BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 14-111

10 JANUARY 2005

Intelligence

INTELLIGENCE IN FORCE MODERNIZATION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ USAF/XOIIA-F (Mr. Bruce Herndon)

Certified by: HQ USAF/XOII (Mr. Kenneth K. Dumm)

Supersedes AFI 14-111, 1 Oct 1997

Pages: 65

Distribution: F

This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations*, by providing guidance in identifying, tasking, and acquiring intelligence essential to force modernization processes of the U.S. Air Force. This includes research and development, acquisition, test, and sustainment activities as well as associated planning, integration, requirements generation and capabilities development processes. This AFI implements policies in Department of Defense Instruction (DODI) 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*; DODI 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*; Department of Defense Directive (DODD) 5000.1, *The Defense Acquisition System*; DODI 5000.2, *Operation of the Defense Acquisition System*; Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01, *Joint Capabilities Integration and Development System*; Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3170.01, *Operation of the Joint Capabilities Integration and Development System*; CJCSI 6212.01, *Interoperability and Supportability of Information Technology and National Security Systems*; CJCSI 3312.01, *Joint Military Intelligence Requirements Certification*; National Security Space (NSS) Acquisition Policy 03-01; Defense Intelligence Agency (DIA) Regulation 55-3, *Intelligence Support for Defense Acquisition Programs*; AFI 10-601, *Capabilities Based Requirements Development*; AFPD 90-11, *Planning System*; AFPD 62-2, *System Survivability*, AFPD 63-1, *Capability-Based Acquisition System*; and AFPD 99-1, *Test and Evaluation Process*. This AFI applies to all Air Force personnel who participate in force modernization processes and to all actual or potential Air Force technology projects and acquisition programs. Adherence is mandatory, except when statutory requirements, DOD, or Joint Staff (JS) directives override. If there is any conflicting guidance between this AFI and DOD 5000-series, CJCS 3170-series, the Federal Acquisition Regulation (FAR), and/or the Defense FAR Supplement, the DOD 5000-series, CJCS 3170-series, FAR, and/or DFAR Supplement shall take precedence. Any organization may supplement this instruction. Ensure all records created as a result of this AFI are maintained in accordance with AFMAN 37-123, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://webrims.amc.af.mil/**. This AFI is approved for public release; distribution is unlimited. Send

proposed supplements or recommended changes to this instruction to Headquarters (HQ) USAF/XOI, 1480 Air Force Pentagon, Washington, DC 20330-1480; email:
mailto:AFXOI.Workflow@pentagon.af.mil.

SUMMARY OF REVISIONS

Revisions to AFI 14-111 consisted primarily of adimnistrative and organizational changes. Organizational changes to the document involved updating the roles and responsibilities of applicable organizations section in **Chapter 3**. Finally, **Attachment 5** – ISP Procedures and Formats was added to reflect an update to the acquisition document process.

Chapter 1

INTELLIGENCE IN FORCE MODERNIZATION PROCESS

1.1. Introduction. Intelligence integration in support of Air Force and Joint systems development has never been more important or challenging than it is in today's environment. When intelligence is not fully integrated into the Air Force's modernization processes, the results often include scheduling delays, costly work-arounds, and unplanned adjustments to Operations & Maintenance, and Pre-Planned Product Improvements (P3I). As future systems become more intelligence-dependent, the cost of omitting intelligence integration will increase. This AFI outlines process and policy to ensure intelligence is integrated appropriately within AF modernization activities.

1.1.1. Desired Effects. To provide qualitative and quantitative improvements in performance and capability and to reduce acquisition time and cost.

1.1.2. Capabilities. The following capabilities are necessary for intelligence to be effectively integrated within force modernization processes:

1.1.2.1. A common understanding of program/initiative intelligence needs across the intelligence, operations, and acquisition communities.

1.1.2.2. A working familiarity of intelligence infrastructure and threat analysis among acquisition/operational authorities and their associated intelligence stakeholders. In-time delivery of tailored/stock intelligence products or customer-funded alternatives.

1.1.2.3. Integration of Intelligence in Force Modernization (IFM) stakeholders into planning, programming, and decision activities to weigh costs/benefits/tradeoffs.

1.1.2.4. An ability to analyze and compare a variety of intelligence requirements and deficiencies across numerous programs/initiatives so as to be able to recommend and advocate prioritized, efficient solutions at reasonable cost.

1.1.3. IFM Process. The IFM process typically involves the following steps:

1.1.3.1. Identifying intelligence-sensitive programs/initiatives.

1.1.3.2. Analyzing intelligence need and identifying the requisite level of effort necessary to address that need.

1.1.3.3. Conducting Intelligence Infrastructure Analysis (IIA).

1.1.3.4. Planning for and developing materiel and non-materiel intelligence solutions.

1.1.3.5. Advocating for resources and deficiency resolution.

1.1.4. Primary Instruments. The primary instruments for implementing IFM are the Intelligence Support Steering Group (ISSG), the Intelligence Support Working Group (ISWG) and the Threat Steering Group (TSG). Success in IFM depends upon the empowerment of Implementing MAJCOM/INs and their Directors of Intelligence (DIs) to engage appropriately in program/initiative execution.

1.2. Identifying Intelligence-Sensitive Programs/Initiatives. In general, the IFM process begins when a force modernization effort is identified as intelligence-sensitive. Intelligence-sensitive efforts include those that produce, consume, process, or handle intelligence data. The effort could be a new acquisition program/initiative, Battlelab initiative, maturing technology, an Analysis of Alternatives (AoA) concept study, an Advanced Concept Technology Demonstration (ACTD), an upgrade to an existing weapon system, or other acquisition related effort. The Battlespace Awareness representative to the Joint Capabilities Integration and Development System (JCIDS) Gatekeeper organization will determine those programs that produce, consume, process, or handle intelligence data, for which joint intelligence certification applies. Once intelligence sensitivity is identified, preferably in the conceptual phase, the IFM community assembles to help shape the effort and ensure requirements for intelligence are effectively addressed. This normally results in the conduct of Intelligence Infrastructure, Threat, and Cross-Program Analyses.

1.2.1. In 2004, SAF/AQ, AF/XI, and the AF-CIO sponsored an effort to streamline the requirements process for Air Force acquisition programs/initiatives. The process that resulted from this effort is called the Lean IT/NSS Acquisition Process. This process focuses on sharing key information throughout the life of each program or system in lieu of generating, staffing, and reviewing redundant documentation. The primary goal of the new process is to acquire systems that, once fielded, will be secure, interoperable, supportable, sustainable and usable (SISSU). To make this goal attainable, the Lean IT/NSS Acquisition Process aims to ensure stakeholder involvement early and often, and provide a mechanism for SISSU needs to be communicated across all stakeholder organizations. Additional information can be found on NIPRNET: <**https://www.xi.hq.af.mil/xiw/xiws/Lean_Reeng/**>.

1.3. Intelligence Infrastructure Analysis (IIA). IIA is the process employed by programs to assess the level of intelligence support required to achieve mission success at Initial Operational Capability (IOC) and throughout its life-cycle. AF intelligence documents the requirements for intelligence threat and infrastructure support necessary to successfully acquire and employ future Air Force capabilities. IIA should begin as early as possible during system development processes for all intelligence-sensitive programs/initiatives. If IIA is not conducted, the Air Force risks developing systems that are sub-optimized or unsupportable. This analysis supports the development of the intelligence content of the Information Support Plan (ISP) (see **Attachment 3**) and the intelligence requirements certification that are directed by CJCSI 3170.01 and described in CJCSI 3312.01.

1.3.1. IIA Content. As a minimum, IIA should identify, as specifically and completely as possible, projected requirements for intelligence products, information, or services to include required performance, descriptive, or qualitative attributes.

1.3.2. IIA Documentation. IIA results should be documented as specified in this AFI. Proper documentation of this analysis will: 1) show traceability to the system's operational baseline; 2) identify derived intelligence requirements and intelligence infrastructure (people, systems, procedures, products, etc.) needed to satisfy the operational requirements; 3) highlight any gaps or system intelligence deficiencies between the required infrastructure and the existing infrastructure; 4) highlight time-phased courses of action necessary to ensure these system intelligence deficiencies are resolved before such time as the support is needed; and 5) identify estimated costs associated with each proposed solution.

1.4. Cross-Program Analysis (CPA). CPA involves an analytical effort designed to “look across” all intelligence-sensitive programs/initiatives and the related intelligence deficiencies. The purpose of CPA is to identify common requirements and achieve synergies within resulting common solutions. Synergies between programs/initiatives and cost savings are realized when solutions are identified that support multiple programs/systems. An additional aspect of CPA is to identify system or program integration issues. In addition, linkage of documented requirements with multiple customer sets serves to strengthen AF requirements forwarded to the larger Intelligence Community for action.

1.5. Intelligence Support Steering Group (ISSG). The ISSG initiates the IFM process for program/initiatives, preferably in the conceptual phase (pre-MS A/KDP A). The ISSG assigns organizations responsibilities for intelligence support, assesses (at a high level) the type of intelligence support each program/ initiative would likely need, starts the necessary processes to build intelligence support cost estimates for insertion into funding processes, and provides an overview of the recommended process needed to identify intelligence requirements and deficiencies. The ISSG is comprised of key personnel including the program/initiative lead, intelligence personnel, and other IFM stakeholders (see **Attachment 4**).

1.6. Intelligence Support Working Group (ISWG). The ISWG brings functional representatives from throughout the intelligence and acquisition communities together to ensure all intelligence considerations for the developing system or capability are addressed. The goal is to derive and develop the intelligence requirements and deficiencies, to research and develop potential solutions to the deficiencies, to create action plans to accomplish those solutions, to estimate solution costs, and to document results in the Weapon Systems Intelligence Support Requirements Database (WSISRD). This information is also integrated into the ISP as the intelligence content and forms the basis for Section 9, *Intelligence Supportability*, of the Capability Development Document (CDD) and Capability Production Document (CPD).

1.6.1. ISWG Participants. Either the program representative designated to oversee intelligence support planning or the intelligence partner who is leading intelligence infrastructure analysis typically chairs ISWGs. The ISSG-designated intelligence partner should participate in ISWGs and ensure the correct intelligence community participants attend the meetings. ISWGs are composed of the following major interest groups:

1.6.1.1. System developers and supporters.

1.6.1.2. System testers.

1.6.1.3. Operational users.

1.6.1.4. Intelligence providers (Intelligence Community representatives, intelligence functional POCs, intelligence requirements managers, etc.).

1.6.2. Difference Between the ISSG and the ISWG. An ISSG is very broad-based and involves only the highest level of program management. It brings together the program office, resource manager, and key intelligence support organizations for the purpose of identifying key roles and responsibilities. ISSGs lay the groundwork for subsequent ISWGs. The ISWG is a follow-on meeting to the ISSG that is convened as a means of identifying all intelligence requirements that must be achieved in order for the program to be successful at IOC and throughout its life-cycle. ISWGs involve detailed analyses and involve every aspect of the program's supported mission from intelligence collection to unit-level mission planners and operators. **Figure 1.1.** and **Figure 1.2.** are visual depictions of where the ISSG and ISWG occur in relation to the DOD 5000 and Space Acquisition Models.

Figure 1.1. ISSG & ISWG in relation to the DOD 5000 Model.

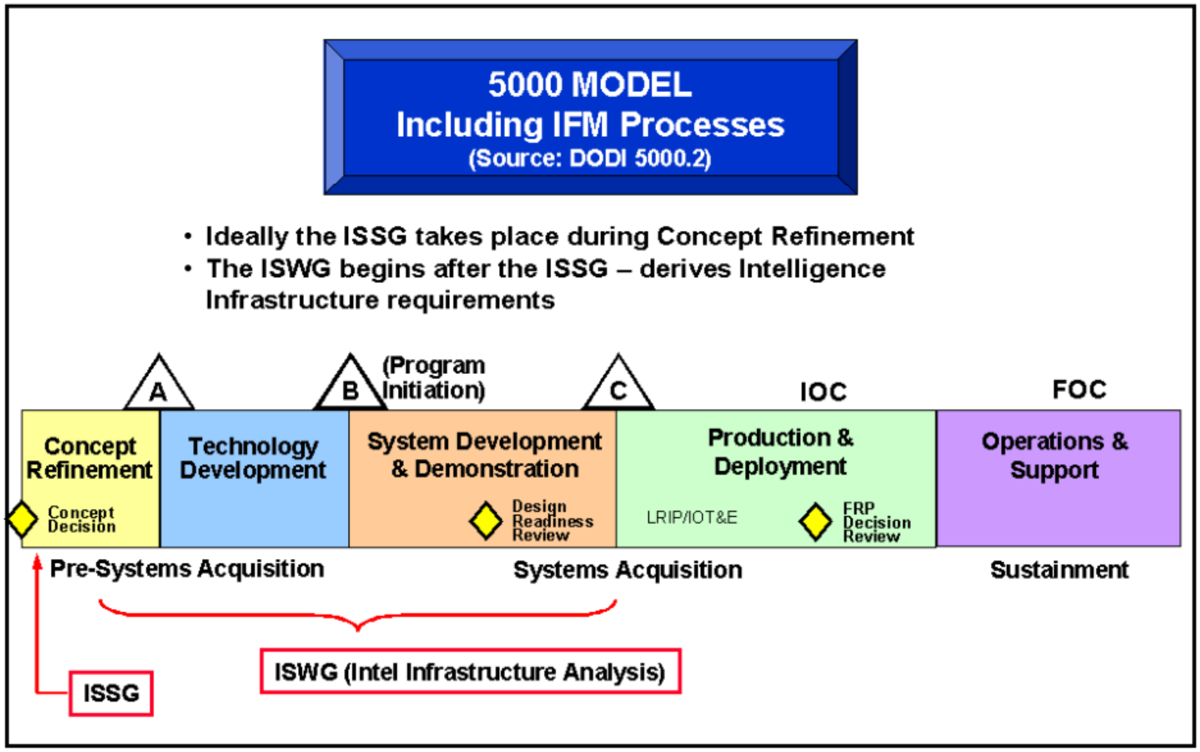
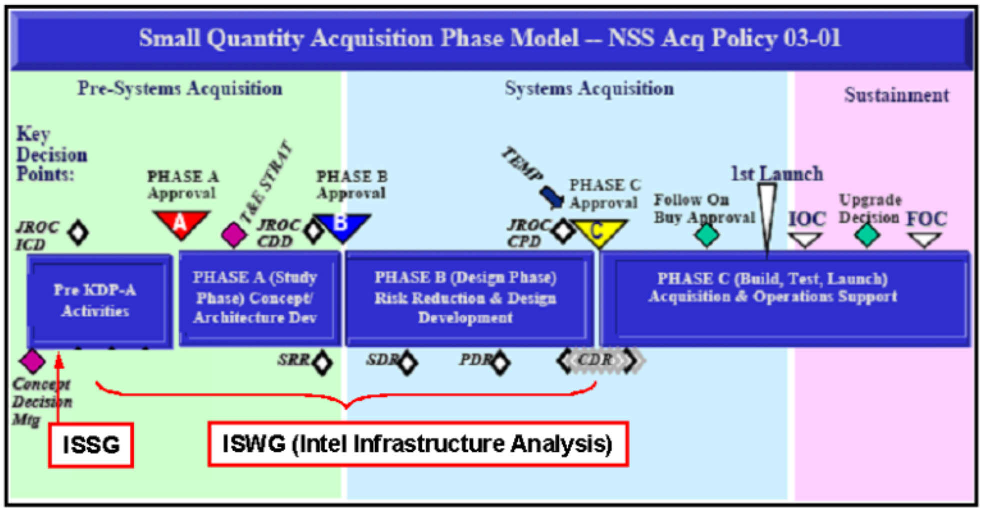
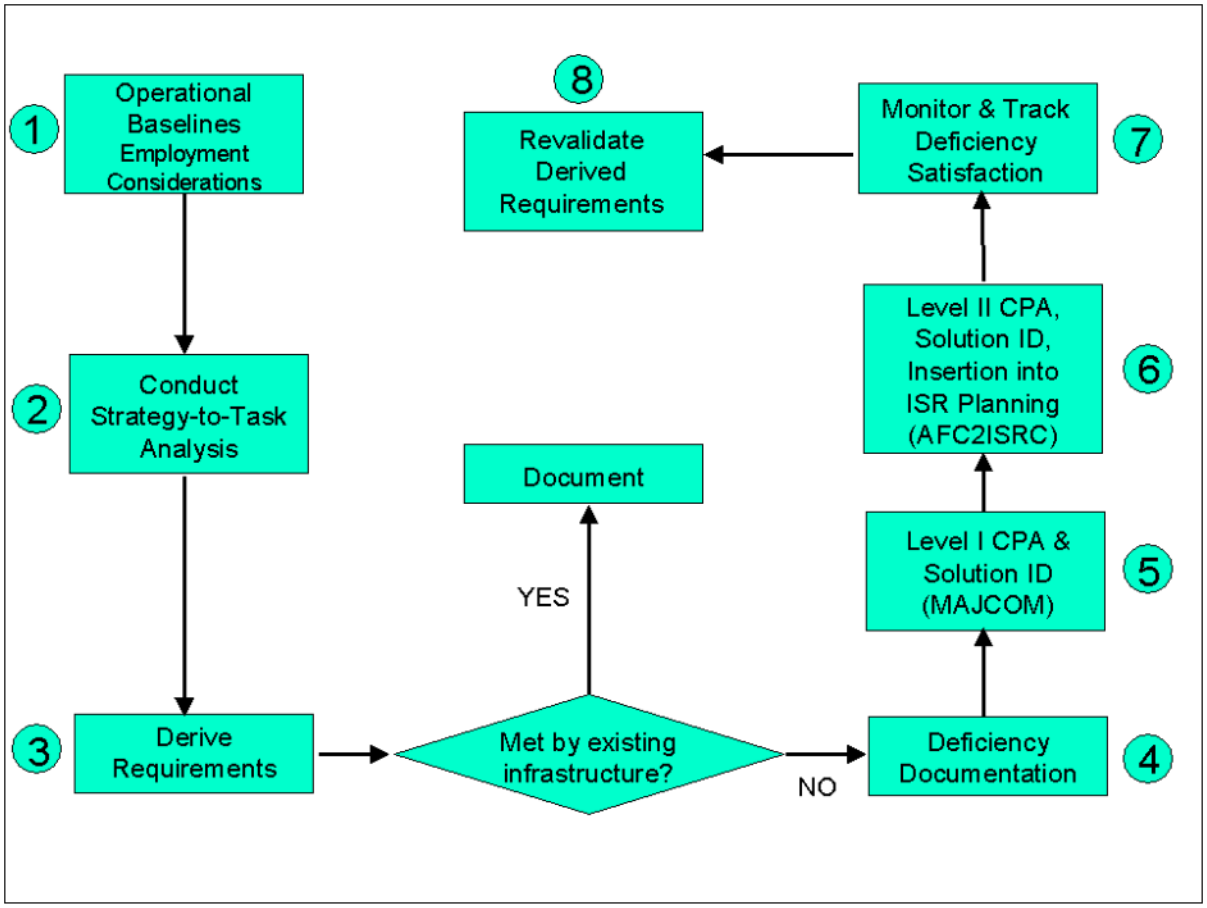


