

**1 OCTOBER 1997**



**Intelligence**

**INTELLIGENCE SUPPORT TO THE AIR  
FORCE ACQUISITION PROCESS**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the SAF/AAD WWW site at: <http://afpubs.hq.af.mil>. If you lack access, contact your Publishing Distribution Office (PDO).

---

OPR: HQ 497 IG/INO  
(Lt Col Richard M. Chapin)  
Supersedes AFI 14-208, 21 March 1994.

Certified by: HQ USAF/XOII  
(Mr. Dennis H. Alvey)  
Pages: 25  
Distribution: F

---

This instruction implements AFPD 14-1, *Air Force Intelligence Planning and Operations*, by providing guidance in identifying and acquiring intelligence to support the Air Force requirements and acquisition process, including technology efforts and Advanced Concept Technology Demonstrations (ACTDs). This AFI applies to all Air Force organizations and covers support beginning with Pre-Milestone 0 (pre-MS 0) and continuing throughout the life cycle of a program, from identification of need through development, acquisition, testing, operational employment, and sustainment and modification. This instruction supports Defense Intelligence Agency (DIA) Regulation 55-3, *Intelligence Support for Defense Acquisition Programs*, March 30, 1992; DoD 5000.2-R *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) Acquisition Programs*, March 15, 1996, with Change 1; Air Force Policy Directive (AFPD) 10-6, *Mission Needs and Operational Requirements*; AFPD 10-14, *Modernization Planning*; AFPD 62-2, *System Survivability*; AFPD 63-1, *Acquisition System*; and AFPD 99-1, *Test and Evaluation Process*. **Attachment 1** lists the references, abbreviations, acronyms, and terms used.

**SUMMARY OF REVISIONS**

**This document is substantially revised and must be completely reviewed.**

This issuance aligns duties for developing Intelligence Support Plans (ISPs). Duties that were previously assigned to HQ USAF/INXXA have been reassigned to the HQ 497 IG. It specifies the essential responsibility of operating commands to define operational requirements of specific weapon systems, and of implementing commands to define acquisition and sustainment requirements. It also specifies that weapon system planning and cost analyses include/consider the cost of unique intelligence support throughout the system lifecycle. Additionally, this revision reflects changes in the production, review, and approval of System Threat Assessment Reports (STARs) and their impact on roles and responsibilities.

ties of HQ 497 IG and other organizations providing threat support to weapon systems acquisition. An expanded role of the Threat Steering Group (TSG) is also outlined.

## **Chapter 1**

### **RESPONSIBILITIES**

#### **1.1. HQ USAF/XOI:**

- 1.1.1. Provides policy guidance to AIA and MAJCOMs on acquisition-associated programs, activities, or issues.
- 1.1.2. Approves Intelligence Support Plans (ISPs).
- 1.1.3. Advises Air Staff and Secretariat on acquisition-associated threat developments.

#### **1.2. HQ/AIA:**

- 1.2.1. Plans and programs for command acquisition-associated intelligence capabilities.
- 1.2.2. Ensures coordination between and confluence of subordinate acquisition-associated TED intelligence plans and operations.

#### **1.3. HQ 497 IG/INO:**

- 1.3.1. Manages overall intelligence infrastructure support to Air Force and Air Force-led joint acquisition and Research and Development (R&D) programs for HQ USAF/XOI, as follows:
  - 1.3.1.1. Ensures all Mission Needs Statements (MNSs) are reviewed for accurate assessment of threat and documentation of intelligence infrastructure support requirements.
  - 1.3.1.2. Ensures all Operational Requirements Documents (ORDs) are reviewed for accurate assessment of threat and documentation of intelligence infrastructure requirements. Ensures unique intelligence information requirements identified in ISPs are included in the corresponding ORD.
  - 1.3.1.3. Ensures draft Program Management Directives (PMDs) are reviewed during the preparation and updating cycle for the proper tasking of intelligence infrastructure support. Works with the Program Element Monitors (PEMs) to ensure direction to write the ISP is included in the PMD (in accordance with AFI 10-601 Paragraph 15).
  - 1.3.1.4. Determines, in consultation with the implementing and operating commands, SAF/AQ, USAF/XOI, and program offices, which acquisition programs require an Intelligence Support Plan (ISP). Programs are considered as early as possible in the acquisition process (preferably pre-MS 0) to determine the need for an ISP.
  - 1.3.1.5. Chairs Intelligence Support Working Groups (ISWGs), which are essentially working-level Integrated Process Teams (IPTs) for total life-cycle intelligence support, and provides program policy and guidance. Assists the operating command, implementing command, and other ISWG members in defining intelligence needs (*e.g.*, collection, production, and dissemination requirements) for development, acquisition, test, operation and sustainment of the system. Ensures these are included in the ISP.
  - 1.3.1.6. Coordinates, as needed, with national intelligence agencies to ensure applicable requirements are satisfied.

- 1.3.1.7. Facilitates the effective and efficient implementation of the requirements identified in the ISP. Conducts the proper analysis and evaluation of options to address programming solutions.
  - 1.3.1.8. Reviews and provides advice on total life-cycle intelligence support to Analysis of Alternatives (AoA) meetings as needed.
  - 1.3.1.9. Reviews and provides advice on sections of the Test and Evaluation Master Plan (TEMP) to the acquisition community relating to total life-cycle intelligence support as needed.
  - 1.3.1.10. Assigns Intelligence Counterpart Officers (ICOs) to acquisition and sustainment programs and R&D efforts as required.
  - 1.3.1.11. Develops ISPs to document required intelligence in close cooperation with the operating command, implementing command, and other ISWG members.
  - 1.3.1.12. Assists in developing intelligence infrastructure life-cycle cost and performance data for inclusion in program plans and cost estimates, and use in AoA.
  - 1.3.1.13. Coordinates with national intelligence organizations (and sister-service intelligence organizations for joint systems) to ensure applicable requirements and costs are identified and included in the ISP.
  - 1.3.1.14. Ensures life-cycle intelligence infrastructure cost data developed by the implementing command (*e.g.*, System Program Director ) is included in the ISP.
  - 1.3.1.15. Reviews ISPs at least annually. Updates ISPs as required and makes updated ISPs available 90 days before each milestone decision.
  - 1.3.1.16. Monitors ISP execution.
  - 1.3.1.17. Develops and maintains ICO standards, procedures, and training programs. Conducts ICO training as needed. Responsible for ISP format standardization.
- 1.3.2. Manages threat support to Air Force and Air Force-led joint acquisition programs for HQ USAF/XOI, as follows:
- 1.3.2.1. Chairs Threat Steering Groups (TSGs) which are essentially working-level IPTs for threat support, for individual programs. The TSG initiates, reviews, and recommends AF approval of System Threat Assessment Reports (STARs) and System Threat Assessments (STAs).
  - 1.3.2.2. Chairs TSGs for Threat Environment Descriptions (TEDs), providing baseline threat projections for Air Force mission areas. Reviews TEDs.
  - 1.3.2.3. Reviews, comments on, and ensures consistency in the threat-related sections of MNSs, ORDs, Mission Area Plans (MAPs), TEMPs and AoAs.
  - 1.3.2.4. Upon request from HQ USAF/XORD, prepares Intelligence Reports for milestone decisions, summits, and other major program reviews that document and update threats to the system. (DIA prepares intelligence reports for Defense Acquisition Board (DAB) reviews.)
  - 1.3.2.5. Participates in Threat Working Groups (TWGs), which are essentially working-level IPTs for threat support, and other forums as required to ensure consistent threat support throughout the program's life.
  - 1.3.2.6. Performs data audits and other evaluations of digital models and simulations to ensure accurate and appropriate representation of the threat.

1.3.2.6.1. Advises the AoA Study Director on models, data sources, target selection, and scenario issues.

1.3.2.6.2. During the PMD preparation process, reviews the draft PMD, as directed, to ensure threat support receives proper tasking.

1.3.3. Ensure that the proper agencies responsible for training are notified of any intelligence-unique training requirements as a result of the ISP process.

#### **1.4. National Air Intelligence Center (NAIC):**

1.4.1. Produces, integrates, coordinates and assures quality in STARs, STAs, and TEDs in accordance with TSG direction.

1.4.2. NAIC/CC, after TSG recommendation, is the final approval authority for STARs/TEDs and final validation authority for STAs for HQ USAF/XOI.

1.4.3. Participates in TSGs, TWGs, and other forums as required, to ensure accurate and appropriate representation of the threat.

1.4.4. Produces other intelligence products in accordance with validated production requirements (PRs) and the DoD Intelligence Production Program (DoDIPP).

#### **1.5. MAJCOM Senior Intelligence Officers (SIO):**

1.5.1. Provide intelligence infrastructure support to weapon systems acquisition programs as follows:

1.5.1.1. Assist in the development of the MNS, identifying general intelligence implications. Make recommendations to 497 IG/INO concerning the selection of acquisition and sustainment programs and R&D efforts for which an ISP should be required.

1.5.1.2. Assign primary ICOs to those acquisition and sustainment programs and R&D efforts selected for ISP development.

1.5.1.3. Participate in ISWGs.

1.5.1.4. Assist HQ 497 IG in developing ISPs for selected acquisition and sustainment programs and R&D efforts. Define intelligence-related operational requirements and concepts of operation (CONOPs) for specific systems and coordinate with HQ 497 IG to ensure these are included in the ISP.

1.5.1.5. Program for intelligence support resources required to satisfy unique weapon systems needs established during the ISP development process.

1.5.1.6. Ensure intelligence infrastructure considerations are properly addressed in ORDs and AoAs, whether or not an ISP is directed for that weapon system.

1.5.1.7. Assists the implementing command in developing intelligence infrastructure life-cycle cost and performance data for inclusion in program plans and cost estimates and use in AoA.

1.5.1.8. Coordinate all ISPs through operating command HQ staff (2-letter level). Ensure DR validates intelligence requirements. Submit final operating command HQ-approved ISP to HQ 497 IG for submission to Air Staff (USAF/XOI) for final approval.

1.5.2. Provide intelligence threat support to weapon system acquisition programs as follows:

- 1.5.2.1. Prepare threat assessments in MNSs, ORDs, CONOPs and AoAs.
- 1.5.2.2. Participate in STAR/STA/TED TSGs and the STAR/STA/TED review processes.
- 1.5.2.3. Assist AoA Study Director, as required, with appropriate threat and scenario inputs for the duration of AoA.
- 1.5.2.4. Prepare and submit Intelligence PRs and Statements of Intelligence Interest (SII).
- 1.5.2.5. Post-Milestone I, update threat data in the AoA and ORD for subsequent milestone reviews.

## **1.6. Implementing Command Designated Intelligence Element:**

- 1.6.1. Develops intelligence needs to support the research, development, test, acquisition, and maintenance of Air Force weapon systems.
- 1.6.2. Provides tailored intelligence support to lab activities, Technical Planning Integrated Product Teams (TPIPTs), development planners, and other pre-Milestone 0 activities. Ensures TPIPTs are aware of intelligence infrastructure issues. Provides information applicable to intelligence infrastructure and product planning from these activities to HQ 497 IG.
- 1.6.3. Assigns ICOs to support selected programs in coordination with HQ 497 IG and the operating command, and participates in ISWGs.
- 1.6.4. Works with the SPO staff to identify, as early as possible, intelligence needs supporting proposed employment of systems/components and to incorporate those needs into program plans and costs.
- 1.6.5. Assists SPO staff in clarifying total life-cycle intelligence support needs identified in the ISP and incorporating those needs into modernization planning documents and the Single Acquisition Management Plan (SAMP), as applicable.
- 1.6.6. Working with the System Program Director and the AFMC Product Center Financial Management (FM) staff, supports the estimation of total life-cycle intelligence cost data and incorporation of that data into program plans and cost estimates. Coordinates with HQ AFMC/IN to identify the appropriate Air Force cost analysis organization for producing the above estimate for inclusion in the ISP. Assists the SPO staff and using command elements in incorporating total life-cycle intelligence cost and performance data for the AoA.
- 1.6.7. Working with the SPO staff, operational command, and AFMC/IN, ensures that intelligence requirements are identified, documented, and addressed in the evaluation of alternative concepts at Milestone I and alternative design approaches at Milestone II.
- 1.6.8. Assists HQ 497 IG/INO in its review of program documentation to ensure that intelligence products required for the operation of the system or its subsystems are included in program logistics planning and the SAMP, as applicable.
- 1.6.9. Coordinates on ISPs before USAF/XOI approval.
- 1.6.10. Provides tailored threat support, facilities definition, and documentation of intelligence threat needs to support the research, development, test, acquisition and sustainment of Air Force Weapon Systems.

1.6.11. Provides routine intelligence support, review of Security Classification Guides, and contractor-release approval; and participates in TSGs and TWGs.

1.6.12. Works with the SPOs and Director of Intelligence to prepare and submit PRs and SIIs.

1.6.13. Maintains threat documentation libraries.

1.6.14. Works with AFOTEC and SPOs to ensure threat data is kept up to date in TEMPs during post-Milestone I.

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

1.7.1. Participates in ISWGs and TSGs.

1.7.2. Through coordination with the operating command, identifies and documents total life-cycle intelligence support requirements for Operational Test and Evaluation (OT&E), and provides data to HQ 497 IG for inclusion in the ISP.

1.7.3. Ensures validated threat assessments are included in TEMPs and Operational Test Plans (OTPs).

## Chapter 2

### THREAT SUPPORT

#### *Section 2A— Threat Support for the Weapon Systems Acquisition Process*

##### **2.1. Threat Support Process.**

**2.1.1. Purpose of Threat Support.** Accurate and timely threat support is needed to assess operational needs, prioritize new programs, and continually refine a system during the acquisition process. Threat support includes threat assessments, data audits, and other threat production identified through the DoDIPP. For the purpose of this instruction, a data audit is the process of verifying that a computer model represents all threat data accurately. HQ 497 IG manages threat support to Air Force acquisition programs for HQ USAF/XOI.

##### **2.2. Assessing Threats.**

2.2.1. Threat assessments support the system's acquisition, planning, programming, and budgeting process. They assess the potential of hostile parties to neutralize or degrade the effectiveness of a specific US system. HQ 497 IG manages three categories of threat assessments in direct support of acquisition programs: STAs/STARs, TEDs, and intelligence reports.

##### **2.2.2. System Threat Assessment Reports and System Threat Assessments:**

2.2.2.1. The STAR is the authoritative threat reference for Acquisition Category I (ACAT I) programs. It:

2.2.2.1.1. Describes in a concise, issue-oriented manner the lethal and non-lethal threats against the proposed US system and the threat environment in which the system will operate.

2.2.2.1.2. Includes appendices (or separate supplements, if required) of detailed technical data, alternative scenarios (when applicable), and supporting analyses.

2.2.2.1.3. Presents a broad overview of the expected threat environment in which the US system will operate at Initial Operational Capability (IOC) (or an established baseline) and IOC/baseline +10 years.

2.2.2.2. The stand-alone STA is the authoritative threat reference for ACAT II programs. Although shorter in content than the STAR, it follows the same format (see **Attachment 2**).

2.2.2.3. The system threat assessment for ACAT III programs (and for ACAT II programs that do not require a stand-alone STA) is found in the threat section in the ORD. In some non-warfighting systems the threat may be listed as not applicable.

##### **2.2.3. Threat Environment Descriptions (TEDs):**

2.2.3.1. TEDs are baseline threat projections used to support:

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

2.2.3.1.2. US Air Force mission areas and other specialized tasks, as Air Force Manual (AFM) 1-1, Volumes 1 and 2, *Basic Aerospace Doctrine of the US Air Force*, specify.



2.2.3.1.3. Pre-Milestone I analyses.

2.2.3.1.4. Programs not subject to the milestone review process.

**NOTE:**

TEDs might also serve as basis from which to develop a STAR.

2.2.3.2. NAIC produces TEDs biennially (with page changes to maintain currency) under the DoDIPP.

**2.2.4. Intelligence Reports:**

2.2.4.1. Intelligence Reports are concise, issue-oriented memorandums that HQ 497 IG:

2.2.4.1.1. Prepares for HQ USAF/XOI signature to support Air Force Milestone decisions, summits, and other reviews of major programs.

2.2.4.1.2. Provides to the SAF/AQ and AF/XO staff prior to the review.

2.2.4.1.3. Uses to update Milestone decision principals on significant intelligence issues and to provide the HQ USAF/XOI position regarding threat to the program.

**2.2.5. Threat Assessments in Other Documents.** MNSs, ORDs, CONOPs, AoA study plans/reports, MAPs, and TEMPs all contain threat assessments. The threat data in these documents must be consistent with the STAR/STA, TED, or DIA-validated information (when the STAR, STA, or TED is not available).

**2.2.6. Other Threat Documents.** Air Force operating and implementing commands produce unique threat documents to satisfy specific customer requirements. The threat data in documents supporting acquisition programs must also be consistent with the STAR/STA, TED, or DIA-validated information.

2.2.6.1. Upon request, HQ 497 IG provides broad guidance, helps incorporate material from relevant documents that other units of the intelligence community have previously produced, and reviews, comments on, and recommends approval of these documents. NAIC/CC is the Air Force approval authority.

**2.3. Classifying Threat Assessments.**

2.3.1. Threat assessments must be at the lowest possible classification consistent with user needs and security considerations. For some programs, creators of threat assessment documents might need to prepare a separate annex at a higher classification level. **NOTE:** Special Access Programs might require special-access STARs or, in some cases, STARs with special-access annexes.

**Section 2B— Supporting Pre-Milestone 0**

**2.4. Developing the Threat Environment Description (TED)**

2.4.1. A TED is the baseline document providing threat projections to AF mission areas. HQ 497 IG assembles and chairs a TSG to determine the scope and provide other guidance to the TED author. TED TSGs will have similar composition to those for STARs (see 2.6.1.), with the difference being

that organizations concerned with requirements, technology development, and mission area planning will typically replace those supporting specific program development.

2.4.2. A TED will contain the following sections:

2.4.2.1. Mission Area Description.

2.4.2.2. The Operational Threat Environment (At current-to-10 years and 10-to-20 years).

2.4.2.3. Threat Systems (At current-to-10 years and 10-to-20 years).

## **2.5. Defining the Threat in Mission Needs Statements (MNSs)**

2.5.1. The operating command prepares the initial threat assessment using DIA-approved threat information (such as TEDs). This threat analysis describes:

2.5.1.1. The actual threat requiring an Air Force response if applicable.

2.5.1.2. The projected threat environment.

### ***Section 2C— Supporting Milestone 0 to Milestone I***

## **2.6. Developing Documentation.**

2.6.1. Threat Steering Group (TSG):

2.6.1.1. After Milestone 0, HQ 497 IG assembles a dedicated TSG to support each ACAT I and II 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. HQ 497 IG chairs the TSG, which includes representatives from:

2.6.1.1.1. HQ 497 IG.

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

2.6.1.1.3. Intelligence staff of the implementing and operating commands.

2.6.1.1.4. Staff of the Program Director

2.6.1.1.5. NAIC.

2.6.1.1.6. SAF/AQ.

2.6.1.1.7. DIA (for ACAT ID programs).

2.6.1.1.8. AFOTEC, when OT&E becomes an issue.

2.6.1.1.9. Operations and Requirements staff representatives from the implementing and operating commands, as appropriate.

2.6.1.1.10. Others as appropriate.

2.6.1.2. TSG responsibilities include:

2.6.1.2.1. Scheduling STAR, STA, TED production.

2.6.1.2.2. Establishing tasking.

- 2.6.1.2.3. Determining requirements for exceptional documents, such as STAR supplements.
- 2.6.1.2.4. Drafting a STAR or STA threat matrix according to the format in Table 2.1. This matrix is illustrative; TSGs may amend specific matrices to suit the needs of their customers and accurately reflect the contents of the STAR.
- 2.6.1.2.5. Preparing a STAR, STA, or TED outline.
- 2.6.1.2.6. Advising on Critical Intelligence Categories (CIC) development.
- 2.6.1.2.7. Conducting a line-by-line review and revision of the draft STAR to provide a "camera-ready" copy to NAIC/CC for approval. The final copy will be accompanied by a Staff Summary Sheet (SSS) reflecting TSG members' coordination for their organizations. The SSS will reflect all pertinent issues, to include potentially contentious positions, and will recommend approval of the document.
- 2.6.1.2.8. Advising on target set selection.
- 2.6.1.2.9. Recommending sources of digital data for analysis.
- 2.6.1.2.10. Identifying appropriate scenarios for AoA use and discussing shortfalls and options.
- 2.6.1.2.11. Developing a countermeasures matrix, if required.
- 2.6.1.2.12. Coordinating support provided by TSG members to Phase 0 activities, AoA, testing, and other efforts to ensure the program is provided complete and consistent threat information.

**Table 2.1. Sample Threat Matrix.**

<b>THREATS TO (US SYSTEM)</b>		
<b>THREAT</b>	<b>IOC</b>	<b>IOC+10 YEARS</b>
THREAT A	HIGH	HIGH
THREAT B	LOW	NIL
THREAT C	NIL	MEDIUM
THREAT D	MEDIUM	HIGH

**2.6.2. Supporting the AoA:**

- 2.6.2.1. The threat analysis portion of the AoA:
  - 2.6.2.1.1. References and is consistent with the STAR.
  - 2.6.2.1.2. Describes projected enemy forces and tactics, including potential countermeasures.
  - 2.6.2.1.3. Describes the strengths and weaknesses of potential adversaries in the designated mission area and shows how these might change over time.
- 2.6.2.2. Baseline scenarios used in the AoA must be based on the Defense Planning Guidance (DPG) Integrated Program Summary (IPS). The AoA may consider excursions from the DPG IPS when they would contribute to the analysis. In these cases, the AoA drafter must work closely with local intelligence staffs and HQ 497 IG to develop plausible scenarios to meet analytic needs.

2.6.2.3. HQ 497 IG reviews, comments on, and approves the intelligence-related sections of the AoA. As part of this review process, HQ 497 IG performs AoA data audits that:

2.6.2.3.1. Verify the accuracy of the threat data in the model.

2.6.2.3.2. Determine, to the extent possible, a level of confidence in the model.

### **2.6.3. Developing the ORD:**

2.6.3.1. The ORD threat assessment concisely describes the threat requiring an Air Force response and the projected threat environment in which the system will operate. The ORD may simply refer to that source, or provide a brief summary organized as shown below. If no STA/STAR exists, the threat section must address the elements below:

2.6.3.1.1. Operational threat environment.

2.6.3.1.2. System-specific threats at IOC and IOC + 10 years.

2.6.3.1.3. Targets (if applicable).

2.6.3.1.4. Reactive threats (i.e., threats expected to be deployed as a direct response to the proposed US system).

### **2.6.4. Developing the TEMP:**

2.6.4.1. The threat section of the TEMP:

2.6.4.1.1. References and is consistent with the STAR.

2.6.4.1.2. Briefly summarizes the threat environment described in the STAR. EXCEPTION: When the TEMP is required before formal program initiation (Milestone I) and no STAR/STA exists, the TEMP drafter will use threat information consistent with DIA- and HQ USAF/XOI-approved intelligence.

2.6.4.1.3. Identifies the type, number, availability, and fidelity requirements for all representations of the threat.

2.6.4.1.4. Compares the requirements for threat representations with available and projected assets and their capabilities.

2.6.4.1.5. Highlights major shortcomings.

2.6.4.2. HQ 497 IG reviews and approves the threat-related sections of the TEMP.

### **2.6.5. Developing the STAR/STA:**

2.6.5.1. A STAR or stand-alone STA is prepared for ACAT I/II programs, and others as required. HQ 497 IG, in conjunction with SAF/AQ, Air Force Materiel Command (AFMC), NAIC, the operating command, and DIA, determines within 30 days of the initial PMD date whether a TSG is required to support the program.

2.6.5.2. If a TSG is warranted, HQ 497 IG will notify appropriate organizations and convene an initial TSG meeting as soon as possible to review/coordinate post-Milestone 0 threat support and ensure timely STAR or STA production to support the Milestone I decision.

2.6.5.3. Based on the draft threat matrix, table of contents, schedule, and other TSG guidance, NAIC drafts the document and makes distribution to TSG members for review.

2.6.5.4. Thirty days (45 days if sister-service review is required) after draft STAR distribution, or as specified by the TSG, each TSG member will provide all other members with their substantive comments (comment exchange).

2.6.5.5. 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. HQ 497 IG will consolidate all comments.

2.6.5.6. The TSG will conduct an intrusive review to ensure the accuracy and quality of the final product. At the completion of the TSG meeting, each member will coordinate for their organization on a 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.

2.6.5.7. NAIC will staff the TSG recommendation, obtain AF approval from NAIC/CC, and publish/distribute final STARS in accordance with (IAW) the production schedule set at the original TSG meeting.

2.6.5.8. The preface of the final AF-approved product will contain the following statement: "This document has been reviewed by USAF/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."

2.6.5.9. NAIC submits AF-approved STARS for ACAT ID (and ACAT IC at Milestone I) programs 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 AF-approved STAR may warrant formal AF appeal. In these cases, the TSG chairman will consult with and represent the TSG membership in presenting/defending the AF position and working with DIA to resolve the issue.

2.6.5.10. After a STAR has been approved and validated, the implementing command will closely monitor the status of critical intelligence categories (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 US system specifications and characteristics.

2.6.5.11. 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.

2.6.5.12. Stand-alone STAs and STAR supplements follow the same review procedures as STARS.

2.6.5.13. On TSG recommendation, NAIC/CC grants Air Force approval of STARS (for ACAT I programs) and STAs (for ACAT II programs). In addition, AF-approved STARS for ACAT ID (and ACAT IC programs at Milestone I only) must be submitted to DIA for validation.

## **2.7. Additional Milestone 0 to Milestone I Support.**

2.7.1. In some instances, additional threat support is needed before formal program initiation (Milestone I). Intelligence provided before Milestone I must:

2.7.1.1. Be consistent with DIA- and HQ USAF/XOI-approved intelligence. Consultation with the TSG is highly recommended to ensure consistency with on-going analysis (for example, the initial STAR is drafted during this phase, but may not be available until the program nears Milestone I).

2.7.1.2. Contain a statement explaining the purpose of the document.

## ***Section 2D— Supporting Post-Milestone I***

### **2.8. Updating the AoA, ORD, and TEMP.**

2.8.1. The operating command updates threat data in the AoA and ORD for subsequent milestone reviews. The implementing command updates threat data in the TEMP.

### **2.9. Updating and Reviewing the STAR.**

2.9.1. About six weeks before the anniversary of a STAR, HQ 497 IG requests TSG members review and provide recommendations as to the need for an update of the STAR.

2.9.2. As TSG chair, HQ 497 IG consolidates recommendations on or before the anniversary date and determines whether the STAR requires an update.

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

2.9.4. If the STAR requires updating, HQ 497 IG will convene the TSG and follow the process outlined in paragraph 2.8.5.3 through 2.8.5.13. **NOTE:** A TSG meeting may also be required if it is unclear whether changes in a threat warrant an update to the STAR.

2.9.5. Threat assessments shall be maintained in a current and approved or validated status throughout the acquisition process in accordance with DoD 5000.2-R, Part 2, Paragraph 2.2.

## Chapter 3

### INTELLIGENCE SUPPORT PLAN PROCESS

#### 3.1. Intelligence Support Plan Process:

**3.1.1. Creating the Intelligence Support Plan (ISP).** The ISP generally represents the “I” in the C4I Support Plan (see DoD 5000.2-R, Paragraph 2.2.1). The ISP (see **Attachment 3**) is the authoritative reference for intelligence support to a specific weapon system, or class of systems, and documents intelligence support requirements, deficiencies, solutions, and costs. The ISP primarily supports the system program manager, the operating commands, and the intelligence community.

3.1.1.1. If an ISP is required, direction to develop it shall be included in the applicable PMD.

3.1.1.2. The ISP addresses requirements and implementation for weapon system life-cycle intelligence support related to:

- Collection management.
- Threat production.
- Collection, exploitation, and production of multi-disciplined, fused intelligence.
- Intelligence dissemination.
- Intelligence manpower and training.
- Targeting intelligence.

Mission Planning Support.

- Geospatial Information and Services (GI&S).
- Combat intelligence data.
- Modeling and simulation.
- Foreign materiel exploitation.
- Foreign military sales.

**3.1.2. Intelligence Counterpart Officers (ICOs).** The ICOs are the focal points for total life-cycle intelligence support to a specific weapon system, or class of systems, for HQ USAF, operating commands, and the implementing command.

3.1.2.1. The ICOs develop and coordinate system-specific ISPs to document and monitor implementation of intelligence support requirements.

3.1.2.1.1. The HQ 497 IG ICO develops and produces the ISP, while the operating and implementing command ICOs ensure the weapon system intelligence requirements identified at their respective commands are addressed in the document. The implementing command ICO also ensures system-unique intelligence costs in the ISP are reflected in program planning and costing documentation.

3.1.2.1.2. The HQ 497 IG ICO develops the ISP in close cooperation with the operating and implementing command ICOs, as well as the test and training communities.

**3.1.3. The Intelligence Support Working Group (ISWG).** The ISWG helps the HQ 497 IG ICO develop the ISP, and provides an official forum for monitoring ISP implementation and revision throughout the weapon system's life cycle. The ISWG includes five major interest groups:

- System developers and supporters.
- System testers.
- Operational users.
- Supporting intelligence providers.
- Those responsible for intelligence training.

3.1.3.1. The HQ 497 IG ICO chairs the ISWG, and coordinates the ISWG agenda with the operating and implementing command ICOs.

**3.1.4. Approving the ISP.** The HQ 497 IG ICO submits the draft ISP for comment to selected operating command, implementing command, and HQ USAF staff elements. The final document, after incorporation of comments, is re-staffed for coordination and approval.

3.1.4.1. Operating command ICOs submit the draft ISP for comment to the Director of Operations (DO), Director of Intelligence (IN), and Director of Requirements (DR) staffs at the operating command. Implementing command ICOs submit the draft ISP for comment to the System Program Director (SPD) and Director of Intelligence (DI) staffs at the implementing command. HQ 497 IG ICOs submit the draft ISP for comment to the HQ USAF/XOI, HQ USAF/XOR and appropriate SAF/AQ Program Executive Officer (PEO) staffs.

3.1.4.2. After resolution of any comments, the operating command ICO will obtain DO and DR coordination. Then, the operating command IN will validate the final ISP. At the same time the implementing command ICO will obtain SPO Director coordination followed by DI validation. Once the ISP is validated by the operating and implementing commands, the HQ 497 IG ICO obtains HQ USAF/XOR and SAF/AQ PEO coordination and HQ USAF/XOI approval.

**3.1.5. 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.

3.1.5.1. 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.

## **3.2. Supporting Milestone 0 to Milestone I.**

3.2.1. Appointed ICOs, with functional experts from other commands and organizations, form an ISWG for directed programs immediately after Milestone 0. The ISWG helps the HQ 497 IG ICO ensure that all intelligence support requirements are identified and addressed, and identifies proposed solutions and alternatives addressing each requirement.

3.2.2. Total life-cycle intelligence support cost data should be used to develop the ISP, and as input to the AoA and the program's overall projected life cycle.

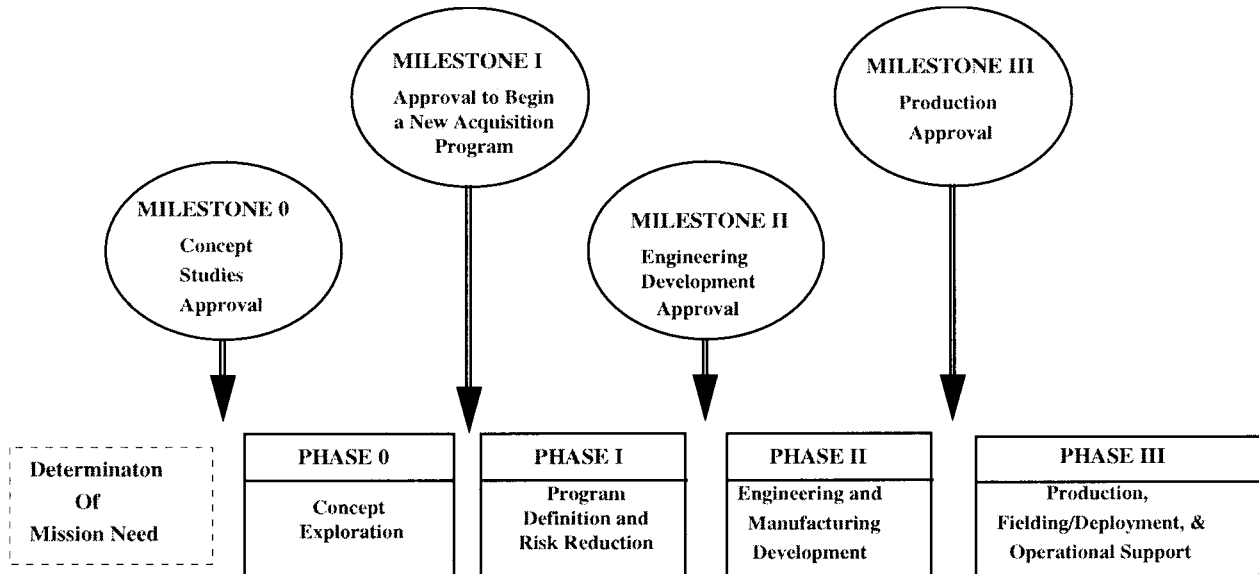
## **3.3. Supporting Post-Milestone I:**



3.3.1. The ISWG and ICOs refine requirements and monitor ISP progress throughout the weapon system's life cycle.

3.3.2. ICOs participate in IPTs and other program management forums to monitor overall intelligence support and ensure that ISP requirements are satisfied.

**Figure 3.1. Acquisition Milestones and Phases. (AFI 10-601)**



JOHN P. JUMPER. Lt Gen, USAF  
DCS, Air and Space Operations

## Attachment 1

### GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

#### *References*

DIAR 55-3, *Intelligence Support for Defense Acquisition Programs*, March 30, 1992

DoD 5000.2-R *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) Acquisition Programs*, March 15 1996 with Change 1.

AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures*

AFI 14-206, *Modeling and Simulation*

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

AFPD 14-1, *Air Force Intelligence Planning and Operations*

AFPD 62-2, *System Survivability*

AFPD 63-1, *Acquisition System*

AFPD 99-1, *Test and Evaluation Process*

#### *Abbreviations and Acronyms*

**ACAT**—Acquisition Category

**ACAT I**—Major Defense Acquisition Programs

**ACAT IA**—Major Automated Intelligence Systems Acquisition Program

**ACAT IAC**—MDA is DoD Component Chief Info Officer. (“C” is for component)

**ACAT IAM**—MDA is OSD, Chief Info Officer. (“M” refers to Major Automated Information System Acquisition Program Review Council)

**ACAT IC**—MDA is the DoD Component head or CAE. (“C” is for component)

**ACAT ID**—MDA is USD(A&T). (“D” refers to the Department, as in DoD)

**ACTD**—Advanced Concept Technology Demonstration

**AFMC**—Air Force Materiel Command

**AFOTEC**—Air Force Operational Test & Evaluation Center

**AFPD**—Air Force Policy Directive

**AoA**—Analysis of Alternatives

**APB**—Acquisition Program Baseline

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

**CAE**—Component (Service) Acquisition Executive

**CIC**—Critical Intelligence Categories

**CONOPs**—Concept of Operations

**DAB**—Defense Acquisition Board  
**DIA**—Defense Intelligence Agency  
**DoDIPP**—Department of Defense Intelligence Production Program  
**DPG**—Defense Planning Guidance  
**GI&S**—Geospatial Information and Services (Formerly Mapping Charting & Geodesy)  
**ICO**—Intelligence Counterpart Officer  
**IOC**—Initial Operational Capability  
**IPS**—Integrated Program Summary  
**ISP**—Intelligence Support Plan  
**I-MSP**—Intelligence Mission Support Plan  
**IRM**—Intelligence Requirements Matrix  
**ISWG**—Intelligence Support Working Group  
**IWSMP**—Integrated Weapon System Master Plan  
**MAP**—Mission Area Plan  
**MDA**—Milestone Decision Authority  
**MNS**—Mission Needs Statement  
**M&S**—Modeling and Simulation  
**NAIC**—National Air Intelligence Center  
**OPR**—Office of Primary Responsibility  
**ORD**—Operational Requirements Document  
**OT&E**—Operational Test and Evaluation  
**OTP**—Operational Test Plan  
**PMD**—Program Management Directive  
**PEO**—Program Executive Officer  
**PR**—Production Requirement  
**RDT&E**—Research, Development, Test and Evaluation  
**SAMP**—Single Acquisition Management Plan  
**SII**—Statement of Intelligence Interest  
**SPO**—System Program Office  
**STA**—System Threat Assessment  
**STAR**—System Threat Assessment Report  
**USDA&T**—Undersecretary of Defense for Acquisition and Technology

**TED**—Threat Environment Description  
**TEMP**—Test and Evaluation Master Plan  
**TPIPT**—Technical Planning Integrated Product Team  
**TSG**—Threat Steering Group  
**TWG**—Threat Working Group

### *Terms*

**Concept Studies**—Studies conducted to evaluate and define the feasibility of alternative concepts. They assess the relative merits of alternative concepts at the Milestone I decision point. (AFI 10-601)

**Analysis of Alternatives (AoA)**—An analysis of the estimated costs and operational effectiveness of alternative materiel systems to meet a mission need and the associated program for acquiring each alternative. (DoD Instruction 5000.2-R)

**Critical Intelligence Categories (CIC)**—Threat capabilities or thresholds set by the program, changes to which could critically impact the effectiveness and survivability of the proposed system.

**Defense Acquisition Board (DAB)**—The Department of Defense corporate body for system acquisition that advises and assists the Secretary of Defense. (DoD Directive 5000.49)

**Defense Planning Guidance (DPG)**—Secretary of Defense's policy and fiscal guidance upon which the military services and defense agencies base their programs and budgets. The DPG provides a broad overview of the expected threat environment and potential adversaries. To establish a thread of continuity in Air Force STARS, DPG scenarios will form the basis for the operation threat environments in STARS.

**Implementing Command**—The command or agency that the Air Force Acquisition Executive designates to manage an acquisition program (usually AFMC). The intelligence support to the manager of an acquisition program usually resides with the Product Center Directorate of Intelligence. For this AFI the roles and responsibilities of the implementing command reside with the organizations identified by the program director as the focal point for intelligence supporting for that specific program.

**Intelligence Support Plan (ISP)**—The authoritative reference document for identifying, planning, and monitoring implementation of intelligence infrastructure requirements for a weapon system from need definition through system retirement. (AFI 10-601)

**Milestones (0 through III)**—Major management decision points in the overall acquisition decision process of a Department of Defense (DoD) system that require Office of the Secretary of Defense and/or DoD component program review. Milestones include both the Defense Acquisition Board and DoD component-equivalent program reviews: (AFI 10-601)

- 0 - Approval to Conduct Concept Studies
- I - Approval to Begin a New Acquisition Program
- II - Approval to Enter Engineering and Manufacturing Development
- III - Production or Fielding/Deployment Approval

**Mission Needs Statement (MNS)**—A document prepared to identify a requirement for a material solution to satisfy a mission deficiency. (AFI 10-601)

**Operating Command**—The command primarily operating a system, subsystem, or item of equipment. Generally applies to those operational commands or organizations that Headquarters US Air Force designates to conduct or participate in operations or operational testing. Interchangeable with the term "Using Command." (AFM 11-1)

**Operational Requirements Document (ORD)**—A document prepared by the respective using command that describes pertinent quantitative and qualitative performance, operation, and support parameters, characteristics, and requirements for a specific candidate weapon system. (AFI 10-601)

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

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

## Attachment 2

### SYSTEM THREAT ASSESSMENT REPORT (STAR) FORMAT

**A2.1. Preface.** A formatted page outlining the scope of the STAR; indentifying the offices involved in preparation, the responsible program office, the information cutoff date, the milestone that it supports; including the Air Force approval statement, and (if applicable) the DIA validation statement.

**A2.2. Table of Contents and List of Figures and Illustrations.**

**A2.3. Executive Summary.** The executive summary consists of three subsections:

- US Systems Technical and Mission Description (with system IOC).
- Key Threat Judgments.
- A Threat Matrix.

In updated STARs, it specifically identifies significant threat changes that have been noted since the last STAR.

**A2.4. Section I. Introduction.** A brief opening statement that includes a short description of the mission need for the system.

**A2.5. Section II. US System Description.** A summary that includes physical and technical characteristics, the IOC, mission, operational concepts, and employment considerations that can reasonably be expected to impact on, or be impacted by, the threat. The program office provides US System Description information. The operating command provides mission and concept of operations information.

**A2.6. Section III. Operational Threat Environment.** An overview of the operational, physical, and technological threat environment in which the system is expected to operate during its lifetime. Areas covered include:

- Threat force levels and enemy doctrine.
- Strategy.
- Tactics affecting system mission and operations.

Countries covered in this section are based on the DPG scenarios.

**A2.7. Section IV. Targets (if applicable).** An analysis of the capabilities and signatures of the full range of targets (such as vehicles, ships, aircraft, or silos) the US system is designed to engage. Target employment, characteristics, command and control, and quantity are included. Types and density of targets may also be covered along with such common parameters as the thickness and types of armor the system must defeat.

**A2.8. Section V. System Specific Threat.** An assessment of the threat weapon systems that are directly relevant to the mission and performance of the US system throughout its operational lifetime. This section consists of two subsections: the threat at IOC of the US system and the threat at IOC plus 10 years. Each subsection assesses the threat using three criteria:

- Threat system technical capabilities.
- Magnitude of the threat (projected force level).
- Threat integration--a combined evaluation of the threat to the US system when a potential adversary's employment doctrine, force levels, and systems are considered together.

**A2.9. Section VI. Reactive Threat.** Summarizes both the likely reactive threat and the technologically feasible threat. The likely reactive threat describes the system or capabilities that adversaries most typically develop and deploy during a specified period. The technologically feasible threat offers alternatives if the adversary's requirements differ from those that intelligence sources have generated. Although not constrained by intelligence projections, the technologically feasible threat is consistent with an adversary's technology, economy, and production capabilities.

**A2.10. Appendices.** Appendix 1 lists the CICs and associated intelligence Production Requirements (PRs). CICs are developed for the initial STAR. Updates to the STAR focus on relevant intelligence that would indicate a threshold indicator has occurred. The CIC threat status is also provided along with each CIC. The system program office and the originating office of the STAR work together to develop CICs. A new intelligence PR is developed for each CIC in the STAR.

**A2.11. References.** A list that contains sources used in the preparation of the document or that provide additional detail on threat topics.

## Attachment 3

### INTELLIGENCE SUPPORT PLAN (ISP) FORMAT

**A3.1. Title Page.** The title page identifies the weapon system the ISP is supporting, overall classification of the document, the responsible operating and implementing command, and date of publication.

**A3.2. Table of Contents and List of Figures and Illustrations.**

**A3.3. Executive Summary.** A brief stand-alone section which should capture the major issues and shortfalls described in the ISP. It should provide a quick overview of the ISP program, the weapon system program, and the key intelligence requirements and implementation plans.

**A3.4. Chapter 1. Introduction.** Since the ISP is still a relatively new concept, this section should discuss the purpose of the ISP and describe total life-cycle intelligence support to the acquisition process. The following subsections should be included:

- Overview. Explains the role of the ISP in supporting a particular weapon system.
- Authority. Lists the directives that govern the ISP.
- Purpose. Explains the ISP process and what it will accomplish.
- Scope. Describes the various total life-cycle intelligence support areas addressed by the ISP.
- How to Use. Briefly describes how the ISP can be used, and by whom.

**A3.5. Chapter 2. Weapon System Description.** This section provides a description of the weapon system sufficient to understand the derived intelligence requirements. It also includes a description of the acquisition strategy, acquisition-related intelligence needs, and the Strategy-to-Task analysis performed to derive the intelligence requirements. The following subsections should be included:

- Weapon System (overview; roles and missions; and the operational baseline, including employment options, the concept of operations, and the operating environment).
- Acquisition Strategy (overview; program schedule; weapon system technologies; developmental and operational testing; training; and any program peculiarities, such as joint requirements, foreign military sales, and advanced concept technology demonstrations).
- Acquisition Related Intelligence Needs (e.g., threat parametric data, modeling and simulation support, test and evaluation needs).
- Strategy-to-Task Analysis (a derivation of the intelligence needs from the operational requirements).

**A3.6. Chapter 3. Intelligence Support Requirements.** This is the heart of the ISP. It needs to capture *detailed* intelligence requirements and the *detailed* plans to satisfy those requirements, to enable the ISP to serve as the *authoritative* reference describing total life-cycle intelligence support for the weapon system. Acquisition Support Requirements (AQ), Testing Support Requirements (TE), Training Support Requirements (TN), and Operations Support Requirements (OP) must all be addressed. The following subsections should be included:



- Intelligence Support Requirements Matrix (overview, intelligence requirement, brief description, status).
- Intelligence Support Requirements. Includes a detailed description of each requirement (e.g., target model validation, digital imagery exploitation support, mission planning, targeting support for testing, etc.), a reference to the source of the requirement in Section 2, detailed satisfaction criteria, status, and a detailed infrastructure solution, including the OPR and suspense.

**A3.7. Chapter 4. Life-cycle Intelligence Infrastructure Cost.** Contains estimated potential costs associated with fulfilling the intelligence requirements (*e.g.*, equipment hardware and software, manpower, training, and facilities).

**A3.8. Appendices/Annexes.** Appendices include an Intelligence Requirements Matrix (IRM), a glossary of acronyms and terms, the Strategy-to-Task analysis, and other information as required. Some programs may require an SCI or SAR annex to address certain requirements, which would follow the format of Chapters 2, 3, and 4 above.