition and requirements (intelligence certification IAW JCIDS Manual) review processes. (T-1)

2.10.17. Identify and manage risks and issues that result from intelligence requirements production planning shortfalls, to include resource planning shortfalls in Planning, Programming, Budgeting, and Execution processes. (T-2)

2.10.18. Provide tailored, command-specific guidance on threat analysis collaboration methods, forums, and best practices IAW this instruction. Participate in acquisition intelligence forums as appropriate (e.g., foreign intelligence threat forums and intelligence supportability forums) to support derivation of intelligence requirements, intelligence costing, assessment of data shortfalls and development of courses of action to address shortfalls. (T-2)

2.10.19. Provide intelligence and forecasting subject matter expertise that supports DAF Foreign Materiel Sales program requirements.

2.10.20. Coordinate with AFOTEC intelligence offices and DIE organizations to ensure development of appropriate threat lists/scenarios that support initial OT&E. (T-2)

2.11. Air Force Operational Test and Evaluation Center (AFOTEC) and Space Training and Readiness Command (STARCOM) will:

2.11.1. Ensure intelligence integrates into operational test and experimentation planning and conduct to support the acquisition life cycle. (T-2)

2.11.2. Identify, organize, train, and equip DAF professionals to execute acquisition intelligence activities IAW this instruction, to include the provision of facilities, personnel, and other resources. (T-2)

2.11.3. Ensure OT&E personnel, to include Test Directors, Program Managers, and analysts, are threat-informed with threat analysis IAW this instruction and DAFI 63-101/20-101. (T-2)

2.11.3.1. Coordinate with program AIAs to ensure consensus program threat analysis products and data are available and incorporated in test design and planning. (T-2)

2.11.3.2. Ensure OT&E program threat/target lists, and threat environments adequately address intelligence dependencies and operationally realistic threat representations. (T-2)

2.11.3.3. Participate in the DAF M&S Council and subordinate working groups.

2.11.3.4. Participate in program threat analysis collaboration and working groups, intelligence supportability, and other acquisition intelligence forums as appropriate. (T-2)

2.11.3.5. Coordinate with MAJCOM, FLDCOM, DRU, FOA and AFMC or SSC program AIAs to identify and document any tailored threats or intelligence support requirements for OT&E beyond those in the Test and Evaluation Master Plan. (T-2)

2.12. Air Force Office of Special Investigations (AFOSI) will:

2.12.1. Ensure counterintelligence products and services are integrated into capability development, test, R&D, and the acquisition life cycle. (T-2)

2.12.2. Collaborate with AFMC or SSC (materiel-focused commands) acquisition intelligence focal points to provide input for program protection planners IAW DoDI O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)*. (T-2)

2.12.3. Coordinate with MAJCOM, FLDCOM, DRU, FOA and AFMC or SSC intelligence focal points to identify counterintelligence topics, vulnerabilities, and collaboration opportunities. (T-2)

3. FORCE DEVLEOPMENT

3.1. **Qualification Training.** Qualification is an ongoing process to attain the knowledge, skills, and experiences ensuring personnel are qualified and current to perform their assigned duties. Intelligence qualification training, consisting of Initial Qualification Training (IQT) and Mission Qualification Training (MQT), follows a building block approach. After completion of MQT, Continuation Training ensures maintenance and progression of knowledge, skills, and abilities of intelligence personnel. Specialized Training addresses additional intelligence tasks required by some positions above and beyond the baseline MQT requirements. Training programs will comply with AFI 14-1020.

3.1.1. Initial Qualification Training. IQT begins upon entry into a mission set and establishes a foundational set of skills developed to a level of detail common across a mission set, without focusing on any organization's specific mission execution. IQT is

defined as Acquisition Intelligence Formal Training Unit (IFTU). All personnel will complete IQT during the first year of assignment to their unit. (T-2)

3.1.2. Mission Qualification Training. MQT applies specific organization and mission context to skills gained in IQT and provides additional training to achieve mission ready qualification. MQT is an organization's program which includes unique local area procedures and ensures trainees to demonstrate knowledge and task proficiency. (T-2)

3.1.3. Continuation Training promotes a continuous learning environment, ensuring that intelligence personnel are always qualified and current to perform their assigned duties by maintaining proficiency in the requisite knowledge, skills, and abilities. In most cases, this is simply documenting activities individuals conduct on a regular basis as part of their duty. Continuation Training is an organization's program which focuses on maintaining perishable skills for currency of knowledge and task proficiency. (T-3)

3.1.4. Specialized Training. Specialized Training addresses additional skills necessary to carry out the organization's uniquely assigned mission(s). Specialized Training requirements are in addition to baseline mission qualification. (T-3)

3.1.5. Difference Training. Individuals moving to a similar mission set as determined by the lead command are assessed by the gaining organization to determine their previous training and experience level. If their previous IQT meets current requirements, the individual may be allowed to "proficiency advance" via an abbreviated in-house IQT or proceed directly to MQT. (T-3)

3.2. **AIA Certification Program (AIACP).** The AIACP validates that AIAs receive the proper training, education, and experience required to effectively execute AIA duties. The DAF Guidance Memorandum for AIACP governs execution of the program. It is encouraged for all personnel that perform intelligence functions supporting acquisition programs and processes and is mandatory for all personnel in AIA-coded billets, which are coded with the AIA special experience identifier. Personnel assigned to AIA-coded billets should complete AIACP within 18 months of assignment to the position. Personnel are awarded the AIA special experience identifier upon AIACP completion. (T-3)

3.3. **Discretionary Training.** MAJCOM, FLDCOM, DRU, FOA and AFMC or SSC execute MQT at their discretion to train AIAs on duties according to specific positions or functions. Commands also execute Continuation Training and Specialized Training at their discretion to develop further expertise and unique skills that are not covered in IQT or MQT. (T-3)

LEAH G. LAUDERBACK, Lt Gen, USAF
Deputy Chief of Staff, Intelligence, Surveillance,
Reconnaissance, and Cyber Effects Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

10 U.S.C. § 4211, *Acquisition Strategy*

DoDI 5000.02, *Operation of the Adaptive Acquisition Framework*, 08 June 2022

DoDI 5000.74, *Defense Acquisition Services*, 24 June 2021

DoDI 5000.75_DAFI 63-144 Business Systems Requirements and Acquisition¸ 26 January 2023

DoDI 5000.80_AFI 63-146, *Operation of Middle Tier of Acquisition (MTA)*, 07 May 2021

DoDI 5000.81_DAFI 63-147, *Urgent Capability Acquisition,* 04 February 2021

DoDI 5000.82, *Acquisition of Information Technology*, 01 June 2023

DoDI 5000.83_DAFI 63-113, *Technology and Program Protection to Maintain Technological Advantage*, 08 March 2022

DoDI 5000.85_AFI 63-151, *Major Capability Acquisition*, 19 August 2022

DoDI 5000.86, *Acquisition Intelligence*, 11 September 2020

DoDI 5000.87_AFI 63-150, *Operation of the Software Acquisition Pathway*, 11August 2021

DoDI 5000.89_DAFI 99-103, *Capabilities Based Test and Evaluation*, 9 December 2021

DoDI 5000.90, *Cybersecurity for Acquisition Decision Authorities and Program Managers,* 31 December 2020.

DoDI 5000.97, *Digital Engineering*, 21 December 2023

DoDI 5200.39, *Critical Program Information (CPI) Identification and Protection Within the Research, Development, Test and Evaluation (RDT&E)*, 01 October 2020

DoDI 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs)*, 4 February 2020

DoDI O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)*, 15 July 2020

DoDD 3000.16, *Vendor Threat Mitigation*, 6 July 2022

DoDD 5205.07 Volume 1, *Special Access Program (SAP) Security Manual: General Procedures*, 30 September 2020

DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 08 August 2016

CJCSI 3318.01, *Acquisition Intelligence Requirements Annual Priorities and Risk Management Framework*, 30 April 2020

CJCSI 5123.01I, *Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System*, 30 October 2021

AFPD 16-7, *Special Access Programs*, 21 November 2017

AFPD 63-1, *Integrated Life Cycle Management,* 7 August 2018

DAFPD 99-1, *Test and Evaluation,* 21 May 2021

AFI 10-601, *Operational Capability Requirements Documentation and Validation*, 27 April 2021

AFI 14-404, *Intelligence Oversight,* 03 September 2019

AFI 14-1020, *Intelligence Mission Qualification and Readiness*, 08 Nov 2017

DAFI 16-701_DAFGM2023-01, *Management, Administration and Oversight of Special Access Programs,* 15 February 2023

AFI 33-322, *Records Management and Information Governance Program,* 28 July 2021

AFI 36-2670, *Total Force Development*, 07 May 2024

AFI 61-101, *Management of Science and Technology*, 14 March 2013

DAFI 63-101/20-101, *Integrated Life Cycle Management*, 16 February 2024

DAFI 90-160, *Publications and Forms Management*, 21 June 2023

AFI 99-114-S, *Foreign Materiel* Program, 22 March 2019

DAFMAN 14-401, *Intelligence Analysis and Targeting Tradecraft/Data Standards*, 26 May 2021

AFMAN 14-405, *Multiple Source, Discipline, and Domain ISR*, 11 May 2020

ICD 203, *Analytic Standards*, 21 December 2022

ICD 206, *Sourcing Requirements for Disseminated Analytic Products*, 22 January 2015

ICD 208, Maximizing the Utility of Analytic Products, 9 January 2017

Directive-type Memorandum (DTM) -18-003 – Prohibition on Providing Funds to the Enemy and Authorization of Additional Access to Records.

Prescribed Forms

None

Adopted Forms

DAF Form 847, Recommendation for Change of Publication, 15 April 2022

AF Form 1067, Modification Proposals, 1 November 1999

Acronyms

AF—United States Air Force

AFI—Air Force Instruction

AFLCMC—Air Force Life-Cycle Management Center

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFOTEC—Air Force Operational Test and Evaluation Center

AFPD—Air Force Policy Directive

AFRL—Air Force Research Laboratory

AFSOC—Air Force Special Operations Command

AIA—Acquisition Intelligence Analysis

AIACP—Acquisition Intelligence Analysis Certification Program

CI—Counterintelligence

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

DAF—Department of the Air Force

DC3—Department of Defense Cyber Crime Center

DIA—Defense Intelligence Agency

DIAI—Defense Intelligence Agency Instruction

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

FLDCOM—Field Command

IAW—In Accordance With

IC—Intelligence Community

ICD—Intelligence Community Directive

IFTU—Intelligence Formal Training Unit

IHA—Intelligence Health Assessment

ISA—Intelligence Supportability Analysis

ISR—Intelligence, Surveillance, and Reconnaissance

IQT—Initial Qualification Training

JCIDS—Joint Capabilities Integration and Development System

KSA—Key System Attribute

MAJCOM—Major Command

M&S—Modeling & Simulation

MQT—Mission Qualification Training

OPR—Office of Primary Responsibility

OT&E—Operational Test and Evaluation

PEO—Program Executive Officer

PPBE—Planning, Programming, Budgeting, and Execution System

RDT&E—Research, Development, Test & Evaluation

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

STARCOM—Space Training and Readiness Command

T-0—Tier 0

T-1—Tier 1

T-2—Tier 2

T-3—Tier 3

TAWG—Technology and Alternatives Working Group

Terms

Acquisition Intelligence—The application of intelligence such as foundational military intelligence about adversary threats and planning for intelligence dependency in acquisition projects, programs, and operations. This is not a new intelligence discipline. (DoDI 5000.86).

Acquisition Intelligence Analyst (AIA)—AIAs are designated DAF professionals of any career specialty, not just intelligence, who have completed the AIA certification requirements IAW DAFI 14-411, and whose primary responsibility deals with integrating intelligence into acquisition/materiel processes. Acquisition intelligence activities include, among others: threat support, to ensure acquisition functions are fully threat informed with authoritative intelligence; intelligence supportability analysis, to identify intelligence necessary to successfully acquire and employ DAF capabilities; ISR interoperability reviews, to ensure materiel systems can integrate with the ISR ecosystem; and intelligence production requirements development, to levy the requirements for specific types of intelligence to support materiel functions or systems. AIAs will abide by all intelligence oversite requirements.

Analysis of Alternatives—Assessment of potential materiel solutions to satisfy the capability need documented in the approved Initial Capabilities Document. It focuses on identification and assesses potential materiel solutions, key trades between cost and capability, total life-cycle cost, including sustainment, schedule, concepts of operations, and overall risk. The AoA will inform and be informed by affordability analysis, cost analysis, sustainment considerations, early systems engineering analyses, threat projections, and market research. It supports a decision on the most cost-effective solution that has a reasonable likelihood of providing the validated capability requirement(s). The AoA is normally conducted during the Materiel Solution Analysis phase, is key input to the Capability Development Document, and supports the materiel solution decision at Milestone A. The AoA may be updated for subsequent decision points and milestone reviews if design changes impact AoA assumptions. (DoDI 5000.02T).

Authoritative—An intelligence product that has been published/posted under the auspices of the Defense Intelligence Analysis Program or equivalent IC programs. It has been produced by the intelligence element recognized in the Defense Intelligence Analysis Program 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 Development Document—Specifies capability requirements in terms of developmental Key Performance Parameters, Key System Attributes, Additional Performance Attributes, and other related information necessary to support development of one or more increments of a materiel capability solution. (DoD 5000.02 *JCIDS Manual*)

Critical Intelligence Parameter (CIP)—A threat capability or threshold established collaboratively by the requirements sponsor and the component capability developer, changes to which could critically impact the effectiveness and survivability of the proposed system. (DIAI 5000.002)

Defense Intelligence Analysis Program (DIAP)—DIA centrally manages defense intelligence analysis and production using a distributed analytical process known as the Defense Intelligence Analysis Program. This program integrates general military intelligence and scientific and technical intelligence production conducted at DIA, Combatant Commands, and service intelligence centers.

Defense Intelligence Enterprise—. The organizations, infrastructure, and measures to include policies, processes, procedures, and products of the Intelligence, CI, and Security Components of the Joint Staff, Combatant Commands, Military Departments, and other DoD elements that perform National Intelligence, Defense Intelligence, intelligence-related, CI, and security functions, as well as those organizations under the authority, direction, and control of the USD(I&S). (DoDD 5143.01)

Foreign Owned, Controlled or Influenced (FOCI)—A U.S. company is considered to be operating under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, to direct or decide matters affecting the management of operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts. (DoDI 5205.87)

Air Force Materiel Command/Space Systems Command—The command 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. (DAFI 63-101_20-101)

Initial Capabilities Document—A category of capability requirements documents that specifies one or more capability requirements and associated capability gaps that represent unacceptable operational risk if left unmitigated. It recommends partially or wholly mitigating identified capability gap(s) with a materiel capability solution, or some combination of materiel and non-materiel solutions. A validated ICD is an entrance criterion necessary for each Materiel Development Decision (MDD) (JCIDS Manual).

Intelligence Certification—An assessment of the integration of intelligence and a statement of adequacy as to whether the IC can provide the required support to the acquisition and operational communities. The certification is the result of collaboration and analysis that leverage the expertise and unique perspective of all applicable offices within Combatant Commands; intelligence and security-aligned combat support agencies; Service Intelligence Production Centers; Military Department Intelligence and Counterintelligence (CI) organizations; and JS/J-2. (JCIDS Manual)

Intelligence Community—All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. Also called IC. (JP 2-0)

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 workarounds, and unplanned adjustments to Operations and Maintenance budgets.

Intelligence Mission Data (IMD)—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). (DoDD 5250.01)

Intelligence Requirement—1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. (JP 2-0)

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—The availability, suitability, and sufficiency of intelligence information and capabilities to support the requirements or system defined in capability development documents. (DoDI 5000.86).

Intelligence Supportability Analysis (ISA)——The process by which the DAF intelligence, acquisition, and requirement communities collaborate to identify, document, and plan for intelligence requirements and supporting infrastructure necessary to successfully acquire and employ DAF capabilities, thereby ensuring intelligence integration and supportability. (DAFI 63-101/20-101 and JCIDS Manual)

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. (JP 2-0)

Joint Capabilities Integration and Development System (JCIDS)——System providing a baseline for documentation, review, and validation of capability requirement across the DAF.

JCIDS Documents (—Initial Capabilities Document**,** Capability Development Document**)** —— 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 Initial Capabilities Document, and Capability Development Document through the intelligence certification process (ref. CJCSI 5123.01I). For programs with Joint Information or Independent Joint Potential Designators, which DIA does not review or validate, DoD components can utilize DIA-validated threat reference information and 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—The program manager's plan for how the program manager and other organizations will address specific program needs for Intelligence Mission Data (IMD). It contains the results of IMD planning and spans the entire lifecycle of an IMD-dependent acquisition program. The LMDP potentially influences programmatic decisions based on the availability of IMD over the life of the program. (DoDI 5000.02).