Figure 1.2. ISSG & ISWG in relation to the Space Acquisition Model.



1.7. Derived Requirements Generation Process: IIA & CPA. IIA is core to the activities of the ISWG. The same basic four steps to conduct IIA should be followed regardless of the weapon, information, C2, or ISR system that is being analyzed. Figure 1.3. depicts the process flow and eight steps for derived intelligence requirements identification, documentation and analysis. IIA is comprised of the first four steps of the derived requirements generation process. The next three steps include Level I CPA, Level II CPA, and the monitoring and tracking of deficiency satisfaction. After completing the initial seven steps, requirements must be revalidated every year to ensure that any significant changes have been taken into consideration.

Figure 1.3. IFM-Derived Requirements Process.


1
Operational Baselines Employment Considerations
2
Conduct Strategy-to-Task Analysis
3
Derive Requirements
Met by existing infrastructure?
YES
Document
NO
Deficiency Documentation
4
Level I CPA & Solution ID (MAJCOM)
5
Level II CPA, Solution ID, Insertion into ISR Planning (AFC2ISRC)
6
Monitor & Track Deficiency Satisfaction
7
Revalidate Derived Requirements
8

1.7.1. Step 1: Define the Operational Baseline and Operational Imperatives.

1.7.1.1. The operational baseline includes the combined technology, targets, tactics, CONOPS, environment, capabilities construct, employment considerations/options, operational factors and threats to the system. This operational baseline serves as a starting point for IIA. The operational baseline will flow from these four sets of questions:

1.7.1.1.1. What operational steps must be taken in the use of this system through all phases of employment? From pre-wartime planning through employment and re-deployment?

1.7.1.1.2. What are the inputs, outputs, and interfaces for the system?

1.7.1.1.3. How will the system be designed? Does the technology drive specific support requirements? What information does the system developer need to optimize system design? What data (based upon the design) does the system need to meet the operational requirements?

1.7.1.1.4. How will the system be employed? In what environments, under what conditions? What capability or effect does the system contribute to?

1.7.1.2. As the program matures, the operational baseline will become more refined, resulting in better-defined derived intelligence requirements. Continued intelligence support analysis will be needed to react to changes or modifications to the operational baseline.

1.7.2. Step 2: Conduct Strategy-to-Task Analysis (STT). STT is a methodology that should be used by ISWGs as they derive intelligence requirements and identify intelligence deficiencies. The STT is a strong framework for depicting operational considerations, system relationships, and requirements. **Figure A3.1.** in **Attachment 3** depicts the STT methodology.

1.7.3. Step 3: Derive Intelligence Requirements. From initial derived intelligence requirement identification, more detailed requirements in terms of timeliness, accuracy, volume, etc. will need to be defined. By systematically looking at each operational consideration for the system inputs/outputs or employment and identifying corresponding derived intelligence requirements, the program can clearly show its linkages and dependencies to intelligence suppliers. A series of functional area checklists (contained in **Attachment 3**) help conduct a systematic assessment to derive intelligence requirements.

1.7.4. Step 4: Identify & Document Intelligence Deficiencies and Costs. Analysis of each derived intelligence requirement against the existing infrastructure and products will determine whether or not there are potential deficiencies to be acted upon.

1.7.4.1. No further analysis is required if the derived intelligence requirement can be fully satisfied by the existing intelligence with no changes to systems, training, manpower, facilities, processes, procedures, and/or policies; i.e., the required information, product, or resources exist in the current infrastructure. These requirements should be included in a depiction of the STT.

1.7.4.2. Further analysis is required if the derived intelligence requirement cannot be fully satisfied by the existing intelligence infrastructure. Shortfalls should be identified as intelligence deficiencies and further defined through intelligence deficiency analysis documentation. Intelligence planners should provide details on each of the intelligence deficiencies and document them within the WSISRD. They should also document any proposed solutions to deficiencies. The goal is to clearly describe the intelligence deficiency, its foundation in an operational requirement, and the plan for satisfying the intelligence deficiency. Estimated costs must be included as early as feasible. Program Offices and supporting Directors of Intelligence should consult with AFMC intelligence costing elements (OAS/OL-AB) to determine what costing data is required for each program/initiative and how it should be used. While documenting deficiencies, it is important to ensure each intelligence deficiency is a discrete deficiency.

1.7.4.3. The program office and the supporting directorate of intelligence share the responsibility for the management of derived intelligence requirements. Derived intelligence requirements are entered into WSISRD by the supporting intelligence organization. This action is accomplished on SIPRNET at <**http://afc2isrc.af.smil.mil**>. The process for submitting requirements at the website can be found under ISR Web Requirement Tools. A user-ID and password are required for login and an automated procedure to obtain them is provided at the website.

1.7.4.4. The Air Force requirements process is described in AFI 10-601, *Capabilities Based Requirements Development*. This AFI describes the actions that must be taken by the sponsors of any program/initiative to attain approval and validation of the requirements that must be fulfilled in order to achieve a specified capability. AFI 10-601 mandates that sponsors submit all capabilities-based requirements documents (ICDs, CDDs, and CPDs) to AF/XORD for review and validation by the Air Force Requirements for Operational Capabilities Council (AFROCC).

1.7.4.5. The AFC2ISRC and MAJCOM SIOs will maintain awareness of intelligence deficiencies and associated solutions. The Implementing MAJCOM will inform the PM of changes in status whenever significant progress or setbacks occur, or before each Key Decision Point/Milestone. The Operating MAJCOM will provide feedback to the Implementing MAJCOM regarding shortfalls in intelligence infrastructure support following program IOC.

1.7.4.6. Identifying Intelligence Deficiency Solution Costs. In many cases, satisfying intelligence deficiencies will require additional funding. Potential cost drivers include the equipment/systems, manpower, training, data formats, collection, production, and facilities supporting an operational capability.

1.7.4.6.1. AFMC/XRI cost specialists should be consulted to cost as many of the intelligence deficiencies/solutions as possible. Intelligence planners will need to provide the costing specialists with assumptions, background data, and access to cost data from similar deficiencies.

1.7.4.6.2. IIA should include documentation of total costs to resolve deficiencies that will be funded by the program/initiative, as well as costs that will be covered by other organizations and agencies [e.g. National Geospatial-Intelligence Agency (NGA), NASIC, Air Education and Training Command (AETC), National Security Agency (NSA), etc.]. All cost estimates should be given in a designated base year dollars. Key facts, assumptions, and costing guidelines should be referenced in all cost estimates.

1.7.4.6.3. By necessity, cost models will vary between programs/initiatives. However, a few guidelines should be applied when getting cost assessments:

1.7.4.6.3.1. Document actual costs where possible and provide costs to AFMC/XRI.

1.7.4.6.3.2. Estimation process and inputs duplicated independently.

1.7.4.6.3.3. Assumptions must be made clear.

1.7.5. Step 5: Conduct Level I CPA. Level I CPA is performed by the MAJCOMs. In this stage, Level I CPA should result in direct feedback to the program/initiative lead with regard to recommended design changes and proposed solutions that take advantage of requirements, including Production Requirements (PR), already articulated and being acted upon for other programs/initiatives. Requirements and potential solutions are identified and documented through AFC2ISRC via WSISRD. WSISRD can be accessed on SIPRNET at <**http://afc2isrc.af.smil.mil**>. The process for submitting requirements at the website can be found under ISR Web Requirement Tools. A user-ID and password are required for login and an automated procedure to obtain them is provided at the website.

1.7.6. Step 6: Conduct Level II CPA. Results of CPA at the MAJCOM level are forwarded to AFC2ISRC for inclusion in AF-level analysis. AFC2ISRC uses the results of Level II CPA to guide AF integration efforts, identify interoperability and capability issues to AF/XI, and provide inputs to the ISR Mission Area Plan (MAP), Intelligence POM and AF POM processes.

1.7.7. Step 7: Monitor and Track Deficiency Satisfaction. The status of derived deficiencies and corresponding impact to system development cost, schedule and performance must be monitored and understood. HQ USAF/XOI, the AFC2ISRC and the MAJCOMs accomplish this monitoring.

1.7.8. Step 8: Revalidate Deficiency Documentation. Revalidation of deficiencies is performed by the MAJCOMs within ISWGs. Each documented deficiency contains a significant amount of perishable information. The solutions, and action items associated with them must be revalidated annually. Any deficiency that has not been formally revalidated will expire one year after it is documented. Deficiencies that have been revalidated and found to be current, even with no additional change, should also be resubmitted with a new "as of" date to reflect the update. Deficiency data must be current to impact ISR MAP and POM processes.

1.8. Information Support Plan (ISP). The ISP is an acquisition document mandated for most service and joint programs and initiatives by Department of Defense and Joint Chiefs of Staff instructions. Among other things, the ISP is comprised of service and joint coordinated documentation from the results of IIA, including identification of shortfalls and details of solutions that are derived, with designation of responsible agencies. JCS/J-2 is responsible to certify the adequacy of the intelligence analysis and results. Guidance for compiling the ISP is provided in **Attachment 5** of this document.

1.8.1. ISP Coordination. Before the ISP enters formal AF-wide coordination, the intelligence portion should be reviewed and agreed to by members of the ISWG team. Authors should seek agreement from key intelligence, operations, requirements, and acquisition players on the derived intelligence requirements and actions needed to remedy intelligence deficiencies. The draft ISP will be reviewed by the Program Office intelligence partner who will assess sufficiency of the intelligence content and report their results to the Program Office and headquarters staffs for information and action. AF/XOIIA-F will direct Air Staff-level intelligence coordination of the ISP.

1.8.2. Intelligence Support Coordination for Space Acquisition Programs. The intelligence supportability content for the Integrated Program Summary (IPS) should be reviewed by the System Program Office (SPO) (or its designee) and AFSPC/IN six weeks before the start of the IPS drafting process. Once approved by AFSPC/IN and the SPO, the intelligence supportability content is forwarded to AF/XOIIA-F for final review/coordination. The intelligence supportability content should arrive at AF/XOIIA-F four weeks before the IPS drafting process begins to ensure sufficient time for review. Formal review and coordination of the complete ISP will occur after Key Decision Point (KDP)-C.

1.8.3. Classifying ISPs. ISPs should be releasable to contractors, as appropriate, under competition sensitivity rules and classified at the lowest classification consistent with user needs and security considerations. There may be a requirement for a separate annex at a higher classification, or one not releasable to contractors. Special Access Programs may require special-access ISPs, or ISPs with special-access annexes.

1.9. Intelligence Certification. Intelligence certification is performed by JCS/J-2 on ISPs, ICDs, CDDs, and CPDs as part of overall acquisition approval for specific programs or initiatives, as directed by CJCSI 3170.01 and described in CJCSI 3312.01. These certifications occur as part of normal document coordination and apply to threat, supportability, and interoperability. This AFI outlines IIA and threat support processes designed explicitly to address JCS/J-2 intelligence certification. A suggested format for documenting IIA results is included as an attachment to this AFI. CJCSI 3312.01 lists all the necessary steps to accomplish certification. Enclosure D of CJCSI 3312 provides a matrix checklist to assure all the required areas are addressed

1.10. Planning and Programming for Intelligence In Force Modernization. Air Force intelligence, planning, programming, requirements, operations, and acquisition communities must work together to ensure derived intelligence requirements and intelligence deficiencies are identified early in the acquisition life cycle of new systems to ensure support is available, sustainable, suitable, and affordable. Resource implications of proposed solutions must be clearly understood and incorporated within corporate planning and programming efforts.

1.10.1. AF/XOI Advocacy. AF/XOI advocacy for intelligence requirements occurs at key points in the planning and programming cycles. This corporate Air Staff advocacy will not take the place of the MAJCOMs' advocacy of requirements, but will supplement their efforts and ensure their visibility at the Air Staff level. To support IFM participation in their MAJCOM POM processes, AF/XOI provides annual IFM guidance to MAJCOM SIOs. This guidance highlights pertinent ISP-derived intelligence infrastructure requirements along with resource considerations raised in ISSGs. In addition, AF/XOI will ensure intelligence infrastructure requirements are addressed in the APPG and PMGM as applicable.

1.10.2. AFC2ISRC Advocacy. The AFC2ISRC conducts AF ISR modernization planning via the ISR MAP to optimize integration and interoperability across all ISR information domains. The resulting Mission Area Plan as well as ISR linkages within other Mission Area Plans and Capabilities Plans are used to guide AF planning and programming activities.

1.10.3. MAJCOM Advocacy. Given current planning and programming procedures, issues cannot be identified from the Air Staff level alone. All issues must first be identified in the MAJCOM POM/IPBS. It is essential, therefore, that IFM action officers in the MAJCOMs successfully insert derived requirements into their own planning and programming processes.

Chapter 2

THREAT SUPPORT

2.1. Threat Analysis. Threat analysis defines the environment in which a U.S. system will operate and identifies threats that could be encountered by that system at IOC and IOC +10 years. Threat support to force modernization includes threat assessments, data audits (simulation validation or SIMVAL), scenarios, and other threat production identified through the Department of Defense Intelligence Production Program (DODIPP) and the DOD Futures Intelligence Program. For the purpose of this instruction, a data audit is the process of verifying that threat information contained in computer models accurately reflects the current DOD intelligence position. Threat analysis accomplishes the following:

2.1.1. It ensures threat-based issues drive efficacy and feasibility decisions of a program or initiative.

2.1.2. It ensures cross-program analysis considerations are included when addressing threat issues.

2.2. Threat Assessments. Threat assessments describe the threat capabilities to be countered by a specific U.S. system and/or assess the potential of hostile parties to neutralize or degrade the effectiveness of that system. Threat assessment documents include Capstone Threat Assessments (CTA), System Threat Assessment Reports (STAR) and System Threat Assessments (STA), intelligence reports, and certain other threat assessments. AF/XOI oversees the production of threat assessment documents developed by the National Air and Space Intelligence Center (NASIC).

2.2.1. Capstone Threat Assessment (CTA).

2.2.1.1. A Capstone Threat Assessment is the DOD Intelligence Community's (IC) official assessment of the principal threat systems and capabilities within a category of warfare (e.g. Air, Space, Information Operations, Naval Warfare, etc.) that a potential adversary might reasonably bring to bear in an attempt to defeat or degrade U.S. weapon systems undergoing development. The Capstones are the product of a community process, not a unilateral development by a single producer, and constitute the authoritative DOD IC position. The Defense Intelligence Agency (DIA) and the Service intelligence production centers develop the CTAs in a collaborative effort. DIA manages the development of, and validates, CTAs.

2.2.1.2. The Capstones will replace the Air Force’s Threat Environment Descriptions (TED) and provide a broad overview of the threat environment and threat capabilities of potential adversaries within a particular category of warfare. They serve as a baseline from which system-specific threat assessments are developed.

2.2.1.3. The CTAs are used to support:

2.2.1.3.1. All planning, programming, budgeting, development, and test and evaluation activities throughout the acquisition process.

2.2.1.3.2. Pre-Milestone (MS) B or pre-Key Decision Point (KDP) B analyses.

2.2.1.3.3. System-specific threat assessments when referenced by a STAR or STA.

2.2.1.3.4. Programs that do not require a system-specific STAR/STA or that are not subject to the milestone review process.

2.2.1.3.5. Automated Information System (AIS) ACAT 1D programs.

2.2.2. System Threat Assessment Report (STAR).

2.2.2.1. The STAR is the authoritative, system-specific threat capabilities reference for Acquisition Category (ACAT) I programs and Space Major Defense Acquisition Programs (MDAP). AIS programs are required by DODI 5000.2 to use the Information Operations CTA. An AIS program can supplement the IO CTA with a system-specific STAR, if required.

2.2.2.2. The STAR is developed by NASIC and either (1) validated by DIA for ACAT ID and Space MDAP programs or (2) approved by NASIC/CC for ACAT IC programs.

2.2.2.3. The STAR includes a system-specific overview of threat system capabilities that could be employed against a proposed U.S. system and the projected threat environment in which the U.S. system will operate at IOC (or an established baseline) and IOC/baseline +10 years. As a minimum, the STAR should include threat capabilities of those countries addressed in the Multi-Service Force Deployment (MSFD) scenarios. (See **Attachment 2** for content and format information.)

2.2.2.3.1. The STAR is typically required by MS B or KDP B and is updated as necessary every 18 months throughout the development of the system.

2.2.3. System Threat Assessment (STA).

2.2.3.1. The STA is the authoritative, system-specific threat capabilities reference for ACAT II and Space Major System programs.

2.2.3.2. Similar to the STAR in format and content, the STA is developed by NASIC and approved by NASIC/CC.

2.2.3.3. The STA is typically required by MS B or KDP B and is updated as necessary every 18 months throughout the development of the system.

2.2.4. ACAT III and Space Non-Major System programs do not require a threat capabilities assessment. Instead, the threat section, and any references identified therein, of the Initial Capabilities Document (ICD), Capability Development Document (CDD), and Capability Production Document (CPD) will summarize the threat capabilities assessment. (For systems still using Operational Requirements Documents (ORDs), the ORD also contains a threat section.) Document authors use their supporting intelligence office to develop the threat capabilities assessment using DIA- and/or AF-approved information. In some non-warfighting systems the threat may be listed as not applicable.

2.2.5. Intelligence Reports. Intelligence Reports are concise, issue-oriented memorandums that:

2.2.5.1. Inform AF/XOI of contentious threat issues of Air Force or DOD acquisition programs or provide a status of programs of interest to AF/XOI.

2.2.5.2. Inform Air Staff and Air Force Secretariat offices of threat issues of Air Force or DOD acquisition programs and the AF/XOI position on those issues.

2.2.6. Other Threat Assessments. Air Force operating and implementing commands produce unique threat documents to satisfy specific customer requirements. The threat data in documents supporting acquisition programs must be consistent with the CTAs, STAR/STA, or other DIA- and/or AF-approved information. When requested or required, AF/XOIIA-F reviews and comments on these documents.

2.2.7. Threat Assessments in Program Documents. JCIDS documents (ICD, CDD, and CPD) and many acquisition documents (CONOPS, Functional Solutions Analysis study plan, Analysis of Alternatives study plan and report, Program Protection Plan, Information Support Plan, Single Acquisition Management Plan, Test & Evaluation Master Plan) contain threat-related information. Document authors should work through their supporting intelligence office to extract threat capabilities from the CTAs, STAR/STA, or other DIA- and/or AF-approved information. Consultation with the Threat Steering Group is recommended if the system-specific threat assessment (i.e. a STAR or STA) is not yet available. AF/XOIIA-F reviews and comments on these documents, as required, during the formal coordination process.

2.2.8. Classifying Threat Assessments. Threat assessments must be classified at the lowest level possible, consistent with user needs and security considerations. For some programs, such as Special Access Programs (SAPs), threat assessment documents might carry a higher classification. In such instances, this might require the preparation of a separate annex at a higher classification level than the basic document. This makes the basic document more accessible to stakeholders while affording the more sensitive information greater protection from improper disclosure.

2.3. Threat Steering Group (TSG).

2.3.1. After MS A or KDP A, a Program Office or MAJCOM may formally request a threat assessment. A TSG may be assembled to meet this request. NASIC, in coordination with AF/XOIIA-F, assembles a dedicated TSG to support each ACAT I, ACAT II, Space MDAP, and Space Major System program. The TSG draws on the expertise of intelligence and acquisition representatives who are stakeholders in the acquisition process and acts as the advisory body on all threat matters related to the specific program. The TSG determines the nature and level of documentation and other required activities to ensure consistent, efficient cradle-to-grave threat support. NASIC chairs the TSG, and AF/XOIIA-F provides oversight.

2.3.2. TSG membership should include representatives from:

2.3.2.1. Intelligence staffs of the Service and Unified Commands, as appropriate

2.3.2.2. Intelligence staffs of the implementing and operating commands

2.3.2.3. Staff of the Program Director

2.3.2.4. SAF/AQ or SAF/US, as appropriate

2.3.2.5. DIA

2.3.2.6. AFOTEC/TSI

2.3.2.7. Operations and Requirements staffs from the implementing and operating commands, as appropriate

2.3.2.8. Other organizations, as appropriate

2.3.3. TSG responsibilities include:

2.3.3.1. Scheduling STAR or STA production.

2.3.3.2. Establishing tasking.

2.3.3.3. Determining requirements for exceptional documents, such as STAR supplements.

2.3.3.4. Preparing a STAR or STA outline.

2.3.3.5. Advising on Critical Intelligence Categories (CIC) development.

2.3.3.6. Conducting a line-by-line review and revision of the draft STAR to provide a "camera-ready" copy to the NASIC Commander for approval. A Staff Summary Sheet (SSS) reflecting TSG members' coordination for their organizations will accompany the final copy. The SSS will reflect all pertinent issues, to include potentially contentious positions, and will recommend approval of the document.

2.3.3.7. Advising on target set selection.

2.3.3.8. Recommending sources of digital data for analysis.

2.3.3.9. Developing a countermeasures matrix, if required.

2.3.3.10. Coordinating support provided by TSG members to Concept Refinement Phase and Technology Development Phase activities (or Study Phase and Design Phase activities for space acquisition programs), testing, and other efforts to ensure the program is provided complete, current, and consistent threat information.

2.4. Threat Working Group (TWG). TWGs are working-level IPTs, with similar membership as that of TSGs, that are held as required to discuss threat issues and ensure consistent threat support to acquisition programs throughout their lifecycle.

2.5. Developing Documentation.

2.5.1. Capstone Threat Assessment (CTA).

2.5.1.1. DIA manages the development of the CTAs and validates the final product. A designated lead producer, along with multiple collaborators, from among DIA and the Service intelligence production centers, will develop and update each CTA.

2.5.1.2. DIA assembles and chairs the Acquisition Intelligence Support Working Group (AISWG), consisting of the appropriate Service representatives (AF/XOIIA-F and NASIC for CTAs involving Air Force lead or collaborative production), to determine the scope and provide guidance to the Capstone producers. The CTAs have independent update cycles, ranging from six months to two years.

2.5.2. Initial Capabilities Document (ICD).

2.5.2.1. The threat assessment of the ICD is prepared using DIA- and/or AF-approved threat information. ACAT ID, or potential ID, programs and Space MDAP programs must include DIA-validated threat references; all others may use AF-approved threat references. In accordance with CJCSM 3170.01, the Threat/Operational Environment section of the ICD includes:

2.5.2.1.1. A general description of the operational environment in which a capability must be exercised.

2.5.2.1.2. A summary of the current and projected threat capabilities (both lethal and non-lethal) to be countered throughout the capability's lifecycle.

2.5.2.1.3. A summary of the organizational resources that provided threat support to capability development efforts.

2.5.2.1.4. A reference of the most current DIA-validated threat documents (mandatory for ACAT ID, potential ID, and Space MDAP programs) and/or AF-approved products or data used. A short source document list of supporting classified publications is suggested for all ICDs and mandatory for any ICD that requires an unclassified threat section. All references should include the document title, classification of title, document number, publication date, and classification of the document. [Note: If a reference document is classified, the classification markings do not make the ICD classified, only a classified title will do so.]

2.5.2.2. As part of the staffing process for JCIDS documents with Joint Potential Designator (JPD) of JROC Interest and Joint Integration, the Joint Staff, J-2/DIA, will provide threat validation, as directed by CJCSI 3170.01. Therefore, the Threat/Operational Environment section of the ICD must meet the Threat Validation certification criteria outlined in CJCSI 3312.01.

2.5.2.3. AF/XOIIA-F will review all AF ICDs (and Joint ICDs which involve the AF) for AF/XOI during the JCIDS document staffing process to ensure threat information meets DOD and CJCS requirements.

2.5.3. Analysis of Alternatives (AoA).

2.5.3.1. When requested or required, AF/XOIIA-F will assist the MAJCOM/IN in obtaining USD(P) and DIA approval of threat scenarios and other threat data in the AoA to ensure that:

2.5.3.1.1. The threat environment in which the system will operate, to include projected adversary forces, strategy and tactics (including countermeasures), limitations on threat effectiveness, and sensitivities to variations in the threat, is accurately described.

2.5.3.1.2. AoA scenarios and threats are validated and reference materials meet DOD and Air Force requirements.

2.5.3.2. Baseline scenarios used in the AoA should be based on the Strategic Planning Guidance (SPG) Defense Planning Scenarios (DPS), unless otherwise directed by USD(P). The AoA may consider excursions from the SPG DPS when they would contribute to the analysis. To the greatest extent possible, the AoA will use MSFD scenario products from NASIC to support scenario needs. In cases where no appropriate MSFD scenarios exist, the AoA study team must work closely with AF/XOIIA-F, NASIC, USD(P), and the local intelligence staff to develop other scenarios or excursions to meet analytical needs.

2.5.3.3. When requested or required, NASIC and AF/XOIIA-F will formally review and evaluate the threat and scenarios portion of AF-led and AF-interest AoAs. As part of this review process, NASIC performs AoA data audits that verify the accuracy of the threat data and the manner in which it is used in models that support the AoA.

2.5.3.4. When requested or required, NASIC and AF/XOIIA-F will formally review and evaluate all AF-led AoAs under consideration for approval by the AFROCC or Joint Requirements Oversight Council (JROC).

2.5.4. Capability Development Document (CDD) and Capability Production Document (CPD).

2.5.4.1. The threat assessment of the CDD and CPD is prepared using the current STAR/STA, if it exists, and DIA- and/or AF-approved threat information. ACAT ID, or potential ID, programs and Space MDAP programs must include DIA-validated threat references; all others may use

AF-approved threat references. In accordance with CJCSM 3170.01, the Threat Summary section of the CDD and CPD includes:

2.5.4.1.1. A description of the projected threat environment in which a capability must be exercised, including the nature of the threat and threat tactics.

2.5.4.1.2. A summary of the current and projected threat capabilities (both lethal and non-lethal) to be countered throughout the capability's lifecycle.

2.5.4.1.3. A summary of the organizational resources that provided threat support to capability development efforts.

2.5.4.1.4. A reference of the most current DIA-validated threat documents (mandatory for ACAT ID, potential ID, and Space MDAP programs) and/or AF-approved products or data used. A short source document list of supporting classified publications is suggested for all CDDs and CPDs and mandatory for any CDD or CPD that requires an unclassified threat section. All references should include the document title, classification of title, document number, publication date, and classification of the document. [Note: If a reference document is classified, the classification markings do not make the CDD or CPD classified, only a classified title will do so.]

2.5.4.2. As part of the staffing process for JCIDS documents with Joint Potential Designator (JPD) of JROC Interest and Joint Integration, the Joint Staff, J-2/DIA, will grant threat validation, as directed by CJCSI 3170.01. Therefore, the Threat Summary section of the CDD and CPD must meet the Threat Validation certification criteria outlined in CJCSI 3312.01.

2.5.4.3. AF/XOIIA-F will review all AF CDDs and CPDs (and Joint CDDs and CPDs which involve the AF) for AF/XOI during the JCIDS document staffing process to ensure threat information meets DOD and CJCS requirements.

2.5.5. Test & Evaluation Master Plan (TEMP).

2.5.5.1. The threat capabilities information in the TEMP is prepared using the current STAR/STA, if it exists, and other DIA- and/or AF-approved threat information. The threat information of the TEMP will:

2.5.5.1.1. Briefly summarize the threat environment described in the STAR/STA. [Exception: If the STAR/STA does not yet exist or is not required, the TEMP drafter will use current DIA- and/or AF-approved products, such as CTAs, and address threat environments at IOC and IOC+10.]

2.5.5.1.2. Identify the type, number, availability, and fidelity requirements for all representations of the threat at IOC and IOC+10.

2.5.5.1.3. Compare the requirements for threat representations with available and projected assets and their capabilities and highlight major shortfalls in the ability to adequately characterize or to accurately represent specific threats listed in the STAR/STA (or other DIA- and/or AF-approved products) within the test environment.

2.5.5.1.4. Reference the STAR/STA, if it exists, and other DIA- and/or AF-approved products or data used.

2.5.5.2. When requested or required, NASIC and AF/XOIIA-F reviews and approves the threat-related sections of the TEMP.

2.5.6. System Threat Assessment Report (STAR) and System Threat Assessment (STA).

2.5.6.1. AF/XOIIA-F, in conjunction with SAF/AQ or SAF/US, the implementing command, the operating command, and DIA, determines within 30 days of the initial Program Management Directive (PMD) date whether a TSG is required to support the program.

2.5.6.2. If a TSG is warranted, NASIC, in conjunction with AF/XOIIA-F, will notify appropriate organizations and convene an initial TSG meeting as soon as possible to review/coordinate post-MS A threat support and ensure timely STAR or STA production to support the MS/KDP-B decision. The implementing command's intelligence office shall formally task production of the STAR/STA by submitting a production requirement in accordance with AFI 14-201.

2.5.6.3. Based on the STAR/STA table of contents, schedule, and other TSG guidance, NASIC drafts the document and distributes it to TSG members for review.

2.5.6.4. Thirty days (45 days if sister-Service review is required) after draft distribution, or as specified by the TSG, TSG members shall provide the TSG Chairman and other TSG members with their substantive comments.

2.5.6.5. Seven calendar days after comment exchange, the TSG will reconvene to conduct a line-by-line substantive and editorial review/revision of the draft. During this seven-day period, each member will review other TSG members' comments/positions and conduct research and/or discussions in preparation for the reconvened TSG. NASIC will consolidate all comments.

2.5.6.6. The TSG will conduct an intensive review to ensure the accuracy and quality of the final product. At the completion of the TSG meeting, each member will coordinate for his or her organization on a staff summary sheet (SSS) recommending AF approval/disapproval. The SSS, signed by the TSG Chairman, will highlight any significant issues that the TSG was unable to resolve and any assessments that are suspected to be highly contentious or of particular concern to the acquisition customer. The reconvened TSG membership will, whenever possible, be the same as for the original TSG. For Joint programs, sister Services will be invited to participate in the TSG.

2.5.6.7. NASIC will staff the TSG recommendation, obtain Air Force approval from the NASIC Commander, and publish/distribute final STARs/STAs in accordance with the production schedule set at the original TSG meeting.

2.5.6.8. The forward of the final Air Force-approved product will contain the following statement: "This document has been reviewed by NASIC/CC as the delegated agent for AF/XOI and is approved for use in support of the (program name) program as of (publication date) and is effective through (18 months after publication date), unless earlier superseded."

2.5.6.9. NASIC submits Air Force-approved STARs for ACAT ID programs (and ACAT IC programs at MS B only) to DIA for validation. The TSG Chairman will review DIA comments prior to incorporation in the STAR for comparison with TSG results. DIA comments directing significant changes to the Air Force-approved STAR may warrant formal Air Force appeal. In these cases, the TSG Chairman will consult with and represent the TSG membership in presenting and defending the Air Force position and working with DIA to resolve the issue.

2.5.6.10. After a STAR has been approved and validated, the implementing command will closely monitor the status of CICs and notify TSG members and the program office of major developments. The TSG will direct interim changes or revisions when significant changes occur in either the threat or the U.S. system specifications and characteristics.

2.5.6.11. The review timelines set forth in this section are subject to modification by the TSG. Once the production schedule has been developed at the initial TSG, any changes of more than two days will be documented by message from the TSG Chairman to the full TSG membership.

2.5.6.12. STAs and STAR supplements follow the same review procedures as STARs.

2.5.6.13. On TSG recommendation, the NASIC Commander grants Air Force approval of STARs (for ACAT I and Space MDAP programs) and STAs (for ACAT II and Space Major System programs). In addition, Air Force-approved STARs for ACAT ID programs (and ACAT IC programs at MS B only) must be submitted to DIA for validation.

2.6. Updating Threat Documentation.

2.6.1. The implementing command will ensure threat data is updated appropriately in program documents for subsequent milestone reviews and decision points. The intelligence provided must be consistent with the most current DIA- and/or AF-approved assessments.

2.6.2. When requested or required, NASIC and AF/XOIIA-F will review all documents/studies for AF/XOI prior to milestone reviews, ensuring the threat information meets DOD and AF standards.

2.6.3. Updating a STAR.

2.6.3.1. Approximately 6 weeks before the one-year anniversary of a STAR, NASIC requests TSG members review and provide recommendations as to the need for an update of the STAR.

2.6.3.2. NASIC consolidates recommendations on or before the anniversary date and determines, with AF/XOIIA-F coordination, whether a STAR requires an update.

2.6.3.3. If a STAR does not require updating, the TSG Chairman will obtain the concurrence of the TSG members on the SSS recommending the NASIC Commander reaffirm the currency of the information and assessments in the STAR. NASIC will publish a new STAR cover, title page, and preface that documents this decision, and will make distribution to STAR recipients.

2.6.3.4. If a STAR requires updating, NASIC will convene the TSG and follow the processes outlined in section **2.5.6.** of this instruction.

2.6.4. All threat capabilities assessments must be maintained in a current and approved or validated status throughout the acquisition process.

Chapter 3

RESPONSIBILITIES

3.1. Headquarters, United States Air Force Director of Intelligence, Surveillance, and Reconnaissance (HQ USAF/XOI).

3.1.1. Provides policy guidance to MAJCOMs and AFC2ISRC on intelligence issues associated with force modernization-associated programs, activities, or initiatives. Provides intelligence support to AF ISP policy- and decision-makers.

3.1.2. Staffs and reviews all AF ISPs to ensure sufficiency of intelligence content. Disseminates HQ USAF/XOI review comments to Director, Information Dominance Programs, Assistant Secretary (Acquisition) (SAF/AQI); Director of C4ISR Integration, Warfighting Integration Directorate (HQ USAF/XII); AFC2ISRC Intelligence Directorate (AFC2ISRC/IN); Implementing Command SIOs; and Operating Command SIOs. Resolves disagreements between AF reviewers on ISP intelligence content issues.

3.1.3. Chairs Intelligence Support Steering Groups (ISSGs).

3.1.4. Oversees completion of the intelligence content of AF ISPs and JCIDS documents.

3.1.5. Advocates for resolution of derived deficiencies with the National Intelligence Community and for funding/resourcing in the corporate Air Staff planning and programming processes. Publishes applicable IFM guidance to MAJCOMs during programming cycles.

3.1.6. Ensures all capabilities documents that support acquisition programs are reviewed for accurate assessment of threat and documentation of intelligence supportability and infrastructure requirements.

3.1.7. Provides requirements and acquisition customers with guidance on architectures, stock intelligence products (including information on databases, tools, foreign materiel exploitation issues, etc.), and other intelligence matters, as applicable.

3.1.8. Educates the AF intelligence force about significance of IFM to future warfighting success. Integrates acquisition intelligence into training courses, career development planning, and other education and training forums, as appropriate.

3.1.9. Ensures intelligence production processes are responsive to acquisition customers, in accordance with AFI 14-201, Intelligence Production and Applications.

3.1.10. Monitors status of AF IFM initiatives and briefs status to DOD and HQ AF senior leadership.

3.1.11. Oversees intelligence threat support to Air Force acquisition programs and AF-led joint acquisition programs throughout their lifecycles.

3.1.12. Oversees Threat Steering Groups (TSGs) and participates in Acquisition Intelligence Support Working Groups (AISWGs) and Threat Working Groups (TWGs).

3.1.13. Reviews capabilities and acquisition documents to ensure accuracy and timeliness of all intelligence threat input, in accordance with DODIPP and other national-level guidelines.

3.1.14. Manages Intelligence Certification process in accordance with CJCSI 3170.01 requirements. Reviews, validates and forwards requests for Intelligence Certification to DIA for approval.

3.2. National Air and Space Intelligence Center (NASIC).

3.2.1. Chairs TSGs, as required.

3.2.2. Participates in ISSGs, ISWGs, AISWGs, TWGs, and TEMs, as required.

3.2.3. Leads, or collaborates in, production of CTAs, as appropriate. Produces STARs, STAs, scenarios, and other threat assessments. Ensures stock intelligence products are available to force modernization customers.

3.2.4. Conducts data audits to verify the accuracy of threat data used in AoA models and the manner in which that data is used.

3.3. Implementing Command SIO (AFMC & AFSPC).

3.3.1. Manages the conduct of IFM as follows:

3.3.1.1. Assists in the development of and reviews strategic plans and other acquisition-related documents to ensure specific intelligence requirements and constraints are documented.

3.3.1.2. Assesses ISP intelligence content for completeness (requirements for intelligence support and requirements by intelligence), supportability (availability, suitability, and sufficiency), and impact (on intelligence strategy, policy, and architecture planning).

3.3.1.3. Identifies intelligence-sensitive programs/initiatives.

3.3.1.4. Monitors, measures, evaluates and reports on the effectiveness of intelligence integration in research and development, acquisition, test and evaluation, and sustainment activities. Characterizes assessments in terms of cost, schedule and performance.

3.3.1.5. Identifies prioritizes and nominates programs/initiatives to AF/XOI for ISSG consideration.

3.3.1.6. Oversees the conduct of Intelligence Infrastructure Analysis (IIA).

3.3.1.7. In conjunction with AF/XOI, Operating Command, AFC2ISRC and national intelligence agencies, documents, coordinates and resolves intelligence deficiencies for programs/initiatives.

3.3.1.8. Assists Analysis of Alternatives (AoA), Advanced Concept Technology Development and Advanced Technology leads, as required, with appropriate intelligence cost data.

3.3.1.9. Teams with MAJCOM to identify intelligence costs associated with the program/initiative. Obtains expertise and cost data from intelligence agencies, as necessary. Works with acquisition counterparts (PM, Technology Lead, etc.) to ensure intelligence infrastructure costs are included in life cycle cost estimates and program budgets. Highlights funding issues to appropriate MAJCOM, AFC2ISRC, and AF/XOIIA-F.

3.3.1.10. Participates in force modernization forums (such as AF capabilities planning forums, the ISR MAP, IPTs, etc.).

3.3.1.11. As required, assists AFC2ISRC in ISR planning activities to ensure intelligence infrastructure is adequately addressed in the ISR Mission Area Plan (ISR MAP), AF capabilities planning processes, and solution analysis processes.

3.3.1.12. Performs Level I Cross-Program Analysis (CPA) of intelligence deficiencies within command purview to ensure consolidation of similar requirements and facilitate development of multi-program solutions. Provides results Level I CPA to AFC2ISRC for inclusion in Level II CPA.

3.3.1.13. Annually revalidates documented derived requirements.

3.3.1.14. Ensures Implementing Command Intelligence personnel receive appropriate education and training to conduct acquisition intelligence competencies. These competencies include (but are not limited to) Intelligence Infrastructure Analysis, intelligence requirements and deficiencies documentation, and Cross-Program Analysis.

3.3.2. Provides intelligence threat support to programs/initiatives as follows:

3.3.2.1. Participates in TSGs for STAR/STA development and review, as appropriate.

3.3.2.2. Oversees documentation and submission of intelligence PRs, and Statements of Intelligence Interest (SII), IAW AFI 14-201, to ensure production of threat documents/data.

3.3.2.3. Updates threat-related text, as appropriate, in post-Milestone B iterations of acquisition-associated documents.

3.3.3. Conducts MAJCOM level intelligence certification of programs and activities in accordance with DOD, JCS and Air Force evaluation criteria. Forwards results of evaluations to AF/XOI upon request.

3.4. Operating Command SIO (ACC, AFSOC, AMC, AFSPC).

3.4.1. Participates in IFM activities as follows:

3.4.1.1. Assists in the development of strategic plans and other acquisition-related documents, studies and analyses ensuring specific intelligence requirements and constraints are documented. Assesses intelligence content of ISPs and JCIDS documents for sufficiency.

3.4.1.2. Identifies prioritizes and nominates force modernization initiatives to AF/XOI for ISSG consideration.

3.4.1.3. In conjunction with AF/XOI, Implementing Command, and AFC2ISRC, assists in the documentation, coordination, and resolution of intelligence deficiencies for programs/initiatives.

3.4.1.4. For pre-program initiatives (AoAs, studies, etc.) partners with the study leads and MAJCOM program leads to perform intelligence infrastructure analysis and document intelligence deficiencies and proposed solutions. Uses the WSISRD to perform this documentation.

3.4.1.5. Performs Level I Cross-Program Analysis (CPA) of intelligence deficiencies within command purview to ensure consolidation of similar requirements and facilitate development of multi-program solutions. Provides results Level I CPA to AFC2ISRC for inclusion in Level II CPA.

3.4.1.6. Advocates for resolution of intelligence deficiencies identified during the intelligence infrastructure analysis process. Works with MAJCOM staff to address resource issues associated with intelligence requirements that should be incorporated within program baselines.

3.4.1.7. Advocates for inclusion of costs associated with intelligence infrastructure analysis-derived requirements/deficiencies in MAJCOM planning, programming and budgeting processes. Highlights funding issues to Implementing Commands, AFC2ISRC and AF/XOIIA-F.

3.4.1.8. Performs annual revalidation of Operating Command derived requirements.

3.4.1.9. Participates in force modernization forums, to include, but not limited to, ISSGs, ISWGs, TEMs, TSGs, TWGs, ISR MAP preparation conferences, the ISR RAWG and the ISR MAT.

3.4.2. Ensures timely and appropriate intelligence threat support and assessments as needed to support MAJCOM acquisition programs and initiatives to include (but not limited to):

3.4.2.1. Using validated or approved intelligence, prepares intelligence-related text in ICDs, CDDs, CPDs, CONOPS, AoAs, Strategic Plans and other acquisition-associated documents, studies and analyses.

3.4.2.2. Participates in TSGs for STAR/STA development and review, as appropriate.

3.4.2.3. Assists Analysis of Alternatives (AoA), Advanced Concept Technology Development and Advanced Technology leads, as required, with appropriate intelligence.

3.4.2.4. Prepares and submits intelligence PRs and SIIs, IAW AFI 14-201, to ensure production of threat documents.

3.4.2.5. Allocates and advocates for/coordinates with the Intelligence Community and other DOD organizations the resources necessary to support IFM.

3.4.3. Oversees development and approves submission of Operating Command requests for Intelligence Certification, as required by CJCSI 3170.01. Forwards requests to AF/XOI for AF-level validation and subsequent submission to DIA for approval.

3.5. Air Force Command and Control & Intelligence, Surveillance, and Reconnaissance Center (AFC2ISRC) SIO.

3.5.1. Provides direct support to the force modernization process working as a lead agency to identify and resolve intelligence infrastructure deficiencies.

3.5.1.1. Assists in the development of CONOPS, PMDs, ICDs, CDDs, CPDs, and other acquisition-related documents to ensure specific Intelligence infrastructure deficiencies are documented.

3.5.1.2. Prioritizes and nominates force modernization program and pre-program initiatives to AF/XOI for ISSG consideration.

3.5.1.3. Participates in force modernization forums, to include, but not limited to, ISSGs, ISWGs, TEMs, TSGs, TWGs, ISR RAWG, and the ISR MAT, as required.

3.5.1.4. Partners with study/initiative leads to analyze intelligence infrastructure, document deficiencies, and develop solution proposals.

3.5.1.5. Reviews intelligence-sensitive ISP content for sufficiency.

3.5.1.6. Administers Weapon System Intelligence Support Requirements Database (WSISRD).

3.5.1.7. Performs Level II Cross-program Analysis (CPA) of Intelligence.

3.5.1.8. Provides feedback on the results of Level II CPA to AF/XOI, Operating and Implementing Commands.

3.5.2. Leads AF efforts to resolve intelligence deficiencies working with AF/XOI, AF/XI, AFC2ISRC Staff, National Intelligence Community, operating and implementing commands.

3.5.2.1. Provides validated intelligence deficiencies to ISR Requirements Analysis Working Group (RAWG) for inclusion in the ISR Mission Area Plan (MAP).

3.5.2.2. Tracks submissions to the ISR MAP and provide advocacy for deficiency solutions.

3.5.2.3. Provides feedback to MAJCOMs and AF/XOI on results of AF-level cross-program analysis and efforts to identify synergistic solutions. Informs AF/XOIIA-F of solutions and/or deficiencies requiring AF/XOI advocacy and action.

3.5.2.4. Advocates funding for solutions in AFC2ISRC planning and programming processes.

3.5.2.5. Provides input to AF/XOI and AF/XI on issues requiring action or advocacy within HQ USAF and National Intelligence Community planning and programming processes.

3.5.2.6. Advocates for inclusion of costs associated with common derived ISR requirements/ deficiencies into AFC2ISRC planning and programming processes.

3.5.3. Provides access to AFC2ISRC-developed architecture products.

3.6. Product Center/Logistics Center/Test Center/Lab Research Site SIO.

3.6.1. Conducts IFM activities as follows:

3.6.1.1. Identifies intelligence-sensitive programs/initiatives and documents them in the Program/ Initiative Status Matrix.

3.6.1.2. Provides tailored intelligence support to lab activities, High Performance Teams (HPTs), development planners, and other pre-Milestone/KDP-A activities. Integrates intelligence infrastructure issues into solutions analysis/development processes.

3.6.1.3. Nominates force modernization initiatives to command SIO for ISSG consideration.

3.6.1.4. Partners with acquisition counterparts (i.e., program managers, SPDs, SSMs, Technology Leads, Chief Engineers, etc.) to ensure appropriate integration of intelligence within systems research and development, acquisition, test and evaluation, and sustainment activities.

3.6.1.5. Participates in and/or co-chairs force modernization forums, to include, but not limited to, ISSGs, ISWGs, TEMs, TSGs, and TWGs as required.

3.6.1.6. Assists in the development, coordination and resolution of potential intelligence infrastructure deficiencies for developing weapon systems. Documents, submits, and annually revalidates these items for action. Uses WSISRD to perform this documentation.

3.6.1.7. Assesses intelligence content of ISPs and JCIDS documents for completeness (requirements for intelligence support and requirements by intelligence), supportability (availability, suitability, and sufficiency), and impact (on intelligence strategy, policy, and architecture planning). Provides results of review to the ISP developer, Command SIO, and AF/XOIIA-F.

3.6.2. Provides threat support to force modernization initiatives as follows:

3.6.2.1. Provides tailored intelligence support and documentation of intelligence requirements to support the research, development, test, acquisition and sustainment of AF force modernization efforts.

3.6.2.2. Works with the program office to prepare PRs, SIIs, and Foreign Materiel Acquisition requests and submits them to the appropriate authority for validation, in accordance with AFI

14-201, Intelligence Production and Applications. Manages Center PR process to ensure PRs are closed and/or revalidated as necessary.

3.6.2.3. Maintains intelligence reference materials and facilitates access to intelligence community databases, such as the Defense Intelligence Information Services Program (DIISP).

3.6.2.4. Works with AFOTEC and SPOs to ensure intelligence information in Test and Evaluation Master Plans (TEMPs) references validated scenarios and remains current during post-Milestone/KDP-B activities.

3.6.3. Assists in development of and develops requests for Intelligence Certification to meet CJCSI 3170.01 requirements. Submits requests for Intelligence Certification to MAJCOM SIO.

3.7. Air Force Operational Test and Evaluation Center (AFOTEC/TSI).

3.7.1. TSI is responsible for ensuring the OT&E program threat lists and the OT&E threat environments are adequately addressed, ensuring appropriate intelligence is used to support test planning and the development of the threat portions of AFOTEC documents.

