AIR FORCE DOCTRINE PUBLICATION 2-0

INTELLIGENCE



U.S. AIR FORCE

01 May 2026

Air Force Doctrine Publication 2-0, *Intelligence*

Table of Contents

Foreword i
Chapter 1: AIR FORCE INTELLIGENCE FUNDAMENTALS 1
NATIONAL POLICY AND GUIDANCE 1
FOUNDATIONS OF INTELLIGENCE PRODUCTION 2
AIR COMPONENT INTELLIGENCE SUPPORT 5
INTELLIGENCE ROLES IN OPERATIONS 7
Chapter 2: COMMAND AND CONTROL, FORCE PRESENTATION, AND ORGANIZATION 10
ROLES AND RESPONSIBILITIES 10
SUPPORT RELATIONSHIPS 15
Chapter 3: INTELLIGENCE PROCESS 18
THE INTELLIGENCE PROCESS 18
PLANNING AND DIRECTION 19
COLLECTION 21
PROCESSING AND EXPLOITATION 24
ANALYSIS AND PRODUCTION 26
DISSEMINATION AND INTEGRATION 30
EVALUATION AND FEEDBACK 31
References 33

FOREWORD

Intelligence is a joint function that serves to provide information, assessments, and estimates to the commanders and their staff to support situational understanding and enable decision-making.

Global Integrated Intelligence, Surveillance, and Reconnaissance (GIISR) is one of the Air Force's Core Functions. ISR is an activity that synchronizes and integrates the planning and operation of sensors, assets, processing, exploitation, and dissemination (PED) systems, and analytic systems or capabilities directly support current and future intelligence operations.

The Air Force Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (AF/A2) is responsible for policy formulation, planning, evaluation, oversight, and leadership of United States Air Force (USAF) global integrated ISR. As the USAF's Senior Intelligence Officer (SIO), the AF/A2 has the authority to collaborate and coordinate with the Under Secretary of War for Intelligence and Security [USW(I&S)] and execute, as delegated, the Secretary of the Air Force's Secretary of the Military Department and Department of War Component Head intelligence responsibilities. As head of the USAF Intelligence Community (IC) element, the AF/A2 coordinates and advocates for USAF ISR capabilities within the Office of the Director of National Intelligence (ODNI).

CHAPTER 1: AIR FORCE INTELLIGENCE FUNDAMENTALS

United States Air Force (USAF) intelligence efforts are guided by a clear hierarchy, flowing from national strategic policy and guidance down to daily operations. The foundation of top-level direction from national security, defense, and intelligence community (IC) standards shapes the organization and prioritization of intelligence forces. From there, this strategic intent is translated into operational practice through specific USAF core functions, such as Global Integrated Intelligence, Surveillance, and Reconnaissance (GIISR).

Intelligence production follows a structured progression, moving from raw data and basic information toward refined assessments and enduring knowledge frameworks. Understanding this progression highlights the essential difference between intelligence as a capability (the processes, people, and systems) and intelligence as a product (the outputs that inform commanders' decisions). Together, these elements form an integrated architecture that aligns national priorities with the execution of the joint intelligence process, ensuring coherence from strategic guidance to tactical application.

NATIONAL POLICY AND GUIDANCE

The President of the United States (US) and the Secretary of War (SecWar) provide strategic guidance for the Department of War (DoW), which directs the prioritization of homeland defense and deterring threats in key regions such as the Indo-Pacific. These strategies create a cascading framework of objectives, priorities, and requirements that flow from the highest levels of national leadership down to the individual analyst and intelligence, surveillance, and reconnaissance (ISR) platform. This alignment ensures a unified effort of national and military intelligence for military operations, linking operational intelligence collection and analysis directly to the nation's strategic objectives.