Major Defense Acquisition Program (MDAP)—The term "major defense acquisition program" means a Department of Defense acquisition program that is not a highly sensitive classified program (as determined by the Secretary of Defense) and— (A) that is designated by the Secretary of Defense as a major defense acquisition program; or (B) in the case of a program that is not a program for the acquisition of an automated information system (either a product or a service), that is estimated by the Secretary of Defense for all increments of the program to require an eventual total expenditure for research, development, and test and evaluation of more than $525 million in Fiscal Year (FY) 2020 constant dollars or, for procurement, of more than $3.065 billion in FY 2020 constant dollars.(10 U.S. Code 4201)

Middle Tier Acquisition—An Acquisition pathway is used to rapidly develop (within 2-5 years) fieldable prototypes within an acquisition program to demonstrate new capabilities and rapidly field production quantities of systems with proven technologies that require minimal development. (DoDI 5000.80)

Milestone—The point at which a recommendation is made, and approval sought regarding starting or continuing an acquisition program, i.e., proceeding to the next phase. Milestones established by DoDI 5000.85 are: Milestone A that approves entry into the Technology Maturation and Risk Reduction (TMRR) phase, Milestone B that approves entry into the Engineering and Manufacturing Development (EMD) phase, and Milestone C that approves entry into the Production and Deployment (P&D) phase. (DoDI 5000.85)

Planning and direction, Collection, Processing and Exploitation, Analysis and Production, and Dissemination—Basis of DoD intelligence gathering. Planning and direction, Collection, Processing and Exploitation, Analysis and Production, and Dissemination takes raw collected data and turns it into usable information. Planning and direction starts by developing a plan to obtain intelligence based on a commander's (in this case a military commander or some other national leader) guidance. The collection step is the physical act of acquiring data. Processing and exploitation convert raw data into usable form. Analysis and production distill the collected data for intelligence value and delivering the desired product. Finally, the intelligence information is disseminated to the senior leadership or customer. (JP 2-0)

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 DAF 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. (DoD 7000.14-R)

Program—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.

Project—An R&D activity or special activity involving the acquisition of capabilities done in and sometimes outside the standard acquisition life cycle.

Program Management Directive—The official Headquarters, U.S. Air Force, document used to convey the guidance and direction of the decision authority and identify the various organizations, along with their essential responsibility, for ensuring the success of a program or other effort. PMDs are required for funded program contained in the Air Force Acquisition Program Master List. (Defense Acquisition University Glossary)

Program Protection Plan or Planning—A living plan to guide efforts to manage the risks to Critical Program Information (CPI) and mission critical functions and components as well as program and system information. This milestone acquisition document captures both systems security engineering (SSE) and security activities and the results of the analyses as the program and system become more defined. (Defense Acquisition Guidebook and DAFI63-101/20-101)

Science and Technology Protection Plan—A management tool to guide Science & Technology (S&T) protection activities involving applicable critical technology areas and applicable horizontal protection guidance. S&T protection activities and the implemented protection measures inform the program protection activities and protection measures when they transition to an acquisition program. S&T protection activities include protection requirements in legally binding agreements such as FAR-based solicitations, broad agency announcements, and Other Transaction Authority agreements, as appropriate, preparing updates to the S&T Protection Plan as technology matures, when the threat changes, or there is a compromise. The DoD Component determines the S&T Protection Plan approval authority. (DoD Technology and Program Protection Guidebook)

Special Access Program (SAP)—A sensitive acquisition, intelligence, or operations and support program, that imposes need-to-know and access controls beyond those normally provided for access to classified information. Also called SAP. (JP 3-05)

Supply Chain Risk Management (SCRM)—The process for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the DoD supply chain from beginning to end to ensure mission effectiveness. Successful SCRM maintains the integrity of products, services, people, and technologies, and ensures the undisrupted flow of product, materiel, information, and finances across the lifecycle of a weapon or support system. DoD SCRM encompasses all sub-sets of SCRM, such as cybersecurity, software assurance, obsolescence, counterfeit parts, foreign ownership of sub-tier vendors, and other categories of risk that affect the supply chain. (Committee on National Security Systems Directive 505 Supply Chain Risk Management 29 August 2017)

Technical Intelligence Data—Data required for Departmental decision analysis and capability development, design, operation, test, evaluation, and training. Technical Intelligence Data includes threat capabilities, threat Modeling and Simulation (M&S) software models, Signatures, Characteristics and Performance, Electronic Warfare Integrated Reprogramming and other technical data types as may be required to perform the specified tasks.

Attachment 2

ACQUISITION INTELLIGENCE ACTIVITIES

A2.1. Responsibilities. Acquisition Intelligence Analysts are the focal point for acquisition intelligence, effectively integrating intelligence into capability development, R&D, test, and the acquisition life cycle. The integration of intelligence activities is the collective responsibility of MAJCOM, FLDCOM, DRU, FOA (e.g., Air Combat Command, Space Operations Center, STARCOM, Air Force Special Operations Command, Air Mobility Command, and Air Force Global Strike Command) and materiel focused AFMC and SSC. This includes command leadership from functional directorates executing capabilities development and senior program/project portfolio offices, down to individual program/project managers, engineers, and AIAs.

A2.2. Tenets. Effective acquisition intelligence is:

A2.2.1. ***Relevant*** , providing meaningful support that enables program/project decision makers to make proactive decisions in advance of the threats.

A2.2.2. ***Iterative*** , providing timely intelligence inputs to the materiel effort along acquisition life cycle timelines in an evolving fashion dictated by materiel development and sustainment needs. Although many existing DoD and DAF policies governing the acquisition life cycle mandate discrete events, times, and artifacts in which intelligence is procedurally integrated, acquisition intelligence must be part of day-to-day capability development, test, R&D, and acquisition life cycle activities above and beyond episodic touchpoints, starting at requirements development.

A2.2.3. ***Tailored*** , focusing products and processes in a timely manner to meet the needs of the users while reducing extraneous information.

A2.2.4. ***Collaborative*** , requiring partnership across acquisition, intelligence, operations, counterintelligence, cybersecurity, and requirements communities to identify and resolve intelligence issues related to new and evolving programs/projects.

A2.2.5. ***Discoverable*** , so that all of those with the collective responsibility for capability development, R&D, test, and the acquisition life cycle have access to the best available and consensus analysis of relevant threats.

A2.3. Requirements. The following conditions are necessary for intelligence to be effectively integrated within acquisition life cycle processes:

A2.3.1. The analysis & production of foundational intelligence with an emphasis on technical intelligence data and threat systems forecasts.

A2.3.2. Subject to data owner approval, a comprehensive understanding of, and complete, access to 1) all aspects of the supported capability development or acquisition life cycle activity, program/project, or function; 2) the relevant intelligence applicable to the supported capability development, life cycle activity, program/project, or function to include applicable IC Controlled Access Programs and Special Access Programs.

A2.3.3. Integration of intelligence activities into all capability development and acquisition life cycle processes and selected documents (e.g., Initial Capabilities Document, Capabilities Development Document) throughout the acquisition life cycle of the program/project.

A2.3.4. Tailored application of intelligence data and processes for each capability development and life cycle activity, program, or function.

A2.3.5. Trained AIAs assigned to organizations conducting capability development, test, R&D, and acquisition life cycle activities who have regular access to program/project decision authorities and are part of program/project decision making bodies/events to inform program/project risk, cost, schedule, and performance with relevant and timely intelligence.

A2.3.6. Integration with the command's intelligence and capabilities development staffs to ensure Initial Capabilities Document and Capabilities Development Document contain requirements to mitigate known and expected future threats, and that these threat assessments are accurate/thorough.

A2.4. Intelligence Sensitivity Determination. A program/project is intelligence-sensitive if at any point in its life cycle: 1) it produces, consumes, processes, or handles intelligence information; or 2) it requires intelligence-related doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P), or intelligence-related planning and direction, collection, processing, analysis and production, and dissemination intelligence support; or 3) it requires threat support to make programmatic decisions. AIAs are responsible for conducting Intelligence Sensitivity Determination and working with the program/project to determine the risk of not integrating intelligence, and whether or not the risk is unacceptable, based in part on an assessment of competing demands for intelligence from the DAF, DoD, and other national security priorities. The Intelligence Sensitivity Determination aids early development of rough-order-of-magnitude estimates for intelligence support to, and risk management of, the program.

A2.5. Intelligence Supportability Analysis (ISA). ISA is the process by which intelligence, acquisitions, and requirements communities identify, plan for, and address intelligence-related requirements and supporting intelligence infrastructure (e.g., ISR collection and analysis, classified facilities, intelligence-related DOTMLP-F) necessary to successfully acquire and employ capabilities, thereby ensuring intelligence supportability requirements are noted/documented/addressed. ISA will begin as early as possible and continue throughout the system life cycle, IAW command guidance, and shall be conducted for all intelligence-sensitive programs.

A2.5.1. IAW DAFI 63-101/20-101 a program/project will ensure ISA is fully integrated into program/project decisions and system engineering. This will include working with AIAs to ensure ISA is integrated into major decision forums/processes to include but not limited to analysis of alternatives, Acquisition Strategy Panels, Initial Capabilities Document, Capabilities Development Document, requirements boards, and requirements oversight council meetings. ISA will also serve as continuity for acquisition intelligence support to the program throughout its life cycle. Program/project managers will ensure ISA helps to drive program/project maturation, to include closing intelligence supportability gaps.

A2.6. Intelligence in the Acquisition Strategy. As described in Title 10 USC § 4211, *Acquisition Strategy* and DAFI 63-101/20-101, program managers and program AIAs will state the program's approach to integrating intelligence as part of the program's documented acquisition strategy, in a cost-effective manner to meet program/project objectives. Integrating intelligence at the start of acquisition strategy development will provide program/project managers greater flexibility in risk mitigation and program/project decision making. In the cases where a program will be seeking a waiver to a regulatory artifact, that waiver will be documented within the acquisition strategy.

A2.7. Test and Evaluation Master Plan. As part of Test and Evaluation Master Plan development, AIAs will in conjunction with the Chief Developmental Tester (Test Manager) and AFOTEC/A-2N, specify the threat types required for test.

A2.8. Configuration Steering Board (CSB). The CSB reviews all requirements changes and any significant technical configuration changes that may result in cost and schedule impacts to the program. IAW DAFI 63-101/20-101, AIAs will ensure relevant intelligence factors, to include non-threat related factors such as ISA, are addressed at the annual program CSB or will work with the program managers to make them part of an out-of-cycle CSB. The goal is to ensure intelligence-driven changes to the program are made early in the lifecycle, so the program outpaces future threats and has the requisite level of ISR interoperability. For instances where the threat has placed the program's Key Performance Parameters at risk, specifically, cases where a CIP has been breached, the CSB will address those issues.

A2.9. Intelligence Health Assessment (IHA). IAW DAFI 63-101/20-101, the IHA is an assessment of a program or project intelligence supportability risks and helps ensure a program/project addresses risk management. IAW command guidance, an IHA will be completed and reviewed by program/project managers. When accomplished, IHA factors will be evaluated and incorporated into the program's overall risk assessment. IHAs may be directed to support programmatic and service level reviews. IHAs are often event-driven and support selected capability development, test, R&D, and acquisition life cycle events/forums at the program/project, command, service, or joint-levels (program/project reviews, boards, program milestones, etc). IHAs can also be updated periodically as significant intelligence related risks are discovered or mitigated.

A2.10. Technical Intelligence Data Requirements Management. IAW CJCSI 3318.01 *Acquisition Intelligence Requirements Annual Priorities and Risk Management Framework*, AF A2/6 and SF/S2 will function as the technical intelligence data requirements and prioritization manager to inform, document, and optimize Defense Intelligence Enterprise support and production across threat M&S software models, signatures, characteristics and performance, and electronic warfare integrated reprogramming. The process for management and prioritization will be promulgated via separate guidance.

A2.11. ISR Interoperability and Capability Review. IAW the JCIDS Manual, a capability being developed needs to integrate with the ISR collection and dissemination ecosystem if the materiel system can collect, disseminate, or must receive intelligence or other relevant battlespace information. This includes the interoperability of subsystems whose primary purpose supports the system's primary mission or system self-protection even if further dissemination of the collected data is not the subsystem's primary purpose. Subsystems may include components that collect or must receive or store adversary electromagnetic signals, geospatial information (e.g., imagery,

terrain data, coordinates), or non-electromagnetic threat system signatures. In coordination with AIAs, programs will review interoperability and capability information and report findings IAW command guidance.

A2.12. Threat Analysis and Tailoring. Led by program managers, MAJCOM, FLDCOM, DRU, FOA and AFMC or SSC (materiel-focused commands) will ensure foreign intelligence threat analysis is fully integrated during all phases of capability development, R&D, test, and the acquisition life cycle with an emphasis on ensuring threat analysis informs key program/project decisions related to risk, cost, schedule, and performance. AIAs will lead this effort and will "tailor in" threat analysis for the program/project based on its requirements and the stage of development or acquisition (reference DoDI 5000.85 *Major Capability Acquisition*, and DoDI 5000.02 *Operation of the Adaptive Acquisition Framework*). Threat tailoring helps to ensure materiel systems and activities are designed from the start to outpace current and future adversary capabilities. Although a collective responsibility, unit/program/project AIAs and acquisition intelligence functional leaders will lead the overall threat integration and will integrate threat intelligence into day-to-day capabilities development, test, R&D, and acquisition life cycle activities to include force modernization forums such as DAF capabilities planning forums, Acquisition Review Boards (also referred to as DAF Review Boards), Acquisition Strategy Panel, CSB, Milestone Decision forums, Threat Working Groups, and Intelligence Support Working Groups, among others.

A2.13. Threat Analysis Collaboration.

A2.13.1. Threat Analysis Collaboration Tasks. Program AIAs will leverage and collaborate with experts from disparate communities and agencies (intelligence, acquisitions, operations, DoD) at all classification levels (including IC Controlled Accesses Programs) to formulate a relevant and timely threat picture that fits the needs of the program/project based on a complete understanding of the program's/project's technology attributes, Key Performance Parameters, and critical components/functions. AIAs will collaborate with program personnel, (in coordination with the program/project manager) IC and service intelligence center threat analysts, counterintelligence representatives, and others to establish and document the program's threat integration strategy as a subset of the program's acquisition strategy. AIAs will include a plan to:

A2.13.1.1. Decide on the relevant threats or classes of threats to the program/project or activities.

A2.13.1.2. Determine the digital threat representation products and data required and how they will integrate with program/projects (e.g., threat databases, M&S).

A2.13.1.3. Review and modify existing or determine new CIPs that place the program/project Key Performance Parameters at risk.

A2.13.1.4. Determine how the program/project will incorporate the threat baseline and update the intelligence assessments on the current and future threats (threat forecasts/roadmaps).

A2.13.1.5. Review the threat intelligence assessments and supporting data, to include models and simulations, used to inform the program for relevance, timeliness, quality, and adherence to Intelligence Community Directive (ICD) standards as required in this instruction (see A2.14.3.1. Analytic Standards and Integrity).

A2.13.1.6. Conduct detailed technical analysis to ascertain potential program/project vulnerabilities, risks, threat-relevant supportability requirements, ISR dependencies, and design recommendations.

A2.13.1.7. Ensure traceability and transparency so program/project offices understand how the data and information supporting the threat assessment was derived. This is critically important when forecasting threats that do not exist yet.

A2.13.2. Threat Analysis Collaboration Methods. MAJCOM, FLDCOM, DRU, FOA and AFMC or SSC (materiel-focused commands) should consider providing tailored, command-specific guidance on threat analysis collaboration methods, forums, and best practices. Program AIAs, program/project managers and operational test shall include the following personnel in threat analysis collaboration efforts: service intelligence center threat analysts, test management leadership from the AFMC or SSC, user/operators, counterintelligence representatives (AFOSI), program and intelligence representatives from the MAJCOM, FLDCOM, DRU, or FOA, operational test (AFOTEC), and other program or intelligence personnel as the program/project managers and AIAs see fit. Threat analysis forums can provide a means for programs to engage the threat analysis community and MAJCOM, FLDCOM, DRU, FOA and AFMC or SSC to accomplish threat analysis collaboration tasks and re-validate/adjust the threat integration strategy. They can also help identify emerging weapons and technologies that may threaten a programs long-term viability (mission effectiveness and survivability). Collaborating to identify and update program threats will help the justification of threat-driven modifications to the program.

A2.13.3. Threat Analysis & Products.

A2.13.3.1. Analytic Standards and Integrity. All AIAs and production will adhere to the analytic standards delineated in ICD 203 *Analytic Standards*, ICD 206 *Sourcing Requirements for Disseminated Analytic Products* and DAFMAN 14-401 *Intelligence Analysis and Targeting Tradecraft/Data Standards*. Further, AIAs will raise concerns pertaining to biased analysis or lack of analytic integrity or objectivity through their chain of command and Ombuds channels, IAW DAFMAN 14-401. If intelligence products are not available, or do not meet the needs of the program, AIAs should work with the IC to develop intelligence collection requirements to fill the gap. Plans for closing gaps can be documented in artifacts such as the IHA, the Acquisition Strategy, Partnership Production Agreements, Test & Evaluation Master Plans, and M&S Strategies among others.

A2.13.3.2. Threat Roadmaps, Forecasts, and Scenarios. IAW command guidance, AIAs in collaboration with program/project managers will integrate threat roadmaps, threat forecasts, and future threat scenarios to shift away from making reactive adjustments to the program and toward implementing proactive changes in advance of the future threat. The future threat environment must be the focus of threat analysis and threat products supporting capability development and the acquisition life cycle, with an emphasis on the R&D conducted by potential adversaries and their emerging and disruptive technologies.

A2.13.3.3. Critical Intelligence Parameters (CIP). A CIP clearly defines the performance threshold at which a foreign system or capabilities may compromise mission effectiveness of the U.S. system or capability based on its Key Performance Parameters and Key Systems Attributes. CIPs define areas of highest priority for ongoing intelligence reporting that ensures program achievement of Key Performance Parameters and Key Systems

Attributes. The focus of a program's intelligence integration will be threat forecasts that enable a program to adjust so CIPs are never breached. Military doctrine, tactics, strategy, and expected employment of systems will be considered in the CIP. CIPs should be built around the specific quantity, type, force mix, system capabilities, and technical characteristics or performance thresholds of a particular foreign capabilities of greatest concern to the program and IC (e.g., radar cross-section, armor type or thickness, or acoustic characteristics).

A2.13.3.4. CIP Development. MAJCOM, FLDCOM, DRU, FOA AIAs and/or program/project sponsors develop CIPs in coordination with service intelligence centers, and other IC agencies as required soon after system Key Performance Parameters are established and update them across the system life cycle (for additional information, reference DAFI 63-101, DoDI 5000.86, DIAI 5000.002 and CJCSI 5123.01I). AFMC and SSC will mature and/or retire existing CIPs based upon program maturation and evolution of related threats. The program AIA will work with the program/project manager to address impacts from critical threats to the program/project and discuss mitigation actions for CIP breaches at an annual or out-of-cycle CSB.

A2.13.4. Publicly Available Information & Open-Source Intelligence. If AIAs research or collect publicly available information, they will do so in accordance with local command policies which will include the use of appropriate managed attribution tradecraft and technology and comply with applicable open-source intelligence policies and standards, as well as DoDM 5240.01 *Procedures Governing the Conduct of DoD Intelligence Activities*.

A2.14. Digitalized Threat Representations. Digitalized threat representations leverage digital technologies and digitized data to characterize threats in a manner that augments primarily human threat analysis processes with software or machine-driven methods. They include M&S, signatures, and databases among others. Where possible data should be centralized, standardized and discoverable. Programs/projects shall identify digitalized threat representation requirements early in a program/projects life cycle and actively engage and support the IC in adequately planning, resourcing, and coordinating production or updates.

A2.14.1. Threat System M&S. IAW CJCSI 3318.01, AF/A2/6 and SF/S2 will function as the M&S requirements and prioritization manager to inform, document, and optimize Defense Intelligence Enterprise support and production. Programs shall consider integrating digitalized threat M&S products into program/project development. Programs and AIAs will collaborate with organic M&S agencies and service intelligence centers, other IC agencies, and MAJCOM, FLDCOM, DRU, FOA to develop the threat M&S portion of the intelligence integration strategy.

A2.14.2. M&S Standards. Threat system M&S products are considered intelligence products and must adhere to ICD, most notably the standards for analysis, sourcing, and utility (ICDs 203, 206, and 208). Traceability and maintainability are key aspects of adherence to IC standards: programs must be able to reliably trace the characteristics of threat M&S back to the source of its underlying intelligence data, and threat M&S must be maintained over time as threat data and technology evolve. Program/project AIAs shall maintain awareness of available threat M&S capabilities and help lead their integration into the program. The integration of threat M&S is most effective when the programs M&S environment is designed

with the IC's standardized threat M&S product types and technical architecture standards in mind.

A2.14.3. Threat System Databases. Threat system databases are considered intelligence products and must adhere to ICD 203 *Analytic Standards*. Threat system databases are maintained by the IC and are also a valuable source of digitalized threat information. Like threat M&S products, program integration of threat system databases is most effective when the program is designed with the IC's standardized threat system databases in mind.

A2.15. Acquisition Intelligence Coordination with Counterintelligence, Supply Chain Risk Management (SCRM), and Cybersecurity. In addition to analysis of foreign threat systems, program threat integration will include analysis of foreign intelligence threats, cyberspace threats, and supply chain threat assessments to include potential vendors with foreign ownership, control, or influence, as part of SCRM. IAW DAFI 63-101/20-101, and as outlined in DoDI 5000.83_DAFI63-113 *Technology and Program Protection to Maintain Technological Advantage* and DoDD 3000.16 *Vendor Threat Mitigation*, programs must manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; foreign influence, foreign intrusion to include both maligned intent and inadvertent introduction of materiel into supply chains and reverse engineering, to include the use of anti-tamper techniques. Intelligence will inform program risks in these areas and factor into the program's protection strategy and associated artifacts to include the Program Protection Plan, Science and Technology Protection Plan and Security Classification Guide.

A2.15.1. Foreign intelligence threat analysis will be done in collaboration with AFOSI IAW DoDI O-5240.24 *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition*. Although AFOSI is the lead for counterintelligence support to programs/projects, program AIAs, IAW command guidance, must proactively engage AFOSI to help integrate foreign intelligence threat analysis and counterintelligence into the Program Protection Plan, Science and Technology Protection Plan.

A2.15.1.1. IAW DoDD 5205.07, Special Access Program (SAP) Policy and DAFI 16-701_DAFGM2023-01, Management, Administration and Oversight of Special Access Programs identifies AFOSI Office of Special Projects (AFOSI/PJ) the office responsible for services to include program security, counterintelligence, counterespionage, major criminal investigations, technical security, and countermeasure services, and other specialized AFOSI activities for SAPs. AFOSI/PJ is also responsible to develop a CI support plan for each Special Access Program.

A2.15.1.2. In addition to foreign intelligence threats, programs/projects AIAs will work with their local SCRM networks and AFOSI to integrate analysis of supply chain threats, to include vendors with foreign ownership, control, or influence as part of program/project SCRM. Intelligence related to supply chain threats both maligned and inadvertent is not always common to traditional intelligence production; therefore, AIAs must leverage a wider range of analytical tools and sources. This starts with MAJCOM, FLDCOM, DRU, FOA and AFMC or SSC (materiel-focused commands) offices responsible for SCRM and includes leveraging publicly available information, special access programs, and possibly collaborating, through their command, with organizations like the Department of Defense Cyber Crime Center (DC3), Defense Technology Security Administration (DTSA), the Air

Force Office of Commercial and Economic Analysis (OCEA), Vendor Threat Mitigation, and the U.S. Department of Commerce (DOC) (DOC SCRM Working Group).

A2.15.2. Cyberspace provides distinctive threat vectors that programs must consider in the threat intelligence section of their acquisition strategy. AIAs should understand the major cyberspace vulnerabilities of their programs/projects and work to integrate relevant and tailored threat assessments. Although not required, AIAs may find it useful to document cyber threat assessments in an Adversary Cyber Threat Assessment (ACTA) report IAW MAJCOM, FLDCOM, DRU, FOA or AFMC or SSC guidance.

A2.16. Intelligence Production Requirements & Collection Requirements. If the intelligence required for a program is not contained in published intelligence or captured as part of the day-to-day dialogue between programs and IC analysts, programs, led by their AIAs, may be required to submit production requirements and collection requirements in accordance with parent command guidance and processes. AIAs will document production requirements and collection requirements in program documentation and periodically update program personnel on their status.

A2.17. Intelligence Oversight.

A2.17.1. U.S. Persons Information. U.S. Persons Information may only be collected in accordance with DoDM 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities and local command policies.

A2.17.2. Proper Use Memorandum. Materiel Enterprise personnel may find themselves supporting programs developing future imagery intelligence capabilities. When these programs operate over domestic areas (defined as the land areas of the 50 United States, the District of Columbia, and the territories and possessions of the United States, to a 12 nautical mile seaward limit of these land areas), a Proper Use Memorandum may be required, per intelligence oversight guidance found in AFI 14-404, Intelligence Oversight.

Attachment 3

ACQUISITION INTELLIGENCE ROLES

A3.1. Acquisition Intelligence Analysts (AIAs). AIAs are DAF professionals whose primary duty is to integrate intelligence into the capability development, test, R&D, and acquisition life cycle processes. Intelligence integration activities include, among others: threat support, to ensure capability development and acquisition functions are fully threat informed (see **paragraph A2.14.3.1**. Analytic Standards and Integrity); intelligence supportability analysis, to identify intelligence necessary to successfully acquire and employ DAF capabilities; ISR interoperability reviews, to ensure materiel systems can integrate with the ISR ecosystem; and intelligence production requirements development, to levy the requirements for specific types of intelligence to support materiel functions, system or projects. DAF professionals must complete the Acquisition Intelligence Analyst Certification Program (AIACP) within 18 months of being assigned to an AIA-coded billet. AIAs assigned to AIA-coded billets must also adhere to the AIACP Guidebook (**https://daf.badgr.com/public/badges/WlZ5Pq_ATT-lhKb6QSJpXw**).

A3.1.1. Acquisition intelligence is a multidisciplinary function, and the AIA workforce should include: intelligence personnel, who analyze the threat, conduct ISR interoperability reviews and intelligence supportability analysis; engineers, who provide additional insight into the technical aspects of threat systems; M&S experts, who assist with the integration of digital threat M&S; and data scientists, who analyze and interpret complex digital data to enable threat informed acquisition decision-making. AIAs will also leverage, and receive support from, other acquisition functions like financial analysts who can estimate the cost of intelligence-driven changes to the program and SCRM analyst.

A3.1.2. Directors of Intelligence (DOIs). In coordination with the command A2/S2, AFMC or SSC may appoint an intelligence professional as the DOI for a PEO. In this role, DOIs serve as the senior AIA for the PEO and lead the execution of acquisition intelligence for the PEO and subordinate programs and give guidance and direction to program AIAs. Commands may also choose to designate an intelligence professional to serve as the Senior Intelligence Officer to perform non-AIA intelligence and security related duties for the parent command and the local installation. Commands may also choose to combine DOI and Senior Intelligence Officer functions into a single position.

A3.1.3. Program/Project AIA. If designated by AFMC or SSC, program/project AIAs will report to a senior program/project leader or the senior program/project AIA and execute acquisition intelligence functions for the program/project. Commands may also choose to designate an AIA as the Senior Intelligence Officer to perform non-AIA intelligence and security related duties for the parent command and local installation (e.g., force protection, classified facility management, personnel security).

A3.1.4. For materiel program offices, per DAFI 63-101/20-101, AIAs take program direction from the program/project manager, and the intelligence function shall be integrated into the program like the integration of logistics, engineering, contracting, and financial management.