3.7.2. Participates in ISWGs and TSGs.

3.7.3. Through coordination with the Operating Command, identifies and documents total intelligence support requirements for Operational Test and Evaluation (OT&E), and provides data to the ISP originator for inclusion in the ISP. Ensures validated threat and intelligence infrastructure assessments are included in TEMPs and Operational Test Plans (OTPs).

3.7.4. Works with MAJCOM/IN and Intelligence Community organizations to ensure appropriate OT&E threat lists/scenario development to support IOT&E.

3.8. AFMC Intelligence Detachment (Office of Aerospace Studies/Operating Location-AB [OAS/OL-AB]).

3.8.1. Ensures intelligence infrastructure and threat considerations are properly addressed in AoAs.

3.8.2. Integrates costs for generating the intelligence analysis and documenting intelligence needs, shortfalls, solutions, and solution cost estimates, as well as funding for the solutions themselves (to the extent the shortfalls are caused or driven by the program), into the AoA's Cost/Performance IPT analysis.

3.8.3. Nominates force modernization initiatives to SIO for ISSG consideration.

3.8.4. Participates in ISSGs and TWGs, as required.

3.9. Program Manager, Single Manager, Product Director, Technology Director, Concept Development Team Leader or Initiative Lead.

3.9.1. In conjunction with local SIO, determines whether systems are intelligence-sensitive and require intelligence infrastructure or threat analysis. If analysis is necessary, requests support from local intelligence staff. For purposes of accomplishing the Intelligence content of the ISP, the Program Manager or project lead should work with the local SIO to identify the intelligence support planner who will interact with the SIO intelligence staff. The designated intelligence support planner could be someone already working within the System Program Office. Ideally, this individual would be an intelligence professional.

3.9.2. Participates in and/or co-chairs force modernization forums, to include, but not limited to, ISSGs, ISWGs, TEMs, TSGs, and TWGs as required.

3.9.3. Includes intelligence costs within life-cycle program costs to include intelligence infrastructure analysis, creation of intelligence content of the ISP, and support for operations and sustainment.

3.9.4. Conduct and document ISR supportability and sustainability analysis as directed in DOD and USAF ISP policy and guidance. If the PM and supporting intelligence office question whether or not the Intelligence content of an ISP is required, they should request a determination be made by their MAJCOM SIO.

3.10. Air Education and Training Command (AETC).

3.10.1. Designs, develops, and teaches IFM training courses at the direction of the Air Force Career Field Manager (AFCFM). All resourcing must be attained and in place prior to conduction of the development and subsequent teaching.

3.10.2. Incorporates IFM concepts and materials into acquisition and intelligence training programs at the direction of the appropriate AFCFM.

RONALD E. KEYS, , Lt General, USAF
DCS/Air and Space Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DOD Directive 5000.1, *The Defense Acquisition System*

DOD Instruction 5000.2, *Operation of the Defense Acquisition System*

DOD Instruction 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*

DIA Regulation (DIAR) 55-3, *Intelligence Support for Defense Acquisition Programs*

CJCSI 3170.01, *Joint Capabilities Integration and Development System*

CJCSM 3170.01, *Operation of the Joint Capabilities Integration and Development System*

CJCSI 3312.01, *Joint Military Intelligence Requirements Certification* (Draft)

CJCSI 6212.01, *Interoperability and Supportability of Information Technology and National Security Systems*

AFI 10-601, *Capabilities Based Requirements Development*

AFI 14-105, *Unit Intelligence Mission and Responsibilities*

AFI 14-201, *Intelligence Production and Applications*

AFI 14-205, *Geospatial Information and Services (GI&S)*

AFI 14-206, *Modeling and Simulation*

AFI 16-1002, *Modeling and Simulation (M&S) Support to Acquisition*

AFI 63-107, *Integrated Product Support Planning and Assessment*

AFPD 10-6, *Mission Needs and Operational Requirements*

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

AFPD 62-2, *System Survivability*

AFPD 63-1, *Capability-Based Acquisition System*

AFPD 90-11, *Planning System*

AFPD 99-1, *Test and Evaluation Process*

National Security Space (NSS) Acquisition Policy 03-01

Abbreviations and Acronyms

ACAT—Acquisition Category

ACC—Air Combat Command

ACTD—Advanced Concept Technology Demonstration

AETC—Air Education and Training Command

AFC2ISRC—Air Force Command & Control and Intelligence, Surveillance, & Reconnaissance Center

AFCA—Air Force Communications Agency

AFCAA—Air Force Cost Analysis Agency

AFI—Air Force Instruction

AFMC—Air Force Materiel Command

AFOTEC—Air Force Operational Test and Evaluation Center

AFPD—Air Force Policy Directive

AFRL—Air Force Research Laboratory

AFROCC—Air Force Requirements for Operational Capabilities Council

AIA—Air Intelligence Agency

AIS—Automated Information System

AISWG—Acquisition Intelligence Support Working Group

AoA—Analysis of Alternatives

APPG—Annual Planning and Programming Guidance

AQ—Acquisition

AQI—Director, Information Dominance Programs, Assistant Secretary (Acquisition)

C4I—Command, Control, Communications, Computers, and Intelligence

C4ISP—Command, Control, Communications, Computers and Intelligence Support Plan *(has been renamed Information Support Plan, ISP)*

CIC—Critical Intelligence Category

CC—Commander

CDD—Capability Development Document

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CJCSM—Chairman of the Joint Chiefs of Staff Manual

CONOPS—Concept of Operations

CPA—Cross-Program Analysis

CPD—Capability Production Document

CTA—Capstone Threat Assessment

DI—Director of Intelligence

DIA—Defense Intelligence Agency

DIISP—Defense Intelligence Information Services Program

DOD—Department of Defense

DODI—Department of Defense Instruction

DODIPP—Department of Defense Intelligence Production Program

DODM—Department of Defense Manual

DPS—Defense Planning Scenario

FM—Financial Management

GI&S—Geospatial Information and Services *(Formerly Mapping Charting & Geodesy)*

GMI—General Military Intelligence

HPT—High Performance Team

HUMINT—Human Intelligence

IC—Intelligence Community

ICD—Initial Capabilities Document

IDHS—Intelligence Data Handling Systems

IIA—Intelligence Infrastructure Analysis

IFM—Intelligence in Force Modernization

IMINT—Imagery Intelligence

IN—Intelligence

IOC—Initial Operational Capability

IOT&E—Initial Operational Test and Evaluation

IPBS—Intelligence Program Budget Submission

IPS—Integrated Program Summary

IPT—Integrated Product Team

ISP—Information Support Plan

ISR—Intelligence, Surveillance, and Reconnaissance

ISSG—Intelligence Support Steering Group

ISWG—Intelligence Support Working Group

IT—Information Technology

JCIDS—Joint Capabilities Integration and Development System

JPD—Joint Potential Designator

JROC—Joint Requirements Oversight Council

KDP—Key Decision Point

MAJCOM—Major Command

MAP—Mission Area Plan

MASINT—Measurement and Signature Intelligence

MAT—Mission Area Team

MDAP—Major Defense Acquisition Program

MS—Milestone

MSFD—Multi-Service Force Deployment

NASIC—National Air and Space Intelligence Center

NGA—National Geospatial-Intelligence Agency

NRO—National Reconnaissance Office

NSA—National Security Agency

NSS—National Security Systems, or National Security Space

OAS—Office of Aerospace Studies

OAS/OL-AB—Office of Aerospace Studies/Operating Location-AB (AFMC/XRI Intelligence Detachment)

OPR—Office of Primary Responsibility

ORD—Operational Requirements Document

OT&E—Operational Test and Evaluation

OTP—Operational Test Plan

P3I—Pre-Planned Product Improvement

PM—Program Manager

PMD—Program Management Directive

PMGM—Program Manager's Guidance Memorandum

POC—Point of Contact

POM—Program Objective Memorandum

PPP—Program Protection Plan

PR—Production Requirement

RAWG—Requirements Analysis Working Group

RDT&E—Research, Development, Test and Evaluation

S&TI—Scientific and Technical Intelligence

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

SAF/US—Under Secretary of the Air Force

SAP—Special Access Program

SIGINT—Signals Intelligence

SII—Statement of Intelligence Interest

SIO—Senior Intelligence Officer

SISSU—Secure, Interoperable, Supportable, Sustainable, and Usable

SPD—System Product Director

SPG—Strategic Planning Guidance

SPO—System Program Office

SSS—Staff Summary Sheet

STA—System Threat Assessment

STAR—System Threat Assessment Report

STT—Strategy-To-Task

TED—Threat Environment Description

TEM—Technical Exchange Meeting

TEMP—Test and Evaluation Master Plan

TSG—Threat Steering Group

TWG—Threat Working Group

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

USD(P)—Under Secretary of Defense for Policy

WSISRD—Weapon System Intelligence Support Requirements Database

XI—Deputy Chief of Staff, Warfighting Integration

XOI—Director of Intelligence, Surveillance and Reconnaissance

XOIIA-F—Force Modernization Branch, Intelligence Applications & Production Division (HQ USAF)

XORD—Requirements Management Division, Director of Operational Capability Requirements (HQ USAF)

Terms

Acquisition Intelligence Support Working Group (AISWG)—A DIA-led, multi-Service forum for discussing acquisition intelligence issues, such as Capstone Threat Assessments, System Threat Assessments, scenarios, and acquisition intelligence policy.

Acquisition Program—A directed, funded effort designed to provide a new, improved, or continuing materiel, weapon, or information system or service capability in response to a validated operational or business need.

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 material alternative to satisfy a mission need.

Capability Development Document (CDD)—A document that captures the information necessary to develop a proposed program(s), 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/KDP 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/KDP C.

Capstone Threat Assessment (CTA)—The DOD Intelligence Community's (IC) official assessment of the principal threat systems and capabilities within a category of warfare (e.g. Air, Space, Information Operations, Naval Warfare, etc.) that a potential adversary might reasonably bring to bear in an attempt to defeat or degrade U.S. weapon systems undergoing development.

Concept Refinement Phase—The first phase of the DODI 5000.2 acquisition management framework during which the initial concept is refined, the Analysis of Alternatives is conducted, and the Technology Development Strategy is developed.

Critical Intelligence Categories (CIC)—Categories of threat information dealing with platforms, weapons, systems, doctrine, or operational employment that, if developed, procured, or implemented by potential adversaries could significantly influence the effective operation of the deployed system. (Refer to DIAR 55-3)

Cross-Program Analysis (CPA)—CPA is an analytical effort designed to “look across” all Intelligence-sensitive programs and the related Intelligence deficiencies. 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 / systems. 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. Two levels of CPA include Level I CPA performed at the MAJCOM level and Level II CPA performed by the AFC2ISRC.

Derived Intelligence Requirement—Intelligence requirements that impact system development and operational employment. These requirements are derived from Intelligence Infrastructure Analysis, Threat analysis and Capabilities analysis.

Evolutionary Acquisition—An acquisition strategy whereby a basic capability is fielded with the intent to develop and field additional capabilities as requirements are refined. The key concept is to rapidly develop and field useful increments of capability (goal of 18 months or less for each delivery of an incremental capability), and to leverage user feedback in refining required capabilities for additional increments.

Implementing Command—The command or agency designated by the Air Force 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 Directorate of Intelligence.

Information Support Plan (ISP)—The ISP (previously known as C4ISP) is an acquisition document mandated for most service and joint programs and initiatives by Department of Defense and Joint Chiefs of Staff instructions. Among other things, the ISP is comprised of the service and joint coordinated documentation of the results of Intelligence Infrastructure Analysis, including identification of shortfalls and details of solutions that are derived, with designation of responsible agencies. JCS/J-2 is responsible to certify the adequacy of the intelligence analysis and results for joint programs.

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/KDP A.

Intelligence Community (IC)—IC members include the Service Intelligence Organizations (Service Cryptologic Elements (SCEs)), NSA, CIA, DIA, NRO, and NGA, as well as Coast Guard Intelligence, Department of Energy, Department of Homeland Security, Department of State, Department of Treasury, and Federal Bureau of Investigation.

Intelligence Deficiency—These are derived intelligence requirements that cannot be met by the current intelligence infrastructure.

Intelligence Infrastructure—The totality of intelligence support needed to ensure effective operation of a system once operational. This includes intelligence people, products, processes, systems, training, and/or facilities.

Intelligence-Sensitive Force Modernization Initiative—Any program/initiative that produces, consumes, processes, or handles intelligence information, thereby requiring threat or intelligence infrastructure support, and which will be measured and evaluated by a program or project office in terms of cost, performance, and impact on warfighter capabilities and fielding, shall be considered intelligence-sensitive. If it is likely that, in the future, the program/initiative would produce, consume, process, or handle intelligence information, then it should be considered intelligence-sensitive.

Intelligence Support Planners—Used as a generic term to refer to individuals who are tasked with creating all, or a portion of, the intelligence content required by this guidance for AF ISPs.

Interoperability—The ability of the systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces, and to use the data, information, materiel, and service so exchanged to enable them to operate effectively together.

ISR MAP Preparation Conference—A meeting (possibly virtual) of IFM intelligence experts from each MAJCOM, AFC2ISRC, and AF/XOIIA-F to determine which capstone deficiencies (created by AFC2ISRC in their cross-program analysis of ISP intelligence content) should be included in the ISR MAP and to establish a prioritized ranking of those deficiencies. The purpose of the meeting is to ensure that the IFM community presents the ISR MAP RAWG with a single, common prioritized list of ISP-derived deficiencies for inclusion in the MAP.

Joint Potential Designator (JPD)—A designation assigned by Vice Director J-8 to specify JCIDS validation, approval, and interoperability expectations.

Key Decision Points (KDP)—Major decision points that separate the phases of a Space acquisition program. (Refer to National Security Space Acquisition Policy 03-01.)

KDP A—Concept/Architecture Development Phase approval

KDP B—Risk Reduction & Design Development Phase approval

KDP C— Acquisition & Operations Support Phase approval

Major Defense Acquisition Program (MDAP)—An acquisition program that is not a highly sensitive classified program and is estimated by the USD(AT&L) to require an eventual total expenditure of more than $365 million in RDT&E funds, $2.190 billion in procurement funds measured in FY 2000 constant dollars, or programs designated as an MDAP by the USD(AT&L).

Materiel Solution—A defense acquisition program (non-developmental, modification of existing systems, or new program) that satisfies identified mission needs.

Milestones (MS)—Major decision points that separate the phases of an acquisition program under the DODI 5000.2 acquisition management framework.

MS A—Technology Development Phase approval

MS B—System Development & Demonstration Phase approval (normally the initiation of an acquisition program)

MS C—Production & Deployment Phase approval

Multi-Service Force Deployment (MSFD)—The MSFD is a digital force projection produced by NASIC that provides details on enemy, friendly, and non-aligned forces in specific geographic areas.

National Security Systems (NSS)—Telecommunications and information systems operated by the Department of Defense – the functions, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves the command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons systems; or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Operating Command—The command primarily operating a system, subsystem, or item of equipment. Generally applies to those operational commands or organizations that Headquarters USAF designates to conduct or participate in operations or operational testing.

Operational Baseline—Described in Sections 2 and 3 of an ISP, the operational baseline should include the combined technology, targets, tactics, CONOPS, environment, employment options, operational factors and threats to the system. This operational baseline serves as a starting point for intelligence infrastructure analysis.

Operational Imperatives—Refinements to the operational baseline. May be expressed in terms of accuracy, precision, timeliness, interoperability, and data formats. Operational imperatives define the basic characteristics of the intelligence support required to make a system effective.

Program Management Directive (PMD)—PMDs direct the implementation of decision documentation in acquisition decision memorandums. PMDs initiate and terminate actions, cite funding sources, and assign responsibilities and tasks to appropriate commands and agencies.

Program Office Intelligence Partner—The intelligence office designated by an ISSG to provide day-to-day intelligence support and oversight on intelligence infrastructure analysis captured in ISP to the program office. Also responsible for distributing ISP-derived deficiency analyses to AFC2ISRC requirements managers.

Strategic Planning Guidance (SPG)—Replaces the policy/strategy sections of the old Defense Planning Guidance. Secretary of Defense's policy and fiscal guidance upon which the military services and defense agencies base their programs and budgets. The SPG provides a broad overview of the expected threat environment and potential adversaries. To establish a thread of continuity in Air Force STARs, SPG scenarios will form the basis for the operational threat environments in STARs.

System Development and Demonstration Phase—The third phase of the DODI 5000.2 acquisition management framework. The purpose of this phase is to develop a system or increment of capability; reduce integration and manufacturing risk; ensure operational supportability; implement human systems integration; design for producibility; ensure affordability; and demonstrate system integration, interoperability, safety, and utility.

System Program Director (SPD)—The single Air Force manager designated by the Program Executive Officer ultimately responsible and accountable for decisions and resources in overall program execution of a military system. (Refer to AFI 10-601)

System Threat Assessment (STA)—System-specific threat assessment produced by the NASIC, under the guidance of a TSG, for ACAT II or Space Major System programs. While following the same format, the STA is generally shorter than a STAR and does not require DIA validation.

System Threat Assessment Report (STAR)—System-specific threat assessment produced by the NASIC, under the guidance of a TSG, for ACAT I programs or Space MDAPs. The STAR identifies and prioritizes foreign threats to a system at initial operational capability (IOC) and at IOC+10 years. STARs are validated by DIA for ACAT ID programs and Space MDAPs, or by NASIC/CC for ACAT IC programs.

Technical Exchange Meeting (TEM)—Held as a subtask to ISWGs to support the derivation, development and documentation of intelligence requirements and deficiencies associated with a proposed program. Not attended by the general members of the ISWG. These meetings include only the technical experts needed to clarify and assess specific program issues that the general ISWG membership is not capable of assessing.

Technology Development Phase—The second phase of the DODI 5000.2 acquisition management framework. The purpose of this phase is to reduce technology risk and determine the appropriate set of technologies to be integrated into a full system.

Weapon System Intelligence Support Requirements Database (WSISRD)—A database designed to support Intelligence in Force Modernization (IFM) implementation. The database is administered by AFC2ISRC/IN, is web-enabled on the SIPRNET, and is used to catalog intelligence deficiencies identified during Intel Infrastructure Analysis. AFC2ISRC/IN uses the database to support Level II Cross-Program Analysis. WSISRD can be found on SIPRNET at <http://afc2isrc.af.smil.mil> under ISR Web Requirement Tools.

Attachment 2

SYSTEM THREAT ASSESSMENT REPORT (STAR) FORMAT

A2.1. Summary. Provides a complete, autonomous threat overview. This section is sharply focused to provide key intelligence judgments. If the Threat Steering Group (TSG) is in agreement on all threat levels for all adversary systems, then the Summary will contain a Threat Matrix (listing major threats and depicting a threat level for each threat at IOC and IOC+10 years). The summary also contains a sub-section entitled, "Significant Changes for this STAR" that identifies significant changes that have been noted since the previous STAR was published and, if a Threat Matrix is included, define the reasons why threat levels were modified.

A2.2. Foreword. Provides the opportunity to identify all of the TSG members and name all of the significant contributors to the STAR. It identifies all of the organizations that coordinated on the STAR and includes names and phone numbers for the STAR author and system Special Program Organization or Joint Program Organization.

A2.3. Section I. Introduction. Includes the mission need for the US system and a sub-section entitled, "Scope of This STAR" that directs the reader to other documents that define threats to critical US systems associated with, but not included in, the STAR.

A2.4. Section II. U.S. System Description. Describes the US system in sufficient detail to assess which threats could jeopardize the proposed system's ability to perform its mission.

A2.5. Section III. Operational Threat Environment. Portrays a generalized, but complete, overview of the operational, physical and technological environment in which the system will have to function. Developments and trends that could reasonably be expected to affect mission capability during the US system's lifetime are projected out to 10 years beyond IOC. Areas covered include enemy doctrine, strategy and tactics affecting system mission(s) and operations. Threat content varies, based on the nature of each program. Should DIA so recommend, a reference to a CTA may replace this section.

A2.6. Section IV. Threats to be countered (if applicable). Includes a full range of targets or other threats to be engaged within the mission areas in which the system is designed to perform. If applicable, an analysis of the actual capabilities and signatures of projected adversary targets/systems is provided.

A2.7. Section V. System-Specific Threat. Focuses on threat capabilities that are relevant to the mission and performance of the US system throughout its operational life. Timeframes for threat "snapshots" are depicted at IOC of the US system and IOC+10 years.

A2.8. Section VI. Reactive Threat. Contains an analytical estimate of the actions potential adversaries might reasonably be expected to take in reaction to the fielding of our developmental system. This estimate is based on historical trends, evidence of research and development, perceived military and political-economic requirements, and technological capabilities. It includes changes in policy, doctrine and tactics or the development of systems with the intent to degrade or defeat our proposed system's capabilities.

A2.9. Section VII. Technologically Feasible Threat. Contains those threats not projected, but considered feasible. Presents plausible alternative courses of action, should the adversary's requirements change from those currently assessed to be most likely. The technologically feasible threat, though not constrained by intelligence projections, is consistent with an adversary's technological base, economic situation, and industrial production capabilities. The technologically feasible threat provides decision-makers with a basis for judgment about the impact on a specific US system, if the threat were to evolve in a direction other than that considered most likely by the US intelligence community.

A2.10. Appendix A. Critical Intelligence Categories (CICs). CICs are categories of threat information established and examined through the collaborative and joint efforts of the intelligence, requirements and acquisition management communities. CICs depict adversary system- and weapon-related characteristics, employment information, and/or technological threshold parameters, changes to which would critically impact the effectiveness or survivability of our proposed developmental system. Each CIC is backed up by a Production Requirement submitted by the SPO/Implementing Command. If a CIC is breached, a telephonic TSG will be called immediately to determine if program reevaluation is necessary.

A2.11. Appendix B. Critical Program Information. Contains system-related information that, if released to potential adversaries, could compromise our developmental system's ability to successfully perform its mission, once fielded. If a Program Protection Plan (PPP) exists, a reference to the PPP should be included in Section II of the STAR/STA, and no Appendix B is required.

A2.12. Appendix C. Abbreviations. A table defining acronyms used in the STAR.

A2.13. Additional Appendixes. May be included, as necessary.

Attachment 3

INTELLIGENCE INFRASTRUCTURE ANALYSIS FORMAT AND CHECKLISTS

A3.1. Intelligence Infrastructure Analysis and ISPs. Intelligence infrastructure analysis, if documented as prescribed below, will result in the content necessary to support DOD ISP requirements. The results of the IIA typically will be used as the intelligence content within the ISP, as the basis for the intelligence support plan within the Integrated Program Summary (for space acquisition initiatives), as input to other acquisition related documents (CDD, CPD, CRD, etc), and to support cross-program analysis. The analysis format recommended below makes visible the logical progression from operational employment or capabilities development concepts to essential supporting infrastructure and interoperability requirements. For programs with moderate or substantial intelligence support needs, the results of IIA will appropriately be documented as an annex to the program ISP to augment and explain the intelligence content within the ISP.

A3.2. Executive Summary. Executive Summary should highlight key intelligence deficiencies and call out any "showstoppers" or major concerns for the program. It should be written for senior-level personnel and be able to stand alone. Ideally, the Executive Summary should be unclassified for widest dissemination.

A3.3. Operational Employment. This section defines the employment concept for the system from which INTELLIGENCE support requirements are derived. Intelligence support planners should ensure that the details of the operational baseline and employment considerations that were used in their requirements analysis process are included. Relevant intelligence activities, interfaces and information flows should be included in the architecture views. "Foreign Threat Considerations" should be included in this portion of the document and is completed as follows:

A3.3.1. If there is no foreign threat annotate this section with "Foreign threat is N/A."

A3.3.2. If there is a foreign threat and that threat is referenced in a system CDD or CPD, this section may refer to the CDD/CPD for threat details.

A3.3.3. If there is a foreign threat and there is no CDD or CPD, this section should contain an appropriate DIA-validated or approved threat reference (e.g., STAR, STA, or CTA).

A3.4. Derived Intelligence Support Requirements. Derived intelligence requirements contain the details of the STT analysis used. ISR Support to Operations (Intelligence Considerations). For each step of the STT analysis, a table should be included that lists the operational considerations, derived intelligence requirements, and the cross-reference to intelligence deficiencies that are discussed in Potential INTELLIGENCE Support Shortfalls and Proposed Solutions discussion. These tables show traceability to operational considerations. The standard STT table format is given in **Figure A3.1.**

Figure A3.1. STT Methodology Table Key.

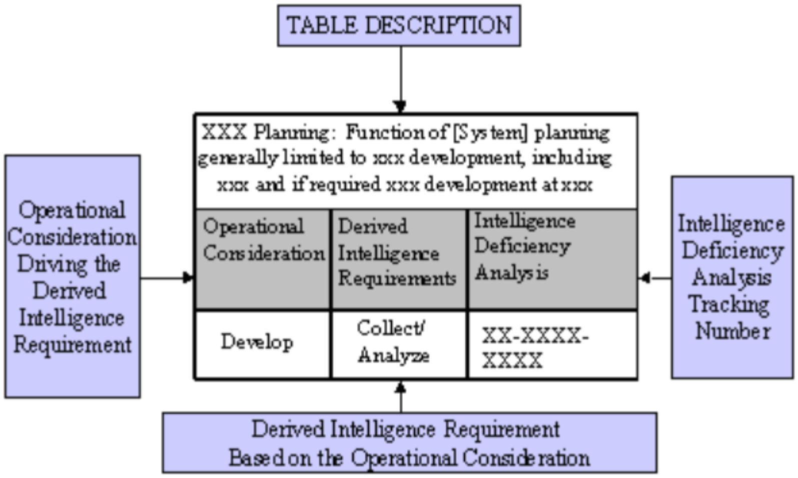


TABLE DESCRIPTION
XXX Planning: Function of [System] planning generally limited to xxx development, including xxx and if required xxx development at xxx
Operational Consideration
Derived Intelligence Requirements
Intelligence Deficiency Analysis
Develop
Collect/ Analyze
XX-XXXX-XXXX
Operational Consideration Driving the Derived Intelligence Requirement
Intelligence Deficiency Analysis Tracking Number
Derived Intelligence Requirement Based on the Operational Consideration

Using a precise coordinate example from a simulated precision-guided munition system, a sample STT is represented in **Table A3.1.** below.

Table A3.1. STT Functions and Intelligence Subtasks.

Mission Execution: Function includes final mission preparation, mission flying, target "acquisition," attacking with weapon, and returning delivery aircraft to base.		
Operational Consideration	Derived Intelligence Requirement	Intelligence Deficiency Analysis
Load mission planning data via Digital Transfer Device (DTD)		
Confirm Mission Acceptance/Designated Mean Point of Impact (DMPIs) Download Global Positioning System (GPS) data to weapon		
Fly mission	Provide Indications and Warning	

Receive targeting update	Provide target coordinate updates in flight	MP-P100-0300 - Precise Point Capability
Derive target coordinates from on-board sensors or third party	Provide third party coordinates	
Release weapons	Process in-flight report (INFLTRP) Collect combat assessment data	
Recover aircraft	Conduct debrief and produce mission report (MISREP)	

A3.5. Potential ISR Support Deficiencies and Proposed Solutions. This section addresses deficiencies in required ISR support capabilities, deficiencies in manpower, training, or doctrine, and any other changes that must be implemented for ISR to support the system. Note: Intelligence partners should ensure existing Intelligence Community products are used to the fullest advantage to resolve potential intelligence deficiencies identified through STT analyses. Each deficiency analysis should be called out separately.

A3.5.1. Identify potential intelligence deficiencies required for system support along with ISWGs-developed solutions and action plans to resolve each deficiency. This information is captured in the intelligence deficiency analysis documentation described below. Each deficiency analysis should begin a new page for ease of identification.

Control Number: XX-YYYY-####

A3.5.2. To enable the Cross-Program Analysis of requirements at the Air Force level, a standard numbering scheme must be followed when documenting these deficiencies. All deficiency analyses will follow the "XX-YYYY-####" numbering scheme described below.

XX = The first characters are a two-letter designator of the category of the process which this intelligence deficiency impacts. This characterization scheme provides a consistent method of identifying the category of requirement. There are nine requirement functional categories:

AQ = Acquisition Support – to include support to testing

OP = Operations Support – catch-all for employment-related requirements

MP = Mission Planning Support

TN = Training Support

TG = Targeting

MS = Modeling & Simulation

AF = Analysis and Fusion

CM = Collection Management

EX = Exploitation and Dissemination Support

A3.5.3. YYYY = The second set of characters is a four character alphanumeric designator (acronym) for the system designated by the author of the deficiency. This designator provides a unique descriptor used to track which program a specific deficiency analysis comes from. AFC2ISRC/IN or AF/XOIIA-F may request a change of the designator to preclude duplicates. Its only use is for tagging specific deficiencies.

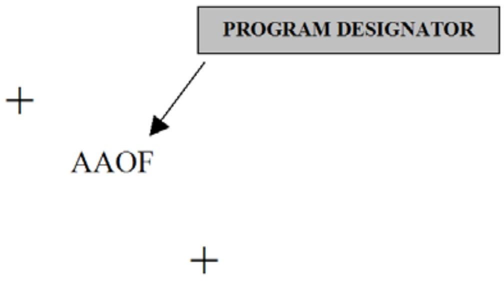
A3.5.4. #### = The final part of the deficiency documentation numbering scheme is a four-digit number defining from which intelligence functional area the solution for the unique deficiency comes. Additional requirements in the same functional area are sequentially numbered (e.g., XX-YYYY-1000, XX-YYYY-1001). Using this numbering scheme consistently provides a mechanism for managing requirements across systems. There are 12 solution functional areas in this part of the numbering scheme:

Table A3.2. Deficiency Control Numbering Key.

SOLUTION FUNCTIONAL AREA	NUMBERING SEQUENCE
GI&S	0100
General Military Intelligence	0200
Comms Infrastructure	0300
Force Management	0400
Imagery Intelligence	0500
Signals Intelligence	0600
Human Intelligence	0700
Measurement & Signature Intel	0800
Intelligence Date Handling Systems	0900
Targeting	1000
Training	1100
Weather	1200

Deficiency Numbering Scheme Example

REQUIREMENT FUNCTIONAL AREA	REQUIREMENT DESCRIPTOR
Acquisition Support	AQ
Operations Support	OP
Mission Planning	MP
Training Support	TN
Targeting	TG
Modeling & Sim	MS
Analysis and Fusion	AF
Collection Mgt	CM
Exploitation and Dissemination	EX



SOLUTION FUNCTIONAL AREA	NUMBERING SEQUENCE
GI&S	0100
General Military Intelligence	0200
Comms Infrastructure	0300
Force Management	0400

SOLUTION FUNCTIONAL AREA	NUMBERING SEQUENCE
Imagery Intelligence	0500
Signals Intelligence	0600
Human Intelligence	0700
Measurement & Signature Intel	0800
Intelligence Date Handling Systems	0900
Targeting	1000
Training	1100
Weather	1200

A3.5.5. As an example, if intelligence support planners are working a program called Advanced Airplane of the Future (AAOF) and have identified a deficiency during capabilities planning that can only be solved with a modification to current intelligence training, the number for this deficiency would be: MP-AAOF-1100.

A3.5.5.1. Title: A descriptive, unclassified title of the requirement that, when read alone, clearly states the deficiency. The title should provide some context for the reader of the requirement.

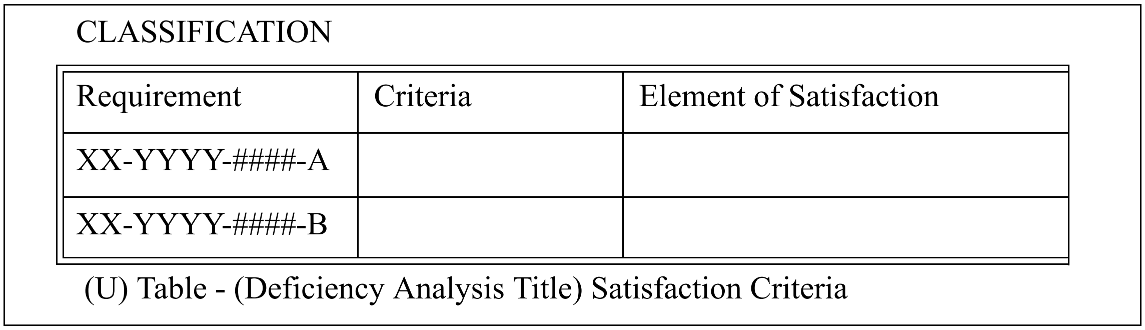
A3.5.5.2. Functional Description: A concise summary of the deficiency analysis. This statement should include a description of the deficiency and the reason the information/resource is required and what operational/acquisition function it supports.

A3.5.5.3. Impact/Risk Statement: A statement addressing what the impact will be if the requirement is not met.

A3.5.5.4. Reference: A reference to the specific section in the CDD, CPD, CONOPS, ISP and/or STT from which this requirement is derived. Include specific chapter/section or a quotation from the CDD/CPD/CONOPS. Reference information is mandatory to provide traceability back to the operational/acquisition requirement.

A3.5.5.5. Satisfaction Criteria: The specific details that fully describe the requirement. Some examples of satisfaction criteria are format, accuracy, timeliness, volume, classification, etc. Define the required capability in as many dimensions as needed and write in terms of measures of performance – the quantitative measure of the lowest level of performance needed to satisfy a requirement. The data to populate the “Criteria” column can be generated using the intelligence functional area checklists. **Figure A3.2.** displays a satisfaction criteria table.

Figure A3.2. Example of Satisfaction Criteria Table.



CLASSIFICATION

Requirement	Criteria	Element of Satisfaction
XX-YYYY-####-A		
XX-YYYY-####-B		

(U) Table - (Deficiency Analysis Title) Satisfaction Criteria

A3.5.5.6. Support Plan/Solution: The solution to the requirement is detailed here. The plan should include as much detail as available. "Potential" solutions may also be listed if the support plan/ solution concept is scenario dependent. As system development progresses, a single solution must be identified.

A3.5.5.7. Significant Action Items: This describes the key action items/steps assigned to implement the time-phased activities, presented in sequence order that will ensure satisfaction of the intelligence deficiency solution. OPRs and operational need dates should be provided. These action items should describe a critical path, which by definition, will result in the overall requirement being satisfied if the action items themselves are successfully executed.

A3.5.5.8. Cost Data: The predicted cost associated with correcting the identified deficiency. If cost information is not available, or the program will not incur a cost, this should be stated. The means to satisfy costs should be identified. This ensures total life-cycle costs can be captured for the system regardless of the funding source.

A3.5.6. Provide a table, including a summary of cost drivers and fiscal year break down of associated costs. An example of a table is **Table A3.3.** below.

Table A3.3. Intelligence Deficiency Analysis XX-YYYY-0100 Estimated Cost to Implement Intelligence Deficiency Solution.

FY (SK)	02	03	04	05	06	07	08	09	10	11	10-YR TOTAL
Hardware	180	0	200	N/A	N/A	N/A	N/A	N/A	N/A	N/A	380
Comm Bandwidth	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
Licenses	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Totals	180	0	200	0	0	0	0	0	0	0	$380

A3.5.7. If one of the cost assumptions is that there will be no program cost for satisfying the requirement, clearly state who will absorb the cost. For example: "Most NGA products and services are provided at no charge to the DOD user." Provide some detail or reference to a system-costing document to describe how the cost numbers were derived for the deficiency analysis. Detailed analysis of cost development may be included as an Appendix to the ISP for ease of reference. This information is intended to provide planners and cost experts with details sufficient to show that the process used in the intelligence deficiency analysis is valid and able to be replicated.

A3.5.8. Overall Requirement Need Date: Provide an actual date or a program milestone (with associated date) by when the requirement must be satisfied.

FUNCTIONAL AREA CHECKLIST #1 FOR IMAGERY INTELLIGENCE (IMINT)

I 1. Is imagery required?

I 2. Who is the customer and where is the intelligence to be delivered?

I 3. Type of imagery required (Optical, RADAR, IR (Infrared), MSI (Multi-Spectral Imagery))

I 4. Essential Elements of Information (EEIs): What specific information must be derived from the imagery?

I 5. Accuracy: coordinates and elevation (circular error (CE), linear error (LE) with confidence level and probabilities (feet, meters, seconds))

I 6. Resolution (inches, feet, meters...), Ground sample distance (GSD)

I 7. Area size: point targets, area coverage, lines of communication (LOCs)...

I 8. Age: How recent must the imagery be?

I 9. Timeliness: What is the latest time the imagery will be useful?

I 10. What are the security classification restrictions?

I 11. Are primary (raw) or secondary (annotated) images required?

I 12. What databases will be used to store and retrieve the IMINT?

I 13. Hard copy: size of print, duplicate positive (DP), original negative (ON), annotations...

I 14. Soft copy: magnetic tape, optical disk, National Imagery Transmission Format (NITF), binary digit (BIT) level...

I 15. Is seasonal coverage required?

I 16. Will detailed, non-imagery graphics suffice?

I 17. Will imagery reports suffice?

I 18. Format/Metadata requirements

I 19. IMINT requirements management

I 20. IMINT collection requirements

I 21. IMINT processing requirements

I 22. IMINT analysis requirements

I 23. IMINT production requirements

I 24. IMINT dissemination requirements

I 25. IMINT application requirements

FUNCTIONAL AREA CHECKLIST #2 FOR SIGNALS INTELLIGENCE (SIGINT)

S 1. Is SIGINT required?

S 2. Who is the customer and where is the intelligence to be delivered?

S 3. Type (e.g. Communications Intelligence (COMINT), Electronic Intelligence (ELINT))

S 4. Essential Elements of Information (EEIs): What specific information must be derived from SIGINT?

S 5. Accuracy: How precisely must SIGINT sensors geolocate electromagnetic emissions for situational awareness and targeting purposes?

S 6. Level of detail: For example, is certain SIGINT reporting required on enemy activity down to regiment, squadron, or flight level? What level of parametric detail is needed on selected radars?

S 7. Age: How recent must the SIGINT information be?

S 8. Timeliness: What is the latest time the SIGINT will be useful?

S 9. Security classification restrictions

S 10. What reporting format is desired?

S 11. What databases will be used to store and retrieve the SIGINT?

S 12. SIGINT requirements management

S 13. SIGINT collection requirements

S 14. SIGINT processing requirements

S 15. SIGINT analysis requirements

S 16. SIGINT production requirements

S 17. SIGINT dissemination requirements

S 18. SIGINT application requirements

FUNCTIONAL AREA CHECKLIST #3 FOR HUMAN INTELLIGENCE (HUMINT)

H 1. Is HUMINT required?

H 2. Who is the customer and where is the intelligence to be delivered?

H 3. Essential Elements of Information (EEIs):
Enemy intentions, plans, and doctrine
Enemy strengths and vulnerabilities
Enemy weapons development
Samples of material

H 4. Level of detail

H 5. Age of information: How recent must the information be?

H 6. Timeliness: When is the latest time the information will be useful?

H 7. Security classification restrictions

H 8. What reporting format is desired?

H 9. What databases will be used to store and retrieve the HUMINT?

H 10. HUMINT requirements management

H 11. HUMINT collection requirements

H 12. HUMINT processing requirements

H 13. HUMINT analysis requirements

H 14. HUMINT production requirements

H 15. HUMINT dissemination requirements

H 16. HUMINT application requirements

FUNCTIONAL AREA CHECKLIST #4 FOR SCIENTIFIC AND TECHNICAL INTELLIGENCE (S&TI)

ST 1. Is S&TI required?

ST 2. Who is the customer and where is the intelligence to be delivered?

ST 3. Essential Elements of Information (EEIs): What specific knowledge must be derived from S&TI?

ST 4. Level of detail: What precision is required for various EEIs? Some technical decisions to be made by your operations and acquisition counterparts demand greater detail about enemy technology than others. Make sure you understand the difference.

ST 5. Age of information: How recent must the data be?

ST 6. Timeliness: When is the latest time the information will be useful?

ST 7. Security classification restrictions

ST 8. What reporting format is desired?

ST 9. What databases will be used to store and retrieve this information?

ST10. S&TI requirements management

ST11. S&TI collection requirements

ST12. S&TI processing requirements

ST13. S&TI analysis requirements

ST14. S&TI production requirements

ST15. S&TI dissemination requirements

ST16. S&TI application requirements

FUNCTIONAL AREA CHECKLIST #5 FOR MEASUREMENT AND SIGNATURE INTELLIGENCE (MASINT)

M 1. Is MASINT required?

M 2. Who is the customer and where is the intelligence to be delivered?

M 3. Type:

--Acoustic: acoustical intelligence (ACOUSTINT), acoustic intelligence (ACINT), SEISMIC

--Electro-optical: infrared intelligence (IRINT), optical intelligence (OPTINT)

--RADAR Intelligence

Radio frequency (RF)/Electro-magnetic pulse (EMP) Intelligence

--Effluent/debris collection

--Laser Intelligence (LASINT)

--Nuclear Intelligence (NUCINT)

--Unintentional Radiation Intelligence (RINT)

M 4. Essential Elements of Information (EEIs): What measurements/signatures of enemy systems are required?

M 5. Accuracy

M 6. Level of Detail: What are the specific parameter requirements needed to support the weapon system navigation and targeting systems, and to help the weapon system survive enemy defenses?

M 7. Age of information: How recent must the information be?

M 8. Timeliness: When is the latest time the information will be useful?

M 9. Security classification restrictions

M 10. What reporting format is desired?

M 11. What databases will be used to store and retrieve this information?

M 12. MASINT requirements management

M 13. MASINT collection requirements

M 14. MASINT processing requirements

M 15. MASINT analysis requirements

M 16. MASINT production requirements

M 17. MASINT dissemination requirements

M 18. MASINT application requirements

FUNCTIONAL AREA CHECKLIST #6 for GEOSPATIAL INFORMATION AND SERVICES (GI&S)/TARGET MATERIALS

MT 1. Is GI&S and/or targeting materials required?

MT 2. Who is the customer and where is the intelligence to be delivered?

MT 3. What types of materials are required?

MT 4. Essential elements of information (EEIs): What specific information must be derived from the GI&S data/targeting materials?

MT 5. Accuracy requirements

MT 6. Level of detail (scale, etc.)

MT 7. Area coverage

MT 8. Age of information: How recent must the information be?

MT 9. Timeliness: When is the latest time the information will be useful?

MT 10. Security classification restrictions

MT 11. What reporting/product formats are desired?

MT 12. What databases will be used to store and retrieve this information?

MT 13. Hard copy: number and size of prints, annotations

MT 14. Soft copy: media, format, compression, encryption (e.g. magnetic tape, optical disk, National Imagery Transmission Format (NITF), binary digit (BIT) level)

MT 15. Is seasonal coverage required?

MT 16. Will detailed, non-imagery graphics suffice?

MT 17. Will imagery reports suffice in some instances?

MT 18. GI&S/TM requirements management

MT 19. GI&S/TM collection requirements

MT 20. GI&S/TM processing requirements

MT 21. GI&S/TM analysis requirements

MT 22. GI&S/TM production requirements

MT 23. GI&S/TM dissemination requirements

MT 24. GI&S/TM application requirements

FUNCTIONAL AREA CHECKLIST #7 for INTELLIGENCE DATA HANDLING SYSTEMS (IDHS)

IDHS 1. Are IDHS required?

IDHS 2. Who is the customer and where is the product/service to be delivered?

IDHS 3. Is automated intelligence data (electric or magnetic media) required for direct input into the weapon system or its associated mission planning system?

IDHS 4. What is the target system?

IDHS 5. What transmission media are needed?

IDHS 6. Is there a known product currently available to meet the requirement? If so, what is it and who is the producer?

IDHS 7. What data format is desired?

IDHS 8. How time-sensitive are the required data?

IDHS 9. How frequent is the need for the data?

IDHS 10. Is update by full-file replacement or report-by-exception preferred?

IDHS 11. Is the requirement for raw intelligence or a fused product?

IDHS 12. Will IDHS send a regular predefined product or is there need to respond to ad hoc tasking/query?

IDHS 13. If ad hoc response is required, will the tasking/query be automated or will it flow through an external (to the system) route?

IDHS 14. What is the highest classification of the target computer system?

IDHS 15. What is the planned classification of any product produced by the target system?

IDHS 16. Where, geographically, is the intelligence information to be delivered?

IDHS 17. Are there already adequate communications in place to support any direct connection required?

IDHS 18. Does the required system exist or is it still in development?

FUNCTIONAL AREA CHECKLIST #8 for FORCE MANAGEMENT: MANPOWER

FM 1. Are intelligence personnel needed to operate or support the system?

FM 2. What type(s) of personnel are needed?

FM 3. How compatible is the new system with systems currently in use?

FM 4. How easy/difficult will the system be to operate/support?

FM 5. What is the operator/system interface?

FM 6. What tasks are required to operate the system? (Include tasks, skills, and knowledge)

FM 7. How many people will need training?

FM 8. How soon will people need to be trained on the system?

FM 9. Will the training be standard regardless of method used? (i.e., in-residence, exportable, on-the-job training (OJT), or mobile training team)

FM 10. Can the system incorporate imbedded training?

FM 11. Is hardware common to other fielded systems?

FM 12. Are operator tasks common to other fielded systems?

FM 13. Is the system interoperable with other fielded systems?

FM 14. What are post-deployment training needs?

FUNCTIONAL AREA CHECKLIST #9 for GENERAL MILITARY INTELLIGENCE (GMI) PRODUCTION

GMI 1. Is GMI required?

GMI 2. Who is the customer and where is the product to be delivered?

GMI 3. What types of products are required?

GMI 4. Essential elements of information (EEIs): What specific information must be derived from GMI?

GMI 5. Age: How recent must the information be?

GMI 6. Timeliness: When is the latest time the information will be useful?

GMI 7. Security classification requirements and restrictions

GMI 8. What databases will be used to store and retrieve this information?

GMI 9. Hard-copy requirements

GMI 10. Soft-copy requirements

GMI 11. Can requirement be satisfied through existing production?

GMI 12. If existing products do not suffice, determine satisfaction through scheduled products

GMI 13. Assess the risk of not having the required intelligence for mission execution

GMI 14. Assess priority of this requirement in context of all outstanding requirements

GMI 15. If no products (existing or scheduled) suffice, begin request/validation of requirement in accordance with DIAM 57-1

FUNCTIONAL AREA CHECKLIST #10 for DEVELOPMENT AND INTELLIGENCE INFRASTRUCTURE ISSUES

DII 1. Does the intelligence needed currently exist?

DII 2. If not, can it be collected with current assets?

DII 3. Are new collection management procedures needed?

DII 4. Is there a product currently available to meet the need? In the proper format?

DII 5. Can a current product be modified to meet the requirement?

DII 6. Is a new product needed? How soon?

DII 7. Are current models adequate to support research, development and testing?

DII 8. Does the Integrated Weapon System Manager have unique intelligence requirements or support needs? (i.e., special modeling or simulation needs, equipment, military construction such as sensitive compartmented information facility (SCIF) space, special security office (SSO) support?)

Attachment 4

ISSG PROCESS

A4.1. Background. The need for an Intelligence Support Steering Group was identified during the development of the Intelligence in Force Modernization strategy. The strategy defines goals and objectives that address shortfalls in Air Force intelligence integration in weapons program development. Specifically, the ISSG engages key acquisition and intelligence players, provides guidance, and assigns responsibilities to turn the concept of intelligence support to acquisition into the reality of fielded capabilities to support the warfighter.

A4.2. Purpose. The ISSG has four primary purposes:

A4.2.1. Assign organizations (intel partners) clear roles and responsibilities for providing intelligence support for the nominated program/initiative. Clear lanes-in-the-road are defined by the ISSG to ensure requirements are understood and POCs are identified.

A4.2.2. Estimate the type and level of intelligence support required to ensure intelligence issues are properly addressed throughout the program/initiative's acquisition process and field operations.

A4.2.3. Provide critical cost and intelligence infrastructure availability information to force modernization decision makers. Known shortfalls, as well as commitments to resolve them, are documented in the ISSG minutes.

A4.2.4. Provide an overview of the Intelligence Infrastructure Analysis process to key acquisition and intelligence personnel.

A4.3. Membership of an ISSG.

A4.3.1. Core members include:

Chair, AF/XOIIA-F

Operating MAJCOM Intelligence

Operating MAJCOM Requirements and/or Operations

Implementing MAJCOM Intelligence

Applicable Center/Lab/Research Site DI

AFC2ISRC Intelligence

Program/Initiative Lead

A4.3.2. Other members may include: Center/Lab/Research Site requirements and future plans offices, SAF/AQ/FM/XI, AFCAA, HQ AFRL, AFOTEC, OAS, intelligence production centers, AIA, other services, agencies, departments, etc.

A4.4. Operational Concept.

A4.4.1. Types of ISSGs. There are three types of ISSGs: Topical, Out-of-Cycle, and Transition.

A4.4.1.1. Topical ISSGs. Topical ISSGs are held annually to address intelligence support planning for a large number of programs. Nominated programs are consolidated into topical areas of interest whenever possible. Topical categories include Aeronautical, Air Armament, C4ISR/IW (Command, Control, Communications, and Computers/ Information Warfare), Space and Missiles, and Joint Programs. Force Modernization initiatives may be placed into one of these general topical categories, or further broken out into smaller ISSG categories, as required. Location of the ISSG will be based on the location of the nominated initiatives. The goal is to host the meeting where the majority of responsible offices/stakeholders reside. Video teleconferencing may also be considered. Nominations that cannot be addressed (for example, due to time constraints or unavailability of principals) at the announced ISSG will be scheduled for the next topical ISSG. If a program/initiative requires immediate support, MAJCOM SIOs should consider requesting AF/ XOI to convene an ISSG outside of the normal cycle.

A4.4.1.2. Out-of-Cycle ISSGs. MAJCOM SIOs can request Out-of-Cycle ISSGs if a program/initiative requires urgent attention or it was not ready to be presented at its applicable topical ISSG. Out-of-Cycle ISSGs are held on an as needed basis. Location of the ISSG will be based on the location of the nominated initiative(s). The goal is to host the meeting where the responsible offices/stakeholders reside. Video teleconferencing may also be considered.

A4.4.1.2.1. After considering/researching the request for an ISSG, AF/XOIIA-F is the decision authority to convene an ISSG. If AF/XOIIA-F decides not to convene an ISSG, they will identify to the requestor suitable references to obtain the information they need about baseline intelligence infrastructure capabilities and costs.

A4.4.1.3. Transition ISSGs. Transition ISSGs are held only if necessary to enable reconsideration of intelligence support needs/shortfalls/costs as the program/initiative matures from one acquisition phase to the next. There may be derived deficiencies that remain "open" as a program begins to transition and the role of intel partner may shift from one DI to the next or from the implementing command to the operating command. The transition ISSG reassigns responsibilities and ensures intel support continues to be seamlessly integrated into the program. The purposes of the transition ISSGs are slightly different from other ISSGs. They include:

A4.4.1.3.1. Address status of outstanding derived deficiencies.

A4.4.1.3.2. Assign responsibility for tracking remaining derived deficiencies.

A4.4.1.3.3. Reassign intelligence partner roles.

A4.4.1.3.4. Refine estimates of the baseline intelligence infrastructure capability to support the weapon/program intelligence needs (based upon the developer's refined understanding of their own issues/problems).

A4.4.1.3.5. Address outstanding derived deficiency costs and the potential budgeting strategy for each.

A4.4.1.4. ISSG Nomination Process. AF/XOI will release an ISSG call for topics message NLT 75 days prior to an ISSG start date. This announcement identifies the ISSG topic and invites MAJCOMs to nominate programs/initiatives that need to be addressed.

A4.4.1.5. Each MAJCOM and AFC2ISRC will solicit nominations from their respective units and headquarters staff. MAJCOM SIOs validate, prioritize, and consolidate their command nominations into a single list that is sent to AF/XOIIA-F, with info to AFMC/XRI. MAJCOM SIOs must ensure that nominations contain all required information and that nominated initiatives meet "intelligence sensitivity" criteria. MAJCOM SIOs must sign nomination packages (electronic signature is acceptable).

A4.4.1.6. Ideally, ISSGs are convened during the concept or technology phase. This enables intelligence interoperability and supportability issues to help shape the design of the future program/ initiative. Major modifications, upgrades, or pre-planned product improvements may also require ISSGs if the program/initiative has not been addressed previously by the ISSG process.

A4.4.1.7. Nomination Evaluation Criteria. The following criteria are used to evaluate ISSG nominations:

A4.4.1.8. Intelligence Sensitivity

A4.4.1.9. MAJCOM requirements (Who wants the system? Has the operational concept been accepted?)

A4.4.1.10. MAJCOM priority (How soon is this system needed?)

A4.4.1.11. Resource constraints (Is there funding or plans to fund intelligence infrastructure analysis and development? Funding for intelligence operations?)

A4.4.1.12. Program milestone or status

A4.4.1.13. Planning for emerging (potential "black") programs (What intelligence infrastructure needs to be in place?)

A4.4.1.14. Accelerated technology integration (higher priority due to operational need)

A4.4.1.15. Intelligence Sensitivity Criteria. The following criteria should be applied to determine intelligence sensitivity of the program/initiative:

A4.4.1.16. Any program/initiative that produces, consumes, processes, or handles intelligence data, thereby requiring threat or intelligence infrastructure support, and which will be measured and evaluated by a program or project office in terms of cost, performance, and impact on warfighter capabilities and fielding, shall be considered intelligence-sensitive. If it is likely that, in the future, the program/initiative would produce, consume, process or handle intelligence information, then it should be considered intelligence-sensitive.

A4.4.1.17. Intelligence Infrastructure = People, Products, Process, Systems, Training, and/or Facilities.

A4.4.1.18. Required information for Nominations. The following information is required in order for AF/XOIIA-F to consider a nomination for an ISSG:

A4.4.1.18.1. Name and description of program/initiative

A4.4.1.18.2. Status (ACAT/Milestone information as applicable)

A4.4.1.18.3. Sponsoring operational MAJCOM

A4.4.1.18.4. Date ISP is needed (if known)

A4.4.1.18.5. Rationale for nomination (intelligence sensitivity level, type of intelligence support issues, etc.)

A4.4.1.18.6. Name, organization, and phone number of POC (Program Manager, study lead, MAJCOM and Acquisition POCs)

NOTE: MAJCOM SIOs must ensure that program managers/study leads understand their role at the ISSG and within IFM Strategy at the time of their nomination.

A4.4.1.19. ISSG Cost Estimating. The ISSG will estimate the approximate cost of intel support planning for each program/initiative. This will include day-to-day intel support by the MAJCOM and production center intelligence staff, ISWG activity, and production of the intelligence support plan. The costs defined during the ISSG are usually defined in man years by the organization responsible for direct intelligence support together with the program initiative lead. This agreement is then integrated into the program/initiative budget/POM. Detailed intelligence costs are defined via the ISWG process.

A4.4.1.20. ISSG Due Outs. The ISSG Chair will ensure the objectives of the ISSG are attained and results are documented. These results as well as ISSG decisions are published via an AF/XOI message. Specifically, the AF/XOI message documents:

A4.4.1.20.1. Clear "lane-in-the-road" responsibilities for each participating member of the ISSG, including assignment of the intel partner and agreement on responsibility for organizing and facilitating associated Intelligence Support Working Groups (ISWGs).

A4.4.1.20.2. Estimates of the level and type of intelligence support required for the program/initiative, project or technology.

A4.4.1.20.3. Preliminary cost estimates for intelligence support.

A4.4.1.20.4. For "Transition ISSGs": reassign responsibility for tracking outstanding derived requirements.

A4.4.1.20.5. For "Transition ISSGs": reassign the intelligence partner role.

ISSG CHECKLISTS

<u>Call for Topics (NLT 75 days before scheduled ISSG)</u>

AF/XOIIA-F will release a "Call for Topics" message requesting that MAJCOMs nominate programs for ISSG consideration.

Note: Following release of the "Call for Topics" message, MAJCOM/INs will also receive a duplicate message via email, to ensure receipt.

MAJCOM SIOs/DIs will assess command development efforts and, in partnership with program managers/study leads, solicit nominations.

MAJCOM SIOs will analyze the nominations to ensure they are intel-sensitive, early in the program/study development process, and fit the specific topical ISSG.

Note: MAJCOM SIOs must ensure that program managers/study leads understand their role at the ISSG and within IFM Strategy at the time of their nomination.

SIOs will validate and send a single nomination list for their command to AF/XOIIA-F <u>within 30 days of receipt of the ISSG Call for Topics Message</u>.

<u>Creating Agenda (NLT 30 days prior to the scheduled meeting date)</u>

AF/XOIIA-F will publish an agenda for the Topical ISSG.

MAJCOM INs will work with AF/XOIIA-F to contact each Force Modernization POC and discuss the following:

> Availability for the Topical ISSG – deconflict timeslots as necessary (and ensure they understand the need to attend the Orientation Session on the first morning of the ISSG). Note: Orientation session includes the ISSG Overview brief and the Infrastructure Analysis brief.
>
> Ensure that a representative who can accept responsibilities on behalf of the program and address general resource issues will attend the Topical ISSG.
>
> Inform them of the need to provide a 10-15 minute System Overview briefing.

AF/XOIIA-F will publish a final agenda including logistics information (lodging, transportation, location, RSVP POC, security requirements, etc.).

ISSGs are usually held at the location where the majority of nominated Force Modernization efforts POCs reside.

<u>Pre-Coordination/Read Aheads (NLT 30 days to 7 days before ISSG)</u>

AF/XOIIA-F, applicable MAJCOM INs, and nominated Force Modernization representatives will coordinate on "AF/XOI Draft Minutes Message".

AF/XOIIA-F, applicable MAJCOM INs, and nominated Force Modernization representatives will coordinate on System Overview Briefs.

AF/XOIIA-F will set up Intel Pre-ISSG Meeting with hosting IN prior to the ISSG meetings.

Meeting must include AF/XOIIA-F, AFC2ISRC/IN, Implementing Command IN, Operating Command IN, hosting IN, other appropriate Intelligence Partners (no Force Modernization initiative representatives at this meeting).

Meeting is to ensure everyone is in agreement on intel community roles and discuss any potential controversial issues before meeting with programs during the ISSGs.

Post ISSG Actions

AF/XOIIA-F will publish the results of the ISSG in a follow-up AF/XOI minutes message (NLT 7 days) after the meeting.

Attendees will follow up on any action items pending from the ISSG (issue resolution, responses to questions, etc.).

The ISSG is the initial step for ISWGs and the eventual Intelligence Infrastructure Analysis.

MAJCOM SIOs should provide a program/initiative's ISWG schedule (NLT 180 days) to AF/XOIIA-F.

AF/XOIIA-F will release an IFM guidance message.

MAJCOM SIOs should provide a consolidated status/recap report of derived Intelligence requirements and deficiencies identified via Intelligence Infrastructure Analysis.

MAJCOM IN

ISSG Nomination Checklist

Assess command development efforts and solicit nominations from the field.

Review field nominations, collate, and/or reassign if necessary to applicable Topical ISSG.

Is the program/initiative intel sensitive?

Has program been addressed by an ISSG before?

Ensure local DI meets with Program Manager (PM)/Study Lead and fully explains the ISSG process.

Ensure PM/Lead will attend ISSG or an appointed representative will be able to represent/speak for them and make decisions related to the program/initiative.

Work with PM and requirements manager/AoA lead to determine program/initiative priority within the MAJCOM.

Draft and submit to AF/XOIIA-F the MAJCOM nominations.

Ensure appropriate field level SIOs and PM/Lead are info'd on MAJCOM nomination message.

OUT-OF-CYCLE ISSG CHECKLIST

MAJCOM SIO Will Request Out-of-Cycle ISSG

MAJCOM SIOs/DIs will assess command development efforts and, in partnership with program managers/study leads, nominate applicable programs/initiatives for an out-of-cycle ISSG. If and only if the program requires urgent attention and/or there is not an upcoming Topical ISSG.

Note: MAJCOM SIOs must ensure that program managers/study leads understand their role at the ISSG and within IFM Strategy at the time of their request.

After considering/researching the request for an ISSG, AF/XOIIA-F is the decision authority to convene an ISSG. If AF/XOIIA-F decides not to convene an ISSG, they will identify to the requestor suitable references to obtain the information they need about baseline intelligence infra structure capabilities and costs.

Creating an Agenda

AF/XOIIA-F will publish an agenda for the Out-Of-Cycle ISSG.

MAJCOM INs will work with AF/XOIIA-F to contact each Force Modernization POC and discuss the following:

Availability for the Out-Of-Cycle ISSG – deconflict timeslots as necessary.

Ensure that a representative who can accept responsibilities on behalf of the program and address general resource issues will attend the ISSG.

Inform them of the need to provide a 10-15 minute System Overview briefing.

AF/XOIIA-F will publish a final agenda including logistics information (lodging, transportation, location, RSVP POC, security requirements, etc.).

Pre-Coordination/Read Aheads

AF/XOIIA-F, applicable MAJCOM INs, and nominated Force Modernization representatives will coordinate on "AF/XOI Draft Minutes Message".

AF/XOIIA-F, applicable MAJCOM INs, and nominated Force Modernization representatives will coordinate on System Overview Briefs.

AF/XOIIA-F will set up Intel Pre-ISSG Meeting with hosting IN prior to the ISSG meetings.

Meeting must include AF/XOIIA-F, AFC2ISRC/IN, Implementing Command IN, Operating Command IN, hosting IN, other appropriate Intelligence Partners (no Force Modernization initiative representatives at this meeting).

Meeting is to ensure everyone is in agreement on intel community roles and discuss any potential controversial issues before meeting with programs during the ISSGs.

Post ISSG Actions

AF/XOIIA-F will publish the results of the ISSG in a follow-up AF/XOI minutes message (NLT 7 days) after the meting.

Attendees will follow up on any action items pending from the ISSG (issue resolution, responses to questions, etc.).

The ISSG is the initial step for ISWGs and the eventual Intelligence Infrastructure Analysis.

MAJCOM SIOs should provide a program/initiative's ISWG schedule (NLT 180 days) to AF/XOIIA-F.

AF/XOIIA-F will release an IFM guidance message.

MAJCOM SIOs should provide a consolidated status/recap report of derived Intelligence requirements and deficiencies identified via Intelligence Infrastructure Analysis.

Attachment 5

ISP PROCEDURES AND FORMATS

A5.1. Background. The ISP replaces the C4ISP originally mandated in the DOD 5000 series directives. CJCSI 6212.01C mandates that an ISP be created for all ACAT programs. The ISP describes system dependencies and interface requirements in sufficient detail to enable testing and verification of IT and NSS interoperability and supportability.

A5.2. Format. Guidelines for the ISP format are contained in DODI 4630.8. This instruction does not currently contain enough detail to rely on exclusively for guidance in identifying data necessary for inclusion. Recommend referring to DOD 5000 series directives for detailed guidance. ISPs are composed using the following format:

Chapter 1 – Introduction (Overview and Program Data)

Chapter 2 – Analysis

Chapter 3 – Issues

Appendix A. – References

Appendix B. – Systems Data Exchange Matrix (System View-6)

Appendix C. – Interface Control Agreements

Appendix D. – Acronym List

Other Appendixes

A5.2.1. **Intelligence Content.** The content within the ISP should mirror chapters four and five from the C4ISP. For organizations that have a C4ISP and need to develop an ISP, it is acceptable to transfer the data from chapters four and five of the C4ISP into the ISP annex renumbering paragraphs as required. This does not eliminate the requirement to update this data annually. Intelligence content associated with each chapter is depicted below:

A5.2.1.1. *Chapter 1 – Introduction*: Overview text should address how the capability relates to the battlespace awareness integrated architecture, or other intelligence support elements of other Joint Functional Areas/Concepts (JFA/JFC), such as targeting subarchitectures as part of the Force Application JFA/JFC. Address whether the desired capabilities described relate to any of the key intelligence Capstone Requirements Documents such as Distributed Common Ground/Surface System (DCGS), Imagery and Geospatial Intelligence (IGI), United States MASINT System (USMS), Moving Target Indicator (MTI), or Unified Cryptologic System (UCS). Program Data addresses any program-related acquisition scheduling issues that have precluded conducting full intelligence information need and supportability analysis. For example, system-level detail may not be available until prime contractor selections have been made, or until the functional solution has been more refined.

A5.2.1.2. *Chapter 2 – Analysis*: Ensure the service or joint intelligence support missions or functions to be provided are consistent with the operational capabilities outlined in the associated CDD or CPD. Ensure intelligence information needs are completely addressed and clearly related to these missions or functions, and that they include the required qualitative and quantitative attributes discussed in Enclosure E of DODI 4630.8. Ensure the scope of analysis for intelligence information needs addresses all stages of acquisition, to include development, testing, training, and operation. Ensure the supportability assessment adequately considers the ability of the service or joint intelligence architecture to both quantitatively and qualitatively satisfy the intelligence information needs. This section of the ISP must contain a description of the Intelligence requirements derived from the Intelligence Infrastructure Analysis outlined in chapter **1.7.** of this document. The content of this section must be consistent with chapter 9 of the associated CDD or CPD.

A5.2.1.3. *Chapter 3 – Issues*: Ensure that all intelligence-related shortfalls, issues, and associated mitigation strategies or resolution paths generated by IIA have been addressed. The content of this section must be consistent with chapter 9 of the associated CDD or CPD.

A5.2.1.4. *Appendix A. – References*: Ensure the Battlespace Awareness Joint Functional Concept is cited if applicable. Ensure the currency of any relevant DIA or Service-validated threat references used.

A5.2.1.5. *Appendix B. – Systems Data Exchange Matrix (System View-6)*: Ensure intelligence nodes and systems/subsystems have been adequately represented in the Systems Information Exchange Matrix (SV-6).

A5.2.1.6. *Appendix C. – Interface Control Agreements*: Not applicable.

A5.2.1.7. *Appendix D. – Acronym List*: Ensure appropriate intelligence-related acronyms are included for clarity.

A5.2.1.8. *Other Appendixes*: If any intelligence considerations exist that are not addressed elsewhere in the ISP, the supporting intelligence office should determine in conjunction with the program manager whether an additional appendix to address the issue would be appropriate.