National Intelligence Strategy (NIS). The Director of National Intelligence's (DNI) strategy calls for a more agile, integrated IC that collaborates across the 18 member agencies and with partners, reinforcing the need for USAF intelligence activities to share data with other services, combatant commands (CCMD), and multinational intelligence partners to inform national decision-making. This emphasizes common standards, data interoperability, and fusion intelligence efforts. The NIS provides the broad IC-wide analytic and workforce priorities and shapes the National Intelligence Priorities Framework (NIPF), framing ***what*** capabilities and adversaries matter most, while the defense intelligence guidance embedded in national defense planning translates those into mission-specific, DoW, and USAF intelligence requirements that shape ***how*** intelligence collection and analysis are conducted daily. This ensures that the USAF's analytic outputs are relevant, timely, and aligned with strategic goals from the President and DNI down to the individual analyst.

Intelligence Community Directives

Intelligence Community Directives (ICDs) are published by the DNI to establish policy and provide definitive direction to the IC (see dni.gov). While numerous directives apply, several directives are foundational to the USAF commander's trust in their intelligence enterprise, such as "ICD 203: Analytic Standards."

Joint Functions. Joint functions are a grouping of capabilities and activities that enable joint force commanders (JFCs) to synchronize, integrate, and direct joint operations. Intelligence is one of seven joint functions along with command and control (C2), information, fires, movement and maneuver, protection, and sustainment. Intelligence provides information, assessments, and estimates to enable decision-making. Intelligence also enables the other joint functions by continuously providing commanders and their staff with a holistic understanding of the operational environment (OE) to inform operational design and planning, intelligence estimates to facilitate plans for future joint military operations, and current intelligence to assess operations in relation to desired effects and objectives.

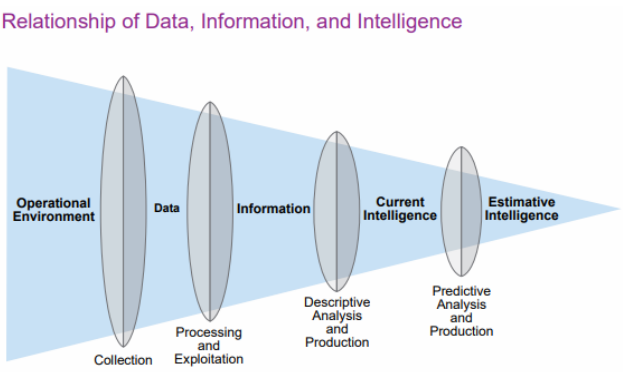
USAF A2's ISR Strategic Vision 2032

USAF A2's ISR Strategic Vision 2032 describes how AF ISR will operate in 2032, with a focus on executing the six Air Force Future Operating Concept (AFFOC) fights, and provides guidance on the strategic resourcing, technology, and human capital choices required to design and develop those forces. AF ISR will provide vital, modern, context-relevant capabilities as a core function of the USAF.

FOUNDATIONS OF INTELLIGENCE PRODUCTION

The production of intelligence at the speed of modern conflict is no longer a matter of simply collecting more data, but of *mastering* the data collected. A deliberate data governance strategy is therefore a prerequisite for any effective intelligence operation. Without it, the immense volume of information from the operating environment remains a chaotic liability rather than a strategic asset. The ultimate goal is to achieve *decision advantage*, which is the ability to make better, faster, and more effective decisions than an adversary. It is gained by accessing superior information, analyzing it more effectively, and acting upon it more decisively.

MASTERING THE DATA-RICH BATTLESPACE FOR DECISION ADVANTAGE



To achieve a decisive edge, military operations aim for decision advantage. This advantage is built on a foundation of information advantage, the culmination of a critical process that transforms raw data into actionable intelligence. Initially, data exists as discrete, unorganized facts such as raw signal intercepts or satellite images. When this data is processed, organized, and given context, it becomes information. Intelligence represents the final, most valuable stage of this progression. It is the product of analyzing information to understand its significance, predict future actions, and identify vulnerabilities. By effectively converting data into information and information into intelligence, a force gains a superior understanding of the OE, enabling the rapid and informed decision-making that is the hallmark of decision advantage.

TAXONOMIES, ONTOLOGIES, KNOWLEDGE MODELS, OBJECTS

Mastering the data-rich environment begins with disciplined organization and standardization at scale. The USAF relies on a structured framework built on taxonomies, ontologies, and knowledge models, which refine raw data into usable intelligence. These components create a common language that enables humans and machines to rapidly interpret, relate, and analyze complex information, accelerating the transformation of data into decision-quality insight.

Proper governance ensures data is discoverable, accessible, and trustworthy, enabling rapid synthesis of intelligence and providing commanders with the sustained decision advantage required to fight and win inside information-dense environments. These distinctions highlight the importance of structured data governance and analytic frameworks.

The USAF intelligence enterprise contributes to the IC by aligning with the Defense All Source Analytic Enterprise (DIAAE) knowledge model for object-based intelligence (OBI) and production (OBP). Successful implementation requires supporting data models and standards, and the Defense Intelligence Core Ontology (DICO) provides a mission-focused framework for organizing defense intelligence data, while the Defense Intelligence Enterprise Knowledge Model (DIEKM), managed by the Defense Intelligence Agency (DIA), serves as the IC model. The DIEKM establishes a uniform structure for organizing information from different sources and domains. It serves as the master blueprint that ensures all intelligence data, regardless of origin, can integrate into a cohesive whole. By standardizing how information is structured, the DIEKM enhances data interoperability, powers machine learning and AI, and enables analysts to access and understand information more efficiently, leading to faster and more accurate intelligence production.

Object-Based Intelligence. OBI is an approach to intelligence analysis that focuses on defining and analyzing specific objects of interest to understand their relationships, vulnerabilities, and potential impact. It is a shift away from traditional methods that often prioritize geographic regions or specific threats. This approach relies on integrating data from diverse sources to build a comprehensive understanding of each object. By understanding object profiles and relationships, analysts can use this form of intelligence to predict future events and potential threats. Changes in object attributes, relationships, or activities can serve as early warnings.[1]

Object-Based Production. OBP is the standardized IC process that organizes data around objects of interest, enabling users to aggregate information across domains and tie it to a specific object. The USAF intelligence enterprise translates this OBP methodology into a mission line known as the disposition of forces (DOF) production process, which supplements theater order of battle and is central to enabling the execution of theater dynamic targets at speed and scale. While both OBI and OBP leverage the concept of "objects," they operate differently and serve distinct purposes. The connection is that they both use a consistent object-based data model.[2] Terms associated with OBP include:

Object. An object is a digital representation of a real-world thing, action, or abstraction. An object is not always a target. Once an object is vetted and validated through the target development process, it may then be designated as a target. In the dynamic targeting process, objects become tracks, and tracks become targets.

Object Management System (OMS). OMS is the application, service, or system-of-systems that enables the production and consumption of information and intelligence within an object-based data construct, aligning all reporting to objects agnostic to the producer or consumer.

Structured Observation Management (SOM). SOM is the method by which geospatial intelligence (GEOINT) observations from satellites, sensors, and other sources are captured, structured, stored, and shared in a standardized format compatible with the OBP. This ensures that GEOINT information can be integrated into the IC's OBP process.

Disposition of Forces (DOF). DOF is the identity, location, activity, and operational status of an object or forces. DOF is informed by the relationships between objects, their assigned garrison locations, and associations to other units, however, the execution of DOF does not cease when objects enter or depart from garrison. DOF provides planners the ability to perform quick queries to provide a dynamic picture of where the adversaries were in the past, where they are going, and where they will be soon.

INTELLIGENCE VS ISR

Intelligence at the operational level equips the commander with the clarity and foresight needed to direct joint forces effectively by informing decision-making, describing the OE in depth, identifying and defining objectives that align with strategic aims, and nominating

[1] For additional information on OBI, see the Air Combat Command's (ACC's) A2 Disposition of Forces (DOF) Concept of Operations (CONOP).
[2] For additional information on OBP, see the ACC DOF CONOP.

those objectives for integration into campaign design. It underpins planning and executing by anticipating adversary actions, synchronizing joint capabilities, and ensuring operations are sequenced to generate decisive effects to achieve the objectives. Simultaneously, intelligence counters enemy deception and surprise while enabling friendly deception efforts that shape adversary perceptions and protect operational intent. Throughout the campaign, it continuously assesses the effectiveness of operations, measuring progress, revealing emerging opportunities, and guiding necessary adjustments to maintain initiative in a dynamic environment.

Intelligence is defined as a product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. It is also the activities that result in the product as well as the organizations that conduct them.

Intelligence, surveillance, and reconnaissance (ISR) are integrated capabilities that collect, process, exploit, and disseminate accurate, timely information to provide the situational awareness necessary to plan and conduct operations. The goal of ISR is to provide precise, timely intelligence to the warfighters and to help the USAF achieve information superiority. ISR activities are how raw data and information are gathered from the OE to answer a specific intelligence requirement.

Intelligence and ISR form a connected but distinct value chain. ISR provides the foundational input: platforms, sensors, and personnel dedicated to collecting raw data from the OE. In its unprocessed state, this data has limited utility for commanders. The intelligence enterprise performs the essential value-added function, transforming that data through exploitation, analysis, and contextualization. The result is intelligence, a refined product that fosters understanding, reduces uncertainty, and enables effective decision-making. This distinction is operationally significant. **Resourcing collection without a proportional investment in analytic capacity produces diminishing returns and fails to generate the decision superiority required to compete and win.**

AIR COMPONENT INTELLIGENCE SUPPORT

Air component intelligence support enables decision advantage for joint and multinational forces through five integrated capabilities: battlespace characterization, collection operations, targeting, production of intel mission data, and intel support to weapon system design and acquisition. These capabilities are delivered to the CCMD or joint task force (JTF) through divisions of an air operations center (AOC).

BATTLESPACE CHARACTERIZATION

The purpose of battlespace characterization is to understand and predict an adversary by examining their capabilities, tactics, dispositions, centers of gravity, and courses of action (COA) within the context of the OE. It is critical for providing indications and warnings, identifying potential vulnerabilities to forces, and identifying opportunities to achieve objectives. The aim of battlespace characterization is to identify what is and is not known by continuously updating and validating assessments. Information gained through

battlespace characterization is a valuable foundation to inform targeting.

COLLECTION OPERATIONS

Collection operations acquire raw data and information about relevant aspects of the OE and provide that information to intelligence processing and exploitation elements. Collection involves tasking and synchronizing ISR sensors, platforms, and exploitation resources to characterize the OE, adversary activities, and infrastructure, and to find, fix, track entities of interest. The aim is to test beliefs, confirm knowledge, and discover intelligence gaps to enhance decision advantage. Collection operations are typically driven by battlespace characterization or targeting requirements.

TARGETING

Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities.[3] Targeting requires a continuous, analytic process to identify, develop, and affect targets to meet commander objectives. Intelligence, including ISR activities to find, fix, track, and target entities, is a critical component of each of the six targeting process steps. Targeting is interdisciplinary and requires the expertise of personnel from many functional disciplines.

Functional Disciplines that Support Targeting

- Strategists and planners bring knowledge of the context and integrated plans.
- Personnel involved in combat operations bring recent experience.
- Intelligence personnel provide analysis of adversary strengths and vulnerabilities and targeting expertise.
- Judge advocates apply the law of war and interpret rules of engagement for mission planning and weapons delivery.

INTELLIGENCE MISSION DATA PRODUCTION

Intelligence mission data (IMD) production is the ability to derive, produce, and rapidly update the intelligence used for programming platform mission systems in development, testing, operations and sustainment to include the following functional areas: signatures, electromagnetic warfare integrated reprogramming, order of battle, characteristics and performance, and GEOINT. The proliferation of information-based weapon systems that require detailed intelligence to operate as designed has significantly increased the need for production and rapid integration of IMD into USAF operations.

INTELLIGENCE SUPPORT TO ACQUISITION

Intelligence support to acquisition and its associated analytical processes enable the acquisition community to impact weapon system design through future threat projections and to capture the intelligence sensitivity of a particular development program. Threat assessments, extending from the current risk out beyond 20 years, include production of System Threat Assessments and System Threat Assessment Reports. Programs also

[3] See JP 3-60, *Joint Targeting*, for additional information.

must be analyzed for intelligence sensitivity to determine if they require intelligence data during development or to perform their mission or require the direct support of intelligence personnel or influence intelligence data at any point in the planning and direction, collection, processing and exploitation, analysis and production, and dissemination cycle. An intelligence supportability analysis will be developed for intelligence sensitive systems.

INTELLIGENCE ROLES IN OPERATIONS

Intelligence is integral to every military operation, but its application is never one-size-fits-all. The character and objectives of a specific mission dictate the focus, tempo, and type of intelligence support required. From the foundational analysis needed for nuclear deterrence to the real-time, tactical insights essential for special operations forces, intelligence personnel and capabilities are expertly tailored and integrated to provide commanders with the specific decision-advantage needed to succeed.

OPERATIONAL UNIT-LEVEL INTELLIGENCE

In support of combat operations, individual unit-level intelligence teams are collectively organized to form the contingency intelligence network (CIN).[4] Wing intelligence personnel form the main teams of the CIN; the combat intelligence cell (CIC), mission planning cell (MPC), and squadron intelligence. The CIN funnels intelligence into and out of a particular wing or organization to support three main functions: mission planning, mission execution, and mission debriefing and reporting.

At the operational level, the CIC interacts with the unit support function inside the AOC's ISR division (ISRD) to gather current intelligence, threat data, and request for information (RFI) responses. They disseminate this information throughout the wing and down to operational squadrons. The MPC provides analysis of possible enemy COA, support to targeting, and timely updates to operational mission planners. Squadron intelligence personnel support specific airframes and communicate relevant intelligence directly to aircrew. The CIN, through the CIC, MPC, and squadron intelligence, keeps the commander and operations crews informed of intelligence that can affect mission execution. Support may include intelligence databases, current threat briefings and training, and assistance with mission planning.

USAF SPECIAL OPERATIONS

USAF special operations are intelligence-intensive and, in some cases, require detailed and tailored intelligence support. Special operations forces (SOF) support tends to rely on organic ISR assets, be less centralized, and focus on tactical intelligence. Intelligence personnel produce detailed, specialized products tailored to the mission, customer, and pace of operation. The sensitivity of SOF missions may constrain the release of post-mission reports. Commanders should report sensitive mission data through special access or routine intelligence channels accordingly.

[4] See Air Force Tactics, Techniques, and Procedures (AFTTP) 3-4.14, *Contingency Intelligence Network,* for additional information.

HOMELAND OPERATIONS

When lawful and authorized to do so, USAF intelligence forces may be tasked to conduct ISR or incident awareness and assessment (IAA) within the homeland. Though similar to ISR, IAA operations are conducted during defense support of civil authorities (DSCA) activities, providing timely and usable information to commanders and local, tribal, state, and federal leaders to save lives, reduce human suffering, and protect property. Though ISR activities may be conducted within the US for homeland defense, IAA is only conducted within the US for DSCA.

Importantly, the laws governing DoW operations in the homeland are different than those that govern overseas operations. These laws place specific restrictions and limitations on the employment or use of military intelligence in the homeland.[5]

NUCLEAR OPERATIONