DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES SPACE FORCE
WASHINGTON DC

SPFI14-411_SPFGM2026-01
16 April 2026

MEMORANDUM FOR DISTRIBUTION C
FLDCOMs/FOAs/DRUs

FROM: USSF/S2
1600 Air Force Pentagon
Washington, DC 20330-1040

SUBJECT: Space Force Guidance Memorandum to SPFI 14-411 Space Force Acquisition Intelligence

By order of the Secretary of the Air Force, this Guidance Memorandum (GM) immediately implements changes to Space Force Instruction (SPFI) 14-411 Space Force Acquisition Intelligence, paragraph 2.1.7., which defines National Space Intelligence Center's (NSIC) roles and responsibilities with the Space Force acquisition intelligence enterprise. This GM fully implements Production Planning, Prioritization, and Resourcing Framework (P3RF) as an NSIC program and directs NSIC to fully execute P3RF as outlined in Department of the Air Force (DAF) DAF Memorandum of Understanding DAFS2-2025181-001. Additionally, this GM implements changes to SPFI 14-411 attachment 2 Threat Intelligence Certification. This GM aligns SPFI 14-411 Intelligence Supportability procedures with Space Force's emerging requirement validation and acquisition process driven by Department of War's acquisition reform. Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other United States Space Force (USSF) publications, the information herein prevails IAW DAFI 90-160.

NSIC will fully implement P3RF as an NSIC program, which includes assigning a P3RF program manager and executing P3RF funds from 3210 NSIC PEC until P3RF PEC is fully funded in FY 27.

As outlined in SPFI 14-411, Attachment 5, the Space Threat Steering Group (STSG) will be responsible for managing the Space Force Intelligence Supportability and Certification processes. Attachment 1 of the GM replaces Attachment 2 in SPFI 14-411 and provides a process to ensure intelligence sufficiency for all Space Force requirements. The STSG, following Attachment 1 of the GM, will develop an S2 signed memorandum of intelligence sufficiency for all Space Force requirements that will be entered into KM/DS. Additionally, STSG will develop, as outlined SPFI 14-411, and Attachment 1 of the GM, an Intelligence Supportability plan for each validated requirement delivered to SAF/SQ. All Intelligence Supportability plans will be certified by S2.

Ensure all records generated because of processes prescribed in this publication adhere to DAFI 33-322, Records Management and Information Governance Program, and are disposed in accordance with the Department of the Air Force Records Disposition Schedule, located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) using the DAF Form 847, Recommendation for Change of Publication; route DAF Forms 847 from the field through the appropriate functional chain of command. The SF/S2 is the OPR for Acquisition Intelligence.

This memorandum becomes void after one year has elapsed from the date of this memorandum, or upon publishing of an interim change or rewrite of any affected publication, whichever is earlier.

Please address questions to the USSF/S2 leads for this effort, Mr. John Eaves (john.eaves.3@us.af.mil) and Mr. Michael Scopel (michael.scopel.1@us.af.mil).

BRIAN D. SIDARI, Maj Gen, USSF
Deputy Chief of Space Operations for
Intelligence

Attachment:
1. Space Force Intelligence Supportability Certification

cc:
ORG/SYM

Attachment 1

SPACE FORCE THREAT APPROVAL AND INTELLIGENCE SUPPORTABILITY AND CERTIFICATION

A1. Applicability. Intelligence Certification is required by Joint Service guidance, and SPFI 14-411 Space Acquisition Intelligence. Intelligence Supportability and Certification is required for all Space Force requirements regardless of acquisition pathway, and includes requirements protected by ACCM or SAP/SAR designation.

A1.1. Threat Approval & Intelligence Supportability. Intelligence supportability identifies and assesses all intelligence support requirements, including anticipated shortfalls, throughout the capability solution's lifecycle. Intelligence supportability categories included, but not limited to:

A1.1.1. Intelligence Resources (Hardware/Software/Connectivity), including manpower, funding, and training
A1.1.2. Intelligence Interoperability
A1.1.3. Intelligence Modeling and Simulation, including Intelligence Mission Data (IMD)
A1.1.4. Counterintelligence and Security

A1.2. Intelligence Certification ensures that capabilities are developed in context of applicable adversary threat and that intelligence support requirements, and shortfalls, have been assessed for completeness and supportability.

A1.3. Space Force HQSF/S2 will provide two intelligence certifications. The first certification addresses Mission Area Requirement Document (MARD) and DOTmLPF-P Change Recommendation (DCR) while the second certification addresses system requirement documents. The requirement intelligence certification will be submitted when the validated requirement document is entered into KM/DS. The second intelligence certification will be issued prior to the acquisition strategy document being certified.

A2. Requirement Intelligence Certification. Requirement intelligence certification is intended to certify that threat intelligence was used to inform the mission area requirement and that the Defense Intelligence Enterprise (DIE)/Intelligence Community (IC) can support the mission area requirement.

A2.1. Threat. The threat laydown that is driving the requirement should be assessed at projected IOC and through the anticipated lifecycle of the mission area requirement.

A2.2 Emerging and disruptive technologies. To reduce technological surprise during the requirements lifecycle, sponsors should identify those emerging and disruptive technologies that, if fielded, would significantly degrade the requirement.

A2.3. IC Data. Sponsor should identify any IC data requirements.

A2.4. Intelligence supportability for requirement validation. HQSF/S5R will address the potential intelligence support requirements to support requirement validation.

A3**.** Acquisition Intelligence Certification. Acquisition intelligence certification is to ensure that all available threat intelligence is integrated into every Space Force acquisition strategy. Additionally, acquisition intelligence certification ensures sponsors have access to all required IC data and that capabilities are supported by approved Capability Intelligence Parameters (CIPs) as directed by Joint Staff guidance.

A3.1 Threat. Consistent with Title 10 § 4211, acquisition strategies will integrate current intelligence assessments into the acquisition process. Threat-related content in capability requirements documents provide the analytic rationale that threat-sensitive capability performance requirements consider adversary developments in military capabilities and intent to challenge U.S. warfighting.

A3.2. Intelligence Supportability. Prior to certification of an acquisition strategy, the sponsors will address each of the intelligence support requirements, summarizing dependencies to documented capability performance requirements, status of submitted intelligence supportability artifacts, and assessed impacts to Defense Intelligence Enterprise Manager and NRO support roles.

A4. Once threat intelligence and intelligence supportability requirements are satisfied and packaged into an Intelligence Support Plan (ISP), HQSF/S2R will staff the intelligence sport plan to HQSF/S2 for certification.

A4.1. SAF/SQ shall ensure program sponsors engage with HQSF/S2 early and continuously throughout the acquisition lifecycle to facilitate the collaborative development of the ISP. This proactive integration ensures all threat and supportability requirements are fully aligned with S2's criteria prior to the formal request for certification, preventing delays and rework.

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

SPACE FORCE INSTRUCTION 14-411

13 FEBRUARY 2026

Intelligence

SPACE FORCE ACQUISITION
INTELLIGENCE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SF/S2R

Certified by: SF/S2
(Maj Gen Brian Sidari)
Pages: 35

This publication is consistent with Headquarters Air Force Mission Directive (HAFMD) 2-4, *Deputy Chief of Space Operations for Intelligence*. It provides guidance and procedures for the acquisition community throughout the Space Force. This publication applies to all civilian employees and uniformed members of the United States Space Force and those with a contractual obligation to abide by the terms of DAF issuances, except where otherwise noted. This publication does not apply to the United States Air Force except for Air Force Reserve and Air National Guard units performing space operations and select career fields assigned or attached to Space Force units or directly supporting Space Force activities. USSF acquisition systems processing both Special Access Program (SAP) and Sensitive Compartmented Information (SCI) will adhere to the more restrictive policies of each of the respective SAP and SCI communities. This publication may not be supplemented. Refer recommended changes and questions about this publication to the OPR listed above using the DAF Form 847, *Recommendation for Change of Product*; route DAF Forms 847 from the field through the appropriate chain of command. The authorities to waive delta/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See DAF Manual (DAFMAN) 90-161, *Publishing Processes and Procedures* for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. For a more complete list of all references and

documents that acquisition intelligence uses to complete the mission, see **Attachment 1** of this publication.

Chapter 1

OVERVIEW

1.1. Overview. This document codifies how Space Force will organize and execute acquisition intelligence to support USSF capability development, acquisitions, and Test & Evaluation (Developmental Testing (DT), Operational Testing (OT), Integrated Testing (IT)). Furthermore, this instruction ensures integration of threat intelligence, to the greatest extent possible, throughout a capability's lifecycle. Additionally, this instruction addresses USSF acquisition intelligence roles and responsibilities for specific organizations. It applies to all USSF entities that create or integrate intelligence into capability development, test, R&D, and the acquisition lifecycle. It applies regardless of entity type, primary function, authority, or funding source. Finally, this instruction also applies to all development and acquisition pathways and processes, such as newly developed USSF service-specific requirements processes. Programs already in the Joint Capabilities Integration and Development System (JCIDS) will continue based on the JCS "Terminate and Transition Plan for JCIDS Memo" dated 21 Aug. 2025 para. 3a. and 3b. Any new and potential follow-on processes, Major Capability Acquisition, Middle Tier of Acquisition, Urgent Capability Acquisition, Software Acquisition Programs, Foreign Military Sales, and Special Access Programs will align with JCIDS replacement procedures IAW the above stated memo.

Chapter 2

PROGRAM MANAGEMENT ROLES AND RESPONSIBILITIES

2.1. Space Force Acquisition Intelligence Core Roles and Responsibilities.

2.1.1. SF/S5R. SF/S5R designated as the DoD Integrator for Joint Space Requirements.

2.1.1.1. Manage the development of operational capability requirements.

2.1.1.2. Include SF/S2R in all applicable operational capability requirements development forums, e.g. Solution Pathway Reviews, Document Writing Teams.

2.1.2. **SF/S2R.** Ensure USSF acquisition intelligence policy, instructions, and procedures adapt to an increasingly agile acquisition trade-space, ensure all statutory and regulatory threat intelligence requirements are met, and normalize USSF threat intelligence processes across the USSF acquisition enterprise and throughout the USSF acquisition lifecycle. Work with sponsors and acquisition intelligence analysts (AIAs) to ensure all USSF acquisitions programs receive proper intelligence certification aligned with prioritized Key Operational Problems (KOPs) identified by the Requirements and Resourcing Alignment Board (RRAB) or as outlined in legacy JCIDS Manual IAW JCS Memo dated 21 Aug. 2025. **(T-0) See Attachment 2.**

2.1.2.1. Validate intelligence requirements for USSF capabilities and advocate for intelligence resourcing of USSF ISR capabilities and USSF acquisition intelligence activities.

2.1.2.2. Collaborate with the Defense Intelligence Enterprise (DIE) and across DAF staff to establish policies for integrating USSF acquisition threat models into DAF and DoD modeling and simulation activities.

2.1.2.3. In collaboration with SF S5/8, review and validate USSF intelligence requirements within the USSF acquisition process. JCIDS processing will only apply to those programs IAW JCS Memo dated 21 Aug. 2025 Para 3a. and 3b. to ensure adversary threats are included throughout the legacy requirements processes.

2.1.2.4. Lead coordination with Assistant Secretary of the Air Force for Space Acquisition and Integration (SAF/SQ), United States Air Force, Test & Evaluation (AF/TE), Space Training and Readiness Command S2 (STARCOM/S2), Combat Forces Command S2 (CFC/S2) and Space Systems Command S2 (SSC/S2) to ensure standardized intelligence support to acquisition, testing, and modeling & simulation activities.

2.1.2.5. Establish threat intelligence integration monitoring and improvement processes to ensure widest utilization of intelligence data.

2.1.3. **Program Executive Officer (PEO).** PEOs and PMs in collaboration with AIAs, define the program of record's intelligence needs in accordance with the appropriate acquisition pathway and regulatory guidance. Ensure programs are fully supported and threat-informed with authoritative intelligence (in accordance with ICD 501, Discovery, and Dissemination or Retrieval of Information Within the Intelligence Community).

2.1.3.1. AIAs aligned to PEO unit manning document (UMD) will execute roles and responsibilities as outlined in **paragraph 2.1.5**. **(T-0)**

2.1.3.2. Program Manager (PM). The PM will design, build, test, deliver, and continuously update systems to consider evolving adversary threats and address acquisition security considerations in accordance with DAFI 63-101/20-101. Additionally, the PM will document a strategy assessing threat progression and ensure intelligence is integrated throughout the entirety of the acquisition lifecycle as outlined in DoDI 5000.85. **(T-0)**

2.1.3.2.1. Collaborate with AIAs, ensure an acquisition program's modular open systems approach and digital threads as outlined in DoDI 5000.86, DoDI 5000.97, and DAFI 63-101/20-101 are tailored in response to threat intelligence inputs. Provide AIAs analytical results generated from Modeling Simulation and Analysis (MS&A) to enable improved tailored intelligence support. **(T-0)**

2.1.3.2.2. Ensure new/changing efforts are appropriately identified to AIAs. **(T-0)**

2.1.3.2.3. Technology Targeting Risk Assessment (TTRA). Along with AIAs, ensure the Air Force Office of Special Investigation (AFOSI), completes a TTRA for each USSF acquisition program. **(T-0)**

2.1.3.2.4. Test and Evaluation Master Plan (TEMP)/Test and Evaluation Strategy (T&E Strategy). PM, collaborating with AIAs will specify the threats required for test. AIAs will coordinate with the National Space Intelligence Center (NSIC) to ensure that identified threats have the appropriate threat model available for test activities. **(T-1)**

2.1.3.2.5. Provide relevant programmatic reference material to support AIAs. **(T-0)**

2.1.3.2.6. Collaborate with AIAs, to prepare a risk management plan that documents the program's use of standard risk management processes. **(T-0)**

2.1.3.2.7. Intelligence Support Plan and Risk Management Plan. Complete Intelligence Support Plan (**Attachment 3**) and its associated Risk Management Plan (**Attachment 4**) for all acquisition programs that are transitioned to CFC. **(T-1)**

2.1.4. **Senior Intelligence Officer (SIO).** The SIO serves as the intelligence advisor to the FLDCOM Commander and is responsible for the execution of the intelligence activities within the Commander's organization to include all subordinate/lateral units. The SIO or delegate will:

2.1.4.1. Ensure the training, resourcing, and placement of AIAs as directed by DAFI 63-101/20-101 in support of PM managed activities IAW DoDI 5000.86.

2.1.4.2. Ensure personnel in the command who conduct intelligence or intelligence-related activities manage an intelligence oversight program IAW DoDD 5148.13 and DAFI 14-404.

2.1.4.3. Ensure the technical ability of the AIAs and the intelligence support provided to all USSF PEOs is IAW DoDI 5000.86.

2.1.4.4. Assess, manage and annually collect intelligence data requirements. Submit new or unmet requirements to SF/S2R during the 2nd quarter of the current fiscal year to identify any emerging intelligence data gaps or unmet production requirements. **(T-0)**

2.1.4.5. Annually, initiate a data call for all USSF threat modeling requirements. Review, prioritize, and submit threat model requirements to NSIC and SF/S2R. Prior year

production requirements will be weighed against existing production gaps and new production requirements will be highlighted. **(T-2)**

2.1.4.6. Makes final adjudication of Intelligence Sensitivity Determination (ISD), approves and signs ISD MFR.

2.1.4.7. Final signatory for certification of regulatory artifacts, threat prioritizations, and Space Threat Steering Group byproducts.

2.1.5. **SSC Intelligence Directorate (SSC/S2).** Intelligence focal point for acquisition life cycle management and direct liaison with the DIE and Intelligence Community (IC) to tailor threat intelligence analysis to USSF acquisition program and USSF lifecycle activities. SSC/S2 provides relevant threat support for program protection planning, anti-tamper measures, Supply Chain Risk Management, TTRAs, and Test and Evaluation Master Plans. In coordination with the PM the AIA is responsible for conducting an ISD to determine the risk of not integrating intelligence into the acquisition program under review. S2/AIAs, in accordance with DoDI 5000.86 and DAFI 63-101/20-101 will:

2.1.5.1. Provide advice and counsel on intelligence, surveillance, and reconnaissance (ISR) matters and assists the program in being fully threat informed with authoritative intelligence. **(T-0)**

2.1.5.2. Partner with PM to ensure risk associated with intelligence-sensitive programs are considered as part of a program's overall risk assessment that align with program timelines. **(T-0)**

2.1.5.3. Partner with PM to develop a tailored acquisition intelligence strategy that at a minimum includes characterization of the threat, identification of intelligence supportability plans, risks, and cost drivers, and residual risk to inform stakeholders. **(T-0)**

2.1.5.4. Provide tailored threat intelligence (e.g., briefing, planning, risk analysis, validated on-line lifecycle threats (VOLT), etc.) to include threat data tailored to digital threads and digital engineering tools. **(T-0)**

2.1.5.5. Conduct Intelligence Supportability Analysis (ISA). **(T-2)**

2.1.5.6. Conduct Intelligence Health Assessment (IHA). **(T-2)**

2.1.5.7. Work with PM to complete a Lifecycle Mission Data Plan (LMDP) for every space acquisition program. Intelligence data gaps, threat model production shortfalls, and intelligence related costs that have not previously been documented need to be sent to SF/S2R. SSC/S2 and AIAs will collect annual intelligence data requirements and submit those requirements to NSIC. **(T-1)**

2.1.5.8. Work with NSIC to assess all programs, plus network edge environments, to determine if an ACTA is required for every new acquisition program. **(T-1)**

2.1.6. **Space Rapid Capabilities Office (SpRCO) Embedded Acquisition Intelligence Analysts.**

2.1.6.1. Lead intelligence support and direct liaison with DIE and IC to tailor threat intelligence analysis and threat intelligence assessments support to Military Service-led rapid acquisition programs. (*tailoring – see* **Attachment 1**) AIAs take direction from PMs but should proactively track threat progression and threat risk to assigned programs; active

tracking of threat should lead to proactive engagement with the PM. SpRCO AIAs will work with DIE/IC to ensure intelligence products are produced in a digital format that is compatible with Model-Based Systems Engineering (MBSE) and USSF Digital Engineering (DE) ecosystem if appropriate for rapid program timelines. SpRCO AIAs will work with the program office and NSIC to complete the following:

2.1.6.1.1. Tailored VOLT and Foundation Threat Intelligence. SpRCO AIAs will request a tailored threat assessment from NSIC for all new acquisition programs ahead of or to support program milestones to meet rapid acquisition program intel needs. **(T-2)**

2.1.6.1.2. Intelligence Sensitivity Determination (ISD). SpRCO AIAs, working with PMs, are responsible for conducting an ISD to determine the risk of not integrating intelligence into the acquisition program under review, and whether the risk is acceptable or unacceptable. This determination is based in part on an assessment of competing demands for scarce intelligence resources being consumed by current DoD or other national security priorities. An acquisition program is intelligence-sensitive if at any point in its life cycle: 1) it produces, consumes, processes, or handles intelligence information; or 2) it requires intelligence-related doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P), or intelligence-related planning and direction, collection, processing, analysis and production, and dissemination (PCPAD) intelligence support; or 3) it requires threat support to make programmatic decisions. The ISD aids early development of rough-order-of-magnitude estimates for intelligence support to, and risk management of, the acquisition program. Any SpRCO program deemed to be intelligence-sensitive will require the development of a SpRCO Rapid Threat Support Plan to document intel needs and will be updated on a regular basis as required. **(T-2)**

2.1.6.1.3. SpRCO Rapid Threat Support Plan. SpRCO AIAs will complete the Threat Support Plan for any SpRCO program deemed to be intelligence-sensitive. Threat Support Plans will be updated as required to account for new intelligence requirements as a program progresses through to fielding of a first-of-kind capability. Identified deficiencies must be briefed to the impacted program manager and program deficiencies must be sent to SF/S2R. **(T-1)**

2.1.6.1.4. Adversary Cyber Threat Assessment (ACTA). SpRCO AIAs, working with program managers, will assess all SpRCO programs' network edge environments to determine if an ACTA is required for each new acquisition program. **(T-1)**

2.1.6.1.5. Technology Targeting Risk Assessment. SpRCO AIAs, working with PM, will ensure AFOSI completes a TTRA for each USSF acquisition program. TTRA is a country-by-country assessment that quantifies risks to a) Critical Program Information (CPI); b) enabling or advanced technologies for weapons systems or programs; and c) facilities such as laboratories, factories, research and development sites (e.g., test ranges), and military installations. **(T-1)**

2.1.6.1.6. Test and Evaluation Master Plan (TEMP) / Test and Evaluation Strategies (TES). SpRCO AIAs, working with the PM and the programs test manager, will specify the threat types required for test. AIAs will ensure that identified threats have the appropriate model type available for test activities. **(T-1)**

2.1.6.1.7. Threat Modeling. Annually, SpRCO AIAs will initiate a data call for all SpRCO threat modeling requirements and will review, prioritize, and submit threat model requirements to NSIC and SF/S2R. Prior year production requirements will be weighed against existing production gaps and new production requirements will be highlighted. **(T-2)**

2.1.7. **National Space Intelligence Center (NSIC).** As the USSF Service Intelligence Center, NSIC is responsible for foundational scientific and technical intelligence analysis on foreign space and counterspace system capabilities, performance, limitations and vulnerabilities as well as how foreign space forces and services contribute to other nations' comprehensive military capabilities and decision making. When the Defense Intelligence Analysis Program (DIAP) authoritative producer for a given issue is another part of the DIE, NSIC will facilitate communication between USSF acquisition intelligence organizations and those authoritative producers.

2.1.7.1. Authoritative Threat Assessments. Produce timely, accurate, and relevant threat intelligence products, including forecasts, roadmaps, assessments, technical intelligence, and threat scenarios. All products must comply with the Defense Intelligence All-Source Analysis Enterprise Management Guide, DoDD 5105.21, and support the test, R&D, and acquisition life cycle. **(T-0)**

2.1.7.2. Tailored Threat Assessments. Produce validated tailored threat assessments in coordination with AIAs to answer acquisition intelligence requirements. Tailored threat assessments include but are not limited to: VOLT report, VOLT page, Adversary Cyber Threat Assessment (ACTA), or relevant finished intelligence. All ACAT 1-D will be validated by Defense Intelligence Agency (DIA). **(T-1)**

2.1.7.3. Critical Intelligence Parameters (CIP). Validate CIP language, monitor CIP breach criteria, and notify programs/projects of impending CIP breaches caused by a foreign entity's demonstrated threat capability IAW the Manual for the Operations of the Joint Capabilities Integration and Development System and DIAI 5000.002. **(T-1)**

2.1.7.4. Threat Modules (TM). Produces comprehensive, authoritative, and validated assessments of foreign threats within NSIC's DIAP lane IAW DIAI 5000.002. Modules project the threat environment in a given threat topic out 20 years and constitute the DoD IC position with respect to those threat topics. NSIC is tasked by DIA to produce and update Threat Modules at least every two years. **(T-1)**

2.1.7.5. Threat Models. Produce Defense Intelligence All-Source Analysis Enterprise (DIAAE) authoritative threat models for space and counterspace systems for USSF, DoD, and IC MS&A activities. NSIC is responsible for verification and validation (V&V) of non-U.S. space and counterspace systems and networks MS&A for the USSF. In support of USSF acquisition activities, NSIC manages the digital threat intelligence baseline and will: **(T-1)**

2.1.7.5.1. Establish clear modeling standards and maintain all-source intelligence tradecraft standards for validated space and counterspace Modeling and Simulation (M&S) and collaborate within DIE as necessary.

2.1.7.5.2. Define processes in-line with DoD Instruction 5000.61 to conduct federated production of space and counterspace threat M&S with DIE authoritative producers and non-DIE M&S producers for all types of M&S.

2.1.7.5.3. Define easy to navigate processes IAW DoD Instruction 5000.61 to enable customers to obtain models and perform simulations of foreign space and counterspace systems and networks that are validated and approved for use by USSF force design, acquisitions, operations, and test communities.

2.1.7.5.4. Coordinate, de-conflict and federate production of space and counterspace M&S across the DIE and IC in conjunction with DIAP authoritative producers.

2.1.7.5.5. Engage with customers to continually improve the development of space and counterspace M&S requirements, ensuring appropriate model types and fidelities are developed to support predictive signature analysis, target development, tactics development, and test requirements.

2.1.7.5.6. Synchronize production of DIE authoritative models, reduce duplication of effort, define M&S standards for federated production, establish verification and validation processes, and codify processes to federate creation of DIE validated models of foreign space and counterspace systems and networks.

2.1.7.5.7. Threat selection for scenarios supporting USSF MS&A activities will be led by NSIC and informed by the mission and capability under test. Threat representation in MS&A scenarios will be based on DIAAE assessed threat order-of-battle (OOB), DIAAE assessed estimates of future threat OOB, and DIAAE threat performance and threat system operations assessments. Overall quantity and placement of the threat in the scenario will be based on the DIAAE assessment of adversarial weapons employment. Threat progression in the scenario and prioritization of threat employment (reversible to non-reversible) will be aligned with the DIAAE assessment of the adversaries' campaign planning activities.

2.1.8. **STARCOM Intelligence Directorate (STARCOM/S2).**

2.1.8.1. Threat Intelligence. Ensure Integrated Test Force, including Test Directors, Program Managers, and analysts, are threat-informed with threat analysis. **(T-2)** STARCOM/S2 will:

2.1.8.1.1. Prioritize Threat/Target lists. Ensure Operational Test and Evaluation (OT&E) program prioritized threat/target lists and threat environments reflect most current DIE/IC assessments and adequately address intelligence dependencies and operationally realistic threat representations. **(T-2)**

2.1.8.1.2. USSF Threat Intelligence Enterprise. STARCOM/S2 participates in Space Threat Steering Group (STSG), cross-program analysis, and other analytical activities across the USSF enterprise to ensure STARCOM equities are captured during program reviews, threat analysis working groups, intelligence supportability analysis, and other lifecycle intelligence activities. **(T-2)**

2.1.8.2. Intelligence Mission Data (IMD). Annually, STARCOM/S2 will submit test and training Intelligence Mission Data requirements to NSIC and SF/S2R. **(T-2)**

2.1.8.3. FMA. Annually, STARCOM will submit Foreign Material Acquisition (FMA) requirements to AF/TEZ. **(T-2)**

2.1.8.4. Threat Modeling. Annually, STARCOM/S2 will initiate a data call for all STARCOM threat modeling requirements. STARCOM/S2 will review, prioritize, and submit threat model requirements to NSIC and SF/S2R. Prior year production requirements will be weighed against existing production gaps and new production requirements will be highlighted. Unmet threat model requirements for STARCOM systems will be coordinated with NSIC for production. **(T-2)**

2.1.8.5. Multi-Domain Threats. STARCOM/S2 will ensure test and training environments incorporate relevant cyber, electronic warfare, and non-kinetic space threats to fully replicate adversary capabilities. **(T-2)**

2.1.8.6. Acquisition Intelligence Training. STARCOM/S2 in coordination with Career Field Managers, will develop training curricula to train and certify Acquisition Intelligence Analyst assigned to acquisition aligned FLDCOMs. **(T-2)**

2.1.9. **CFC Intelligence Directorate (CFC/S2).**

2.1.9.1. Lifecycle Support. Coordinate with PM, AIAs or SSC/S2 to determine acquisition intelligence lifecycle support required for intelligence-sensitive programs/projects to ensure new acquisition programs meet intelligence supportability throughout the program lifecycle. **(T-2)**

2.1.9.2. Emergent Threat**.** Integrate future threat assessments during capability fielding, support, and sustainment. Determine necessary intelligence support, data dependencies, and infrastructure to address these threats. **(T-2)**

2.1.9.3. FMA and FME. Annually, CFC/S2 will submit FMA/FME requirements to AF/TEZ. **(T-2)**

2.1.9.4. Intelligence Mission Data. Annually, CFC/S2 will submit operational and training Intelligence Mission Data requirements to NSIC and SF/S2R. **(T-2)**

2.1.9.5. Combat Force Proponent – Fielding Process. CFC S2 is responsible for providing a recommendation for the Operational Acceptance / Fielding of all intelligence-sensitive acquisition programs and capabilities. **(T-2)**

2.1.9.6. Threat Modeling. Annually, CFC/S2 will initiate a data call for all CFC modeling requirements. CFC/S2 will review, prioritize, and submit threat model requirements to NSIC and SF/S2R. Prior year production requirements will be weighed against existing production gaps and new production requirements will be highlighted. **(T-2)**

2.1.10. **Space Development Agency (SDA).** SDA program managers, following guidance outlined in **paragraph 2.1.5**, will incorporate authoritative DIE threat intelligence into SDA acquisition programs, process, and documents as directed by DoDI 5000.80 Operation of Middle Tier of Acquisition, DoDI5000.80_DAFI63-146 Operation of the Middle Tier of Acquisition (MTA), DoDI 5000.86 Acquisition Intelligence, and DoDI 5000.91 Product Support Management for the Adaptive Acquisition Framework. Programs already in the Joint Capabilities Integration and Development System (JCIDS) will continue based on the JCS "Terminate and Transition Plan for JCIDS Memo" dated 21 Aug. 2025 para. 3a. and 3b. Any new and potential follow-on processes, Major Capability Acquisition, Middle Tier of

Acquisition, Urgent Capability Acquisition, Software Acquisition Programs, Foreign Military Sales, and Special Access Programs will align with JCIDS replacement procedures IAW the above stated memo.

BRIAN D. SIDARI, Maj Gen, USSF
Deputy Chief of Space Operations
for Intelligence

Attachment 1

GLOSSARY OF REFERENCES AND TERMS

References

Public Law No: 118-31, *NDAA for Fiscal Year 2024*, 22 December 2023

Executive Order 14265, *Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base*, 9 April 2025

Final Report to Congress, Fiscal Year 2024 NDAA, Section 811: *Modernizing the Department of Defense Requirements Process*, 14 July 2025

Secretary of Defense Memorandum *Reforming the Joint Requirements Process to Accelerate Fielding of Warfighting Capabilities*, 20 August 2025

JCS Memorandum *Terminate or Transition Plan for Joint Capability Integration and Development System and Interim Guidance for Joint Requirements*, 21 August 2025

OUSD A&S, *Intelligence Support to the Adaptive Acquisition Framework (ISTAAF) Guidebook,* September 2023

OUSD R&E, *DoD Technology and Program Protection Guidebook,* 26 July 2022

DoDD 3100.10, *Space Policy*, 30 August 2022

DoDD 5105.21, *Defense Intelligence Agency*, 25 January 2023

DoDD 5135.02, *Under Secretary of Defense for Acquisition and Sustainment (USD(R&E)),* 15 July 2020

DoDD 5250.01, *Management of Intelligence Mission Data (IMD) in DoD Acquisition*, 29 August 2017

DoDI 3115.17, *Management and Oversight of DoD All-Source Intelligence*, 21 September 2020

DoDI 3150.09, *The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy*, 31 August 2018

DoDI 5000.02, *Operation of the Adaptive Acquisition Framework*, 8 June 2022

DoDD 5000.59, *DoD Modeling and Simulation (M&S) Management*, 15 October 2018

DoDI 5000.80, *Operation of the Middle Tier of Acquisition*, 25 November 2024

DoDI 5000.80/DAFI63-146, *Operation of the Middle Tier of Acquisition (MTA)*, 7 May 2021

DoDI 5000.85, *Major Capability Acquisition,* 6 August 2020

DoDI 5000.86, *Acquisition Intelligence*, 11 September 2020

DoDI 5000.89, *Test and Evaluation*, 19 November 2020

DoDI 5000.91, *Product Support Management for the Adaptive Acquisition Framework*, 4 November 2021

DoDI 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs,* 12 September 2024

CJCSI 3030.01B, *Implementing Joint Force Development and Design*, 1 July 2025

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

CJCSI 3170.01I, *Joint Capabilities Integration and Development System (JCIDS),* 23 January 2015.

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

JCS JCIDS Manual, *Manual for the Operation of the Joint Capabilities Integration and Development System,* 30 October 2021

JP 2-0, *Joint Intelligence (Incorporating Change 1, 5 July 2024),* 26 May 2022

DIEM-A Standard 401, *Defense Intelligence Threat Support to Acquisition*,16 April 2024

DAFPAM 63-128, *Integrated Life Cycle Management*, 3 February 2021

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

HAFMD 2-4, *Deputy Chief of Space Operations for Intelligence,* 24 April 2023

One Red, Bring Your Own Blue Modeling, Simulation, and Analysis Guidance, 16 August 2023

SPFI 16-1002, *USSF Threat Modeling, Simulation, and Analysis Guidance*, 20 November 2025

AFI 16-1001, *Verification, Validation, and Accreditation (VV&A)*, 29 April 2020

AFI 16-1005, *Modeling & Simulation Management*, 23 June 2016

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

Adopted Forms

DAF Form 847, *Recommendation for Change of Product*

Terms

Acquisition Category (ACAT)—Categories established to facilitate decentralized decision making and execution and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority, and applicable procedures. ACAT categories include: ACAT I, ACAT II, ACAT III, ACAT IV (Navy and Marine Corps only), and Abbreviated Acquisition Program (Navy and Marine Corps only). (DoDI 5000.85)

Acquisition Category ID (ACAT ID)—ACAT ID for which the Major Decision Authority (MDA) is the Defense Acquisition Executive (DAE), unless delegated. The "D" refers to the Defense Acquisition Board, which advises the USD(A&S) at major decision points. (DoDI 5000.85)

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

Acquisition intelligence analyst (AIA)—Responsible for integrating intelligence into acquisition/materiel processes. Acquisition intelligence activities include, among others: threat

support, to ensure acquisition functions are fully threat informed with authoritative intelligence; intelligence supportability analysis, to identify intelligence necessary to successfully acquire and employ DAF capabilities; ISR interoperability reviews, to ensure materiel systems can integrate with the ISR ecosystem; and intelligence production requirements development, to levy the requirements for specific types of intelligence to support materiel functions or systems. AIAs will abide by all intelligence oversite requirements.

Additional Performance Attribute—Performance attribute of a system not important enough to be considered a Key Performance Parameter (KPP) or Key System Attribute (KSA), but still appropriate to include in the Capability Development Document (CDD) or updated CDD. APAs are expressed using a threshold/objective format, using parameters which reflect Measures of Performance (MOPs). APAs must be measurable, testable, and support efficient Test and Evaluation (T&E).

Air Force Materiel Command/Space Systems Command (AFMC/SSC)—The command designated by the AF Acquisition Executive to manage an acquisition program. The intelligence support to the manager of an acquisition program usually resides with the Product Center/Logistics Center/Lab Research Site Intelligence Division/Branch. (DAFI 63-101/20-101)

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

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

Capability Development Document (CDD)—A CDD (includes the Information System (IS) CDD variant) specifies capability requirements in terms of developmental Key Performance Parameters (KPPs), Key System Attributes (KSAs), Additional Performance Attributes (APAs), and other related information necessary to support development of one or more increments of a materiel capability solution. A sponsor approved draft CDD is necessary for a Milestone A acquisition decision and each RFP release in support of the Technology Maturation and Risk Reduction (TMRR) phase of the Defense Acquisition System. A validated CDD is also necessary for each Development Request for Proposal (RFP) Release Decision Point and Milestone B acquisition decision. The CDD format is in the Joint Capabilities Integration and Development System (JCIDS) Manual, which is available online. (DoDI 5000.02)

Critical Intelligence Parameter (CIP)—A CIP is a defined threat capability or technology development threshold that, if attained (breached) may impede the lethality, survivability, or

sustainability of U.S. defense acquisition systems. CIPs therefore receive focused intelligence analysis and reporting that informs revisions to requirements, incremental upgrades, or potentially new acquisition programs to ensure capabilities remain technologically competitive on the modern battlefield. Acquisition intelligence professionals help the program office to identify CIPs and submit them via PRs in COLISEUM. Periodically reviewing open CIPs enables risk-based decisions for program resiliency. CIPs are monitored and tracked in the Defense Intelligence Threat Library, which is the authoritative source for CIPs and CIP statuses. (DIAI 5000.002, ISTAAF Guidebook)

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

Defense Acquisition Program—Technology demonstration, research effort, development planning activity, quick reaction capability, study, concept, initiative, system, modification, sustainment effort or upgrade involving intelligence support during research and development, acquisition, test, modernization, or sustainment.

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

Defense Intelligence Threat Library (DITL)—DIA managed online repository of Threat Modules. (DIAI 5000.002 JUN 18)

Developmental Test and Evaluation (DT&E)—Any testing used to assist in the development and maturation of products, product elements, or manufacturing or support processes. Any engineering-type test used to verify status of technical progress, verify that design risks are minimized, substantiate achievement of contract technical performance, and certify readiness for initial operational testing. Development tests generally require instrumentation and measurements and are accomplished by engineers, technicians, or soldier operator-maintainer test personnel in a controlled environment to facilitate failure analysis. (DoDI 5000.02)

DIAAE—The collective set of all DoD organizations that execute all-source analysis activities in production of Defense Intelligence. (DoDI 3115.17)

Digital Engineering (DE)—A means of using and integrating digital models and the underlying data to support the development, test and evaluation, and sustainment of a system. (DoDI 5000.02)

Digital Engineering Ecosystem—The interconnected infrastructure, environment, and methodology (process, methods, and tools) used to store, access, analyze, and visualize evolving systems' data and models to address the needs of the stakeholders. (DoDI 5000.02)

Federal Acquisition Regulation (FAR)—The regulation for use by federal executive agencies for acquisition of supplies and services with appropriated funds. The FAR is supplemented by DoD, the military departments, the Defense Contract Audit Agency (DCAA), the Defense Information Systems Agency (DISA), and the Defense Logistics Agency (DLA). The DoD supplement is called the DFARS (Defense FAR Supplement). (DoDI 5000.02)

Foreign Materiel Acquisition (FMA)—FMA activities that include gaining physical possession of, or access to, an item of foreign material or technology. (DoDD S-3325.01E)

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

Initial Capabilities Document (ICD)—A category of capability requirements documents that specifies one or more capability requirements and associated capability gaps that represent unacceptable operational risk if left unmitigated. It recommends partially or wholly mitigating identified capability gap(s) with a materiel capability solution, or some combination of materiel and non-materiel solutions. A validated ICD is an entrance criterion necessary for each Materiel Development Decision (MDD). (DoDI 5000.02)

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

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

Intelligence Costing—An integral part of the ISA is the estimation of costs associated with the Intelligence resources required to support the acquisition programs. The lack of understanding of these costs can result in scheduling delays, costly workarounds, and unplanned adjustments to Operations and Maintenance budgets.

Intelligence Data (ID)—Data used for RDT&E, such as M&S, consisting of Characteristics and Performance (C&P), Electromagnetic Spectrum/Electronic Warfare (EMS/EW) Signatures, OOB and Geospatial information to develop and test in a full Multi-Domain Scenario for capability validation of platforms and systems under development.

Intelligence Mission Data (IMD)—DoD intelligence used for programming platform mission systems in development, testing, operations, and sustainment including, but not limited to, the functional areas of signatures, electronic warfare integrated reprogramming (EWIR), OOB, characteristics and performance (C&P), and geospatial intelligence (GEOINT). (DoDD 5250.01)

Intelligence Requirement—1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence

to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. (JP 2-0)

Intelligence-sensitive—Any program/initiative that produces, consumes, processes, or influences intelligence information, thereby requiring threat or intelligence infrastructure support. If it is likely that, in the future, the program will produce, consume, process, or influence intelligence information, it should be considered intelligence-sensitive. (DAFI14-411)

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

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

Intelligence, Surveillance, and Reconnaissance (ISR)—Term referring to the activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. (JP 2-0)

JCIDS Documents—(Initial Capabilities Document (ICD), Capability Development Document (CDD)). IAW CJCSI 3170.01I and the JCIDS Manual, DIA validates the threat and intelligence supportability information in all JROC Interest, JCB Interest, and Joint Integration Initial Capabilities Document, and Capability Development Document through the intelligence certification process (ref. CJCSI 5123.01I). For programs with Joint Information or Independent Joint Potential Designators, which DIA does not review or validate, DoD components can utilize DIA-validated threat reference information and data contained in DoD service validated and authoritative intelligence products for their JCIDS documents. JCIDS only applies to legacy programs which meet JCS Memo dated 21 Aug. 2025 continuation criteria. Programs meeting para 3a. and 3b. will continue in JCIDS process.

Joint Capabilities Board (JCB)—The JCB is a board below the Joint Requirements Oversight Council (JROC) and provides review and endorsement of documents and adjudication of lower level issues prior to validation by the JROC. The JCB has validation authority for Joint Capabilities Integration and Development System (JCIDS) documents with a Joint Staffing Designator (JSD) of "JCB Interest." The JCB is chaired by the Joint Staff (JS) Director, J-8. It is comprised of general or flag officers, or government civilian equivalent, from the Services and Combatant Commands. (CJCSI 5123.01I)

Joint Requirements Oversight Council (JROC)—An organization that assists the Chairman, Joint Chiefs of Staff in identifying, assessing, and validating joint military requirements to meet the National Defense Strategy (NDS), and in identifying the core mission area associated with each requirement, ensuring consideration of trade-offs among cost, schedule, and performance objectives for joint military requirements, in establishing and assigning priority levels for joint military requirements. (DoDD 5135.02)

Key Operational Problem—Areas identified in the NDS that the DoD needs to focus on improving. (Secretary of Defense Memorandum)

Key Performance Parameter—Performance attribute of a system considered critical or essential to the development of an effective military capability. KPPs are contained in the Capability Development Document (CDD) and the updated CDD and are included verbatim in the Acquisition Program Baseline (APB). KPPs are expressed in term of parameters which reflect Measures of Performance (MOPs) using a threshold/objective format. KPPs must be measurable, testable, and support efficient and effective Test and Evaluation (T&E).

Key System Attribute—Performance attribute of a system considered important to achieving a balanced solution/approach to a system, but not critical enough to be designated as a Key Performance Parameter (KPP). KSAs must be measurable, testable, and support efficient and effective Test and Evaluation (T&E). KSAs are expressed in terms of Measures of Performance (MOPs).

Life Cycle—The span of time associated with a technology, concept, system, subsystem, capability, initiative, or end-item that begins with the conception and initial development of the requirement, continues through development, acquisition, fielding, sustainment, until the time it is either consumed in use or disposed of as being excess to all known materiel requirements. (DoDI 5000.02)

Lifecycle Mission Data Plan (LMDP)—The program manager's plan for how the program manager and other organizations will address specific program needs for Intelligence Mission Data. It contains the results of Intelligence Mission Data planning and spans the entire lifecycle of an Intelligence Mission Data-dependent acquisition program. The LMDP potentially influences programmatic decisions based on the availability of Intelligence Mission Data over the life of the program. (DoDI 5000.02)

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

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

Models Based Systems Engineering (MBSE)—The formalized application of modeling to support system requirements, design, analysis, verification, and validation activities beginning in the conceptual design phase and continuing throughout development and later system life-cycle phases. (DoDI 5000.97)

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

for intelligence value and delivering the desired product. Finally, the intelligence information is disseminated to the senior leadership or customer. (JP 2-0)

Planning, Programming, Budgeting, and Execution System (PPBE)—A cyclic process containing four distinct but interrelated phases: Planning—Produces a fiscal forecast, planning guidance, and program guidance; Programming—Creates the DAF portion of the DoD's Future Years Defense Program (FYDP) by defining and examining alternative forces and weapons and support systems; Budgeting—Formulates and controls resource requirements, allocation, and use; and Execution—Measures and validates the performance of the planning, programming, and budgeting phases. (DoD 7000.14-R)

Program Management Directive (PMD)—The official Headquarters, U.S. Air Force, document used to convey the guidance and direction of the decision authority and identify the various organizations, along with their essential responsibility, for ensuring the success of a program or other effort. PMDs are required for funded program contained in the Department of the Air Force Acquisition Program Master List. (DoDI 5000.02)

Program Protection Plan or Planning (PPP)—The Program Protection Plan is the program manager's single source document used to coordinate and integrate all protection efforts designed to protect critical information and resources, and to prevent inadvertent disclosure of leading-edge technology to foreign interests. Program Protection Planning is a comprehensive effort that encompasses all security, technology transfer, intelligence, and counterintelligence processes through the integration of embedded system security processes, security manpower, equipment, and facilities. (DAFI 63-101/20-101)

Risk Management Plan (RMP)—A document that describes a program's risk management approach and activities. (Note: some programs document their plans in a combined Risk, Issue, and Opportunity (RIO) Management Plan. Others document their plans in separate documents, that is, separate Risk Management, Issue Management and Opportunity Plans.) Now it is called the Program Risk Process (PRP). (DoDI 5000.02)

Requirements and Resourcing Alignment Board (RRAB)—Each budget cycle, the RRAB shall select topics from the top-ranked KOP and nominations from the co-chairs to perform analysis, issue programming guidance, and recommend allocation of funding from the Joint Acceleration Reserve (JAR). (SECDEF Memo 20 Aug 2025)

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

Special Access Program (SAP)—A sensitive acquisition, intelligence, or operations and support program, that imposes need-to-know and access controls beyond those normally provided for access to classified information. Also called SAP. (DoDI 5205.11)

Supply Chain Risk Management (SCRM)—The process for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the DoD supply chain from beginning to end to ensure mission effectiveness. Successful SCRM maintains the integrity of products, services, people, and technologies, and ensures the undisrupted flow of product, materiel, information, and finances across the lifecycle of a weapon or support system. DoD SCRM encompasses all sub-sets of SCRM, such as cybersecurity, software assurance, obsolescence, counterfeit parts, foreign ownership of sub-tier vendors, and other categories of risk that affect the supply chain. (DIAI 5000.002, ISTAAF Guidebook)

Supportability—Supportability refers to the availability, suitable, and sufficiency of required intelligence support needed by a capability. Assessing supportability requires a comparison of the Sponsor's stated operational/capability requirements with the expected intelligence support capability, throughout a capabilities solution's projected lifecycle. The ability to adequately assess supportability depends upon the completeness of the Sponsor's declaration of the capabilities intelligence support requirements and must be evaluated within the context of any shortfall mitigation strategies found. Availability refers to whether the intelligence data, information, infrastructure, or resources are, or are expected to be, available throughout the capability solution's projected lifecycle; suitability refers to whether the required intelligence data, information, infrastructure, or resources are, or are expected to be, appropriate to support the capability; and, sufficiency refers to whether the intelligence data, information, infrastructure, or resources are, or are expected be, adequate to support the Sponsor's capability. (DoDI 5000.02, ISTAAF Guidebook)

Tailoring—Tailoring recognizes that acquisition programs are not all the same. Policy permits customized reviews, processes, and decision support information to accommodate the unique characteristics of a program while still meeting the statutory and regulatory needs for decision making and oversight. Tailoring ensures a program or project can balance all types of risks, including technical, programmatic, or strategic risks in providing the needed capability to the warfighter or user in the shortest time while ensuring affordability, supportability, system safety and performance. AIAs responding to a PMs need to tailor an acquisition program, provide tailored threat intelligence products for those programs for which there is no timely, standardized threat reporting from the Intelligence Community. (DAFPAM 63-128)

Test and Evaluation (T&E)—Process by which a system or components are exercised and results analyzed to provide performance-related information. The information has many uses including risk identification and risk mitigation and empirical data to validate models and simulations. T&E enables an assessment of the attainment of technical performance, specifications, and system maturity to determine whether systems are operationally effective, suitable and survivable for intended use, and/or lethal. There are various types of T&E defined in statute or regulation: Developmental Test and Evaluation (DT&E), Operational Test and Evaluation (OT&E), Live Fire Test and Evaluation (LFT&E), and Interoperability Certification.

Test and Evaluation Master Plan (TEMP)—Document that describes the overall structure and objectives of the T&E program and articulates the necessary resources to accomplish each phase. It provides a framework within which to generate detailed T&E plans and documents schedule, and resource implications associated with the T&E program. The TEMP serves as the overarching document for managing a T&E program. (DoDD 5000.01)

Technology Targeting Risk Assessment (TTRA)—A country-by-country assessment that quantifies risks to a) Critical Program Information (CPI); b) enabling or advanced technologies for weapons systems or programs; and c) facilities such as laboratories, factories, research and development sites (e.g., test ranges), and military installations. TTRAs are an important foundation for the Multi-Disciplined Counterintelligence Threat Assessment (MDCITA), which reports adversary collection capabilities relative to the program's critical information and the protection of that information. TTRA is an MS-A requirement document for ACAT I-III programs that have identified CPI. (DIAI 5000.002)

Threat—The sum of the potential strengths, capabilities, and strategic objectives of any adversary that can limit U.S. mission accomplishment or reduce force, system, or equipment effectiveness. It does not include natural or environmental factors affecting the ability or the system to function or support mission accomplishment, mechanical or component failure affecting mission accomplishment unless caused by adversary action, or program issues related to budgeting, restructuring, or cancellation of a program. (DIAI 5000.002 JUN 18)

Training System Requirements Analysis (TSRA)—The TSRA is a formal and systematic front-end analysis of the weapon system to determine training system requirements and provides alternative solutions for a training system acquisition or modification. The TSRA uses the Instructional System Development (ISD) process and supportability analyses to address total training requirements (training hardware, software, facilities, instructional media, etc.) throughout the life cycle of the weapon system being defined. (DAFPAM 63-128)

Validated IMD Supportability Report (VISR)—The VISR provides a technical evaluation of the enterprise's ability to support Intelligence Mission Data demands throughout a weapon system's life cycle. It gives decision makers the mission context about Intelligence Mission Data production status (holdings and efforts to fill gaps) and warns the intelligence enterprise of analytic and production demands; it also facilitates IPC production/resource planning. The VISR also explains the Intelligence Mission Data dependency, production suitability, and availability of Intelligence Mission Data with additional recommendations to stakeholders. (ISTAAF Guidebook 2023)

Validated On-Line Lifecycle Threats (VOLT)—The VOLT is the authoritative threat assessment tailored for one or more programs as applicable. VOLTs include threat modules and can include additional tailoring to articulate the relevance of each module to a specific acquisition program or planned capability. Acquisition intelligence professionals can request combined VOLTs to serve multiple ACAT I-III programs, but MCAs and programs on the DOT&E Oversight List require a unique, system-specific VOLT. VOLT development starts with the establishment of a Threat Steering Group composed of program office representatives, DIA/Service Intelligence Production Center representatives, DevOps Test representatives, DOT&E representatives (if under DOT&E oversight) and the program's acquisition intelligence analyst. The goal is to identify the program's KPPs, critical components/functions, and relevant threats, including a review or addition of CIPs. (ISTAAF Guidebook 2023)

Attachment 2

THREAT AND INTELLIGENCE CERTIFICATION

A2.1. Introduction: Intelligence Certification is intended to ensure that capability solutions are developed with sufficient and complete threat data, all intelligence supportability requirements are documented, and all threat modeling and simulation requirements are documented. Service managed requirements will receive intelligence certification from SF/S2, while intelligence certification for JROC managed requirements will be managed by J-283/ Intelligence, Requirements, Certification Office (IRCO).

A2.2. Applicability: SF/S2 leads the intelligence certification for service level requirements, while J-283/IRCO leads the intelligence certification process for the Joint Staff on behalf of the J-2 Directorate. Intelligence certification is applicable to all capability development documents regardless of acquisition pathway; including documents protected by Alternative Compensatory Control Measure (ACCM) or Special Access Program (SAP)/Special Access Required (SAR) designation. Updates to threat baseline or updates to a capability development document will require revalidation of intelligence certification of the effected document; increments and Annexes may be considered on a case-by-case basis with adequate justification to the USSF S5 Gatekeeper. In the event of a Critical Intelligence Parameter (CIP) breach or Classified Information Compromise Assessment (CICA) initiation, the certification will be reviewed and reassessed for adequacy and supportability based on updated threat analysis and subsequent CIP breach review. Intelligence certification requirements are aligned with prioritized Key Operational Problems (KOPs) identified by the RRAB, while legacy programs identified by JCS Memo dated 21 Aug. 2025 will continue as outlined in Manual for the Operations of the Joint Capabilities Integration and Development System (JCIDS Manual), Annex G Appendix G Enclosure B, and intelligence certification process are located IRCO's SIPRNET website **https://intelshare.intelink.sgov.gov/sites/irco/SitePages/Home.aspx**.

A2.3. Elements of the Threat and Intelligence Certification to be satisfied:

A2.3.1. Threat Approval.

A2.3.1.1. Tailored Threat Assessment/ Defense Intelligence Threat Library (DITL).

A2.3.1.2. Threat Environment and Threat Progression.

A2.3.1.3. Lifecycle Cyber Assessment.

A2.3.1.4. CIPs.

A2.3.1.5. Supply Chain Risk Assessment focusing on foreign influence.

A2.3.1.6. IMD/ Lifecycle Data Management Plan (LMDP).

A2.3.2. Intelligence Manpower, Resources, Funding, and Training.

A2.3.2.1. Lifecycle manpower requirements.

A2.3.2.2. Assessed shortfalls (hardware, software, training).

A2.3.2.3. Intelligence funding for support requirements.

A2.3.3. Intelligence Interoperability.

A2.3.3.1. External dependencies (e.g., mission partners, data tools, databases, etc.).

A2.3.3.2. Specific external networks, data sets, tools, etc., that enable capability.

A2.3.3.3. New IC Data Standards / Network compatibility.

A2.3.4. Targeting.

A2.3.4.1. Does capability have any dependencies with targeting support?

A2.3.4.2. Targeting product requirements throughout the lifecycle.

A2.3.4.3. Assessed targeting support gaps/shortfalls.

A2.3.5. Space.

A2.3.5.1. Space-based intelligence support requirements.

A2.3.5.2. Space-based intelligence gaps/shortfalls.

A2.3.6. Counterintelligence.

A2.3.6.1. Critical Program Information (CPI).

A2.3.6.2. Supply Chain Threat Assessment (SCTA).

A2.3.6.3. Technology Targeting Risk Assessment (TTRA).

Attachment 3

COMBAT FORCES COMMAND (CFC) INTELLIGENCE SUPPORT PLAN

A3.1. Overview.

A3.1.1. The Intelligence Support Plan (ISP) provides decision-makers with a comprehensive overview of intelligence support requirements, the intelligence infrastructure (people, systems, procedures, products, etc.) needed to satisfy the requirements, any gaps or shortfalls between the required infrastructure and the current/planned infrastructure, time-phased courses of action necessary to ensure these shortfalls are resolved. It also contains additional data on recommended solutions and system supportability. The ISP is a vital tool that provides CFC/S2 with the information required to vote in support of the operational acceptance/fielding of intelligence-sensitive programs. This guidance supersedes the Mission Area Intelligence Requirements Document (MAIRD) and is in addition to the new SpRCO Rapid Threat Support Plan (RTSP).

A3.2. Policy.

A3.2.1. CFC requires all capabilities to be fully burdened IAW the Fully Burdened Space and Ground Capabilities for Space Weapon Systems Delivery Memo dated 10 Feb 2023. The ISP will document how intelligence was integrated during the development, acquisitions and decision-making processes, so that operationally accepted capabilities are combat-ready and able to provide our Guardians with the capabilities needed to outcompete rivals, deter aggressors, and defeat adversaries.

A3.2.2. This appendix (**ATTACHMENT 3**) applies to all intelligence-sensitive capabilities seeking Operational Acceptance (OA) or Fielding, regardless of acquisitions agency (Space Development Agency (SDA), Space Rapid Capabilities Office (SpRCO), Dept of the Air Force Rapid Capabilities Office (DAFRCO), FLDCOMs, etc.) or acquisition pathway (Adaptive Acquisition Framework, Rapid Acquisitions Programs etc.). Intelligence sensitive is defined as any program/initiative that produces, consumes, processes, or influences intelligence information, thereby requiring threat or intelligence infrastructure support or if it is likely that, in the future, the program will produce, consume, process, or influence intelligence information.

A3.2.3. The PEO, PM, SIOs, and AIAs will provide the required documentation to CFC/S2Z for compilation and review as part of the Combat Force Proponent – Fielding Process. Intelligence risks and gaps require a risk management plan. CFC/S2Z will work with the PEO, PM, SIO, AIAs and operational units to develop risk management plans for operational intelligence risks or gaps. CFC/S2Z will assist with the development of non-operational intelligence risks and gaps management plans as requested. The ISP will be reviewed by CFC S2 prior to any operational acceptance or fielding decisions.

A3.3. ISP format and minimum required information.

A3.3.1. Introduction.

A3.3.1.1. Narrative: Summary of the program's operational scope.

A3.3.2. Intelligence Sensitivity Determination Memo.

A3.3.3. Threat and Intelligence Certification Documentation

A3.3.3.1. ICD/CDD section 2 and section 9.

A3.3.3.2. Completed CIPs.

A3.3.3.3. Completed LMDP.

A3.3.3.4. Tailored Threat Support Plan (TSP) and threat intelligence.

A3.3.4. Intelligence Support to System Development.

A3.3.4.1. Counterintelligence (CI)/Foreign intelligence threats.

A3.3.5. Intelligence support to Testing.

A3.3.5.1. Technical OPSEC Assessment (TOA).

A3.3.5.2. SIGINT Threat Mitigation Report (STMR).

A3.3.5.3. Intelligence sections of DT/OT plans.

A3.3.6. Intelligence Support to Operations.

A3.3.6.1. Intelligence Supportability Analysis (ISA).

A3.3.6.2. Intelligence support to the Intelligence Process (TCPAD) (as needed).

A3.3.6.3. Intelligence support to OPSEC/MILDEC Plans (as needed).

A3.3.6.4. Training System Requirements Analysis (TSRA) (as needed).

A3.3.6.5. Intelligence Health Assessment (IHA).

A3.3.6.6. Technology Readiness Assessment (TRA).

A3.3.6.7. Test and Evaluation Master Plan (TEMP) or Test and Evaluation Strategies (TES).

A3.3.6.8. Essential Elements of Information (EEI).

A3.3.6.9. Cross Program Analysis (CPA) Documents.

A3.3.6.10. Technology Targeting Risk Assessments (TTRAs).

A3.3.6.11. Program Protection Plans (PPP).

A3.3.7. Intelligence Risk Management plan for each identified risk/gap.

A3.3.7.1. Detailed description of the risk and the cause.

A3.3.7.2. Risk Category: Critical or Substantive, include rational.

A3.3.7.3. Mitigation Strategy: Accept/Avoid/Transfer/Control/Monitor.

A3.3.7.4. Mitigation Plan: The proposed solution to the risk is detailed here. A graphical representation of the infrastructure elements that support this solution can also be presented. If the solution concept is scenario-dependent, potential alternative solutions may also be listed.

A3.3.7.5. Actions: Specific steps to implement the Mitigation Plan and assigned AOs.

A3.3.8. Additional information as needed.

A3.3.9. Acronym List.

A3.3.10. Definitions.

Attachment 4

RISK MANAGEMENT PLAN (RMP)

A4.1. Overview.

A4.1.1. A risk is an unwanted event that may or may not occur in the future. A risk has three components, 1) a future (yet-to-happen) root cause that, if corrected or eliminated, would be prevented along with its potential consequences, 2) a probability (or likelihood), assessed at the present time, of that future root cause occurring, 3) the consequence (or impact) of that future occurrence. The culmination of the Intelligence Support Plan is the RMP, which encompasses the identification, analysis, mitigation planning, mitigation plan implementation, and tracking of intelligence risks to the program. The RMP identifies risk drivers, dependencies, root causes, and corrective action, as well as consequence management. As a best practice, RMPs should focus more on the causal factors that enable the existence of risk rather than on consequence management. Eliminating the root cause of a risk avoids its consequences. Missing or incomplete ISP requirements are considered a risk and should be included in the RMP.

A4.2. Policy.

A4.2.1. **Risk Management Plans will include the following sections.**

A4.2.1.1. Introduction and overview of program risks/causes.

A4.2.1.2. In depth, look at each risk.

A4.2.1.3. Risk: Describe the risk and the cause.

A4.2.1.4. Risk Category: Critical or Substantive include rational.

A4.2.1.5. Mitigation Strategy: Accept/Avoid/Transfer/Control/Monitor.

A4.2.1.6. Mitigation Plan: The proposed solution to the risk is detailed here. A graphical representation of the infrastructure elements that support this solution can also be presented. If the solution concept is scenario-dependent, potential alternative solutions may also be listed.

A4.2.1.7. Actions: Specific steps to implement the Mitigation Plan and assigned action officers.

A4.2.2. **The following documents inform the RMP.**

A4.2.2.1. Adversary Cyber Threat Assessment (ACTA).

A4.2.2.2. Capabilities Development Document (CDD).

A4.2.2.3. Capabilities Production Document (CPD).

A4.2.2.4. Initial Capabilities Document (ICD).

A4.2.2.5. Intelligence Health Assessment (IHA).

A4.2.2.6. Lifecycle Mission Data Plan (LMDP).

A4.2.2.7. Program Protection Plan (PPP).

A4.2.2.8. Systems Engineering Plan (SEP).

A4.2.2.9. Technology Readiness Assessment (TRA).

A4.2.2.10. Test and Evaluation Master Plan (TEMP) or Test and Evaluation Strategies (TES).

A4.2.2.11. Validated Online Life-cycle Threat (VOLT) Report.

A4.2.3. **Risk Categories.**

A4.2.3.1. Critical**:** Any issue that would prevent the program's ability to provide a required operational/functional capability. A critical issue shall frequently relate to another supporting program (e.g., information required from another program), program synchronization, lack of resources, technology gaps, or other factors. Missing integrated architectural product content may constitute a critical issue.

A4.2.3.2. Substantive: Any issue that would significantly impact the program's ability to provide a required operational/functional capability. Missing integrated architectural product content may constitute a substantive issue.

A4.2.4. **Risk Mitigation.** What is the plan to address the risk? Risk can be:

A4.2.4.1. Accepted: Acknowledge the risk event and the program is prepared to accept the consequences.

A4.2.4.2. Avoided: The program reduces or eliminates the risk event by taking an alternate path.

A4.2.4.3. Transferred: Reassigning or delegating responsibility for tasks to mitigate a risk to another entity (e.g., transferring financial responsibility).

A4.2.4.4. Controlled: Actively reduce risk to an acceptable level.

A4.2.5. **Risk mitigation strategies should address the risk in the following order.**

A4.2.5.1. Reducing the likelihood of occurrence.

A4.2.5.2. Reducing the impact.

A4.2.5.3. Accepting the risk.

A4.2.6. **Consider the following when choosing the best mitigation option.**

A4.2.6.1. Is the risk mitigation plan feasible?

A4.2.6.2. Is the risk mitigation plan affordable in terms of funding and any additional resources needed (e.g., personnel, equipment, facilities)?

A4.2.6.3. Is adequate time available to develop and implement the risk mitigation plan?

A4.2.6.4. What impact does the risk mitigation plan have on the overall program schedule and on the technical performance of the system?

A4.2.6.5. Are the expectations realistic given program circumstances, constraints, and objectives?

A4.2.7. **Consider the following when developing risk response strategies.**

A4.2.7.1. Time.

A4.2.7.2. Cost.

A4.2.7.3. Quality.

A4.2.7.4. External Considerations – Impact on other projects.

A4.2.8. **Monitoring the Risk:** How has the risk changed or how are the risk mitigation plans working?

A4.2.8.1. Track the implementation and progress of the risk mitigation activities, not just the development and planning of the selected strategy.

A4.2.8.2. Include Technical Performance Measures as an integral activity when monitoring risks after selecting the appropriate risk mitigation strategy.

A4.2.8.3. Conduct regular status updates to monitor risks for changes to likelihood and/or consequences.

A4.2.8.4. Document risks that can be retired as well as risks that are still being mitigated to prevent an unnoticed relapse of the retired risk.

A4.2.8.5. Keep lines of communication open to notify management when ability to mitigate the risk is ineffective.

Attachment 5

SPACE THREAT STEERING GROUP (STSG) CHARTER

A5.1. Authorities and References: HEADQUARTERS AIR FORCE MISSION DIRECTIVE 2-4, 24 APRIL 2023 Special Management: DEPUTY CHIEF OF SPACE OPERATIONS FOR INTELLIGENCE

DIEM-A Standard 401, Defense Intelligence Threat Support to Acquisition

CJCSI 3318.01 Acquisition-Intelligence-Requirements Annual Priorities and Risk Management Framework

DoDD 3100.10 Space Policy

DoDI 3115.17 Management and Oversight of DoD All-Source Intelligence

DoDI 3150.09 The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy

DoDD 5000.59 DoD Modeling and Simulation (M&S) Management

DoDI 5000.86 Acquisition Intelligence

DoDI 5000.91 Product Support Management for the Adaptive Acquisition Framework

DoDI 5000.97 Digital Engineering

DoDD 5250.01 Management of Intelligence Mission Data (IMD) in DoD Acquisition

DAFI 63-101/20-101 Integrated Lifecycle Management

DAFI 63-125 Nuclear Certification Program

A5.2. Objective and Scope.

A5.2.1. The Space Threat Steering Group (STSG) enables acquisition sponsors, program managers, and AIAs to fully integrate timely and accurate intelligence into acquisition programs to ensure all acquisition programs, regardless of acquisition pathway or access control requirements (CAP/SAP), are fully threat informed and supported throughout the acquisition lifecycle as directed by DoD1 5000.86, DoDI 5000.80. and DAFI 63-101/20-101. STSG activities must align with the MEIA and RRAB to ensure integration of industry contributions and rapid experimentation.

A5.2.2. Additionally, STSG ensures an acquisition program's modular open systems approach and digital threads as outlined in DoDI 5000.97 and DAFI 63-101/20-101, are tailored in response to threat intelligence inputs. STSG ensures space acquisition threat intelligence is detailed and integrated throughout the capability's lifecycle, with particular focus on the emerging battlespace to comply with Title 10, United States Code, section 3601. STSG is not

a fixed group on a fixed schedule, rather, the STSG is a dynamic group that adapts to individual capability requirements. STSG activities must align with the Mission Engineering Integrations Activity (MEIA) and RRAB to ensure integration of industry contributions and rapid experimentation.

A5.3. Leadership and Membership.

A5.3.1. STSG consists of senior executive-level representatives from USSF S2 and senior action officer (AO) representatives from STSG core members. Additionally, select offices will provide additional functional expertise. The STSG Chair shall approve changes and additions to STSG.

A5.3.2. Each core member organization is required to designate a primary and alternate representative. Representatives should have the authority to speak on behalf of their organization on threat intelligence, requirements, and acquisition related issues.

A5.4. Roles and Responsibilities.

A5.4.1. **USSF S2 - STSG Chair:** HAF Mission Directive 2-4, Deputy Chief of Space Operations for Intelligence, 24 April 2023, designated USSF S2 as the Head of the Intelligence Community Element (HICE) for space; serving as the USSF's HICE, the S2 is responsible for fulfilling service tasks and responsibilities flowing from Executive Order 12333, U.S. Intelligence Activities for space related intelligence, including acquisition intelligence. In the capacity of STSG Chair, USSF S2 serves as the authority for collaboration and coordination across the Intelligence Community (IC) to enable threat intelligence integration and intelligence certification for USSF capabilities. USSF S2 oversees NSIC activities, as well as overseeing, coordinating, and supervising USSF intelligence support to USSF acquisition, testing, operations and training to ensure accurate and consistent threat modeling. Therefore, USSF S2 serves as the threat authority for the space requirements community when there are analytic disputes on the interpretation of finished threat intelligence used to support space acquisitions.

A5.4.2. **SF/S2R - Overall STSG process owner:**

A5.4.2.1. Provide overall STSG management and establish STSG business rules.

A5.4.2.2. Ensures qualified intelligence analysts are supporting the requirements development phase.

A5.4.2.3. Participate in SF/S5R weekly, monthly, and quarterly tag-ups, Solution Pathway Reviews, Weapon System Reviews (WSR), and other meetings to assess intelligence need within new requirements.

A5.4.2.4. Collaborate with NSIC and DIA to assess emerging disruptive technology and assess impact to new requirements.

A5.4.3. **AIAs - STSG Co-lead:**

A5.4.3.1. Lead coordination of intelligence supportability analysis and cyber threat analysis in collaboration with the PM. Works with PM to meet IRCO Intelligence Certification Checklist requirements.

A5.4.3.2. Lead the coordination with SF/S5R and PM to identify and prioritize threats to capability.

A5.4.3.3. Document threat intelligence gaps and any unmet countermeasure requirements.

A5.4.3.4. In collaboration with IPC's, draft critical intelligence parameters (CIP) for acquisition programs.

A5.4.3.5. Lead section 2 and section 9 of ICD/CDD writing in collaboration with NSIC.

A5.4.3.6. Leads the development of the Lifecycle Mission Data Plan (LMDP).

A5.4.4. **SF/S2I.** Ensure capability requirements, and its associated concept of operation, are synchronized with the programs threat baseline.

A5.4.5. **NSIC – Support Role.**

A5.4.5.1. Lead analytical support to the requirements process.

A5.4.5.2. Establish, maintain, and disseminate a standardized threat baseline for use by the acquisition program's stakeholders.

A5.4.5.3. Provide service level threat validation and production (DIAP IPC) support to acquisition program.

A5.4.5.4. Lead threat forecasting, projection, and counterspace kill-web assessments.

A5.4.5.5. Develop threat environment assessments that support IOC+10-year lifecycle or time epochs that align with the acquisition programs Lifecyle.

A5.4.6. **Sponsor (S5R/PM):**

A5.4.6.1. Notifies SF/S2R of weekly, monthly, and quarterly tag-ups, Solution Pathway Reviews, Weapon System Reviews, and other meetings to enable threat intelligence integration.

A5.4.6.2. Ensure threat intelligence requirements are identified early, address acquisition programs IOC+10 years requirement, and that intelligence production requests are tailored to meet requirements of modular open systems and digital threads.

A5.4.6.3. Works with AIAs and NSIC to meet intelligence certification checklist requirements.

A5.4.6.4. Document threat intelligence gaps and any unmet threat intelligence requirements.

A5.4.7. **CFC S2.**

A5.4.7.1. Identify early risk to system integration.

A5.4.7.2. Ensures threat intelligence is sufficient to support system development, acceptance, and integration.

A5.4.7.3. Identify threat model needs for system acceptance and integration.

A5.4.8. **STARCOM Intelligence Directorate (S2).**

A5.4.8.1. Identify threat model needs for OT&E.

A5.4.8.2. Ensures threat intelligence is sufficient to support OT&E.

A5.4.8.3. Identify early risk to system transition to OT&E.

A5.4.9. **Additional members when core members identify need:**

A5.4.9.1. SSDP

A5.4.9.2. SWAC

A5.4.9.3. NRO Intelligence LNO (by invitation)

A5.4.9.4. DIA TLA-3 (by invitation)

A5.4.9.5. DTRA (by invitation)

A5.4.9.6. Delta 12

A5.5. Administration.

A5.5.1. **STSG Chair recommends, develops, and manages the administrative process.**

A5.5.2. **STSG initiation:**

A5.5.2.1. SF/S2R will notify members of a new acquisition program.

A5.5.2.2. SF/S2R will organize an STSG kick-off meeting.

A5.5.2.3. SF/S2R will develop an agenda and provide the agenda to members in advance of scheduled meetings.

A5.5.3. **Meeting/attendance:**

A5.5.3.1. STSG will identify intelligence requirements of new acquisition program.

A5.5.3.2. STSG co-leads will establish STSG schedule for each capability to meet the needs of the capabilities acquisition pathway.

A5.5.3.3. Members/technical specialists are required to attend meetings/provide updates.

A5.5.3.4. STSG co-leads will provide meeting minutes to members/stakeholders.

A5.5.4. **Assigned tasks/accountability:**

A5.5.4.1. STSG co-leads will assign/track tasks.

A5.5.4.2. STSG Chair will address members/technical specialist failing to meet suspense's.

A5.5.5. **Comment resolution:**

A5.5.5.1. STSG co-leads will adjudicate all comments associated with taskings and coordinate resolutions.

A5.5.6. **Expected Outcomes/Deliverables.**

A5.5.6.1. Increased collaboration between NSIC, AIAs, S5R, PMs, STARCOM/OTTI, CFC, and IC.

A5.5.6.2. ICD/CDD section 2 (threat summary) and section 9 (intelligence supportability) completed as outlined in the JCIDS manual; a threat summary and intelligence supportability analysis will be completed for all service managed requirements and acquisition programs. *JCIDS will only apply legacy JCIDS programs meeting JCS Memo dated 21 Aug. 2025 continuation criteria. ICD/CDD documents will change with new

requirements processes implemented IAW FY 2024 NDAA Section 811, EO 14265, the SecWar memo dated 20 August 2025, and the JCS Memo dated 21 August 2025.

A5.5.6.3. Completed CIPs.

A5.5.6.4. Completed LMDP.

A5.5.6.5. Threat and Intelligence Certification Memo

A5.5.6.6. Tailored Threat Support Plan (TSP) and threat intelligence tailored to work within modular open systems and digital threads.

A5.6. Threat Support Plan. A Threat Support Plan (TSP) is the primary output of a Space Threat Steering Group (STSG) (see **Attachment 4**). A STSG will be formed for all acquisition programs regardless of the programs acquisition pathway or cost that are determined to be intelligence-sensitive.

A5.6.1. Threat Prioritization. Acquisition Intelligence Analyst (AIAs)-led STSG will determine if a *defense acquisition program* is *intelligence-sensitive*. Threat prioritization will be aligned with DIE assessed threat progression and, to the greatest extent possible, will reflect assessed adversary threat progression and how the assessed threat progression impacts programs mission design (capability). **(T-0)** *See Terms of Reference for threat definition.*

A5.6.2. Threat Capability Warning Matrix. Most stressing threats to mission design and most destructive threats to mission design will be developed and presented in a format that supports acquisition and digital engineering (DE) activities. **(T-1)**

A5.6.3. Critical Intelligence Parameter (CIP). CIP development will follow current DIA guidance. Additionally, CIPs will be submitted into COLISEUM by AIAs for approval/adjudication at the beginning of a program's Initial Capabilities Document (ICD)/Capabilities Development Document (CDD) development as outlined in current CIP guidance. Emerging and disruptive technology affecting a program's CIPs should be well understood by the program's STSG, who should be monitoring CIPs in collaboration with National Space Intelligence Center (NSIC) and other service intelligence production centers as required. **(T-1)**

A5.6.4. Lifecycle Mission Data Plan (LMDP). The LMDP is the program manager's (PM) plan that defines how the capability intends to use intelligence data (ID) required to operate the system. ID can include threat capabilities capability and performance (C&P) data, threat models, electronic warfare (EW), infrared (IR), and other technical data types. Gaps in ID diminish the capabilities of systems and can expose vulnerabilities. AIAs will work with the PM to develop an LMDP before the acquisition program's first Milestone decision point. **(T-0)**

A5.6.5. Modeling & Simulation. Threat modeling requirements for the full lifecycle of the program, to include, but not limited to the purposes of integration into Test & Evaluation (DT, OT and IT), training software, mission planning software, and targeting software will be identified in the LMDP. In accordance with DoDI 5600.01, all threat models used support DoD processes, products, or procedures are required to be validated through the authority of the Director, DIA. AIAs will submit production requirements for all models identified in the LMDP through COLISEUM and will submit waiver requests for non-validated threat models in accordance with CJCSI 3318.01.

A5.6.6. As outlined in DoD and DAF guidance IAW DIAP, only NSIC and partner service intelligence centers are authorized to produce validated red threat models for space and counterspace. Additionally, NSIC will create links between analytic organizations, and enable sharing and the transmission of NSIC produced threat models. **(T-0)**

A5.6.7. STSG ensures the program's KPP/KSA account for emergent threat for legacy JCIDS programs. STSG will evaluate capability solutions ensuring development is aligned with prioritized Key Operational Problems (KOPs) identified by the RRAB.

A5.7. Effective Period and Modification.

A5.7.1. These procedures become effective upon the date of signature on the host document, SPFI 14-411, and will be reviewed every two years. Recommendations for modifying the procedures prior to biennial review may be submitted to the STSG Chair by any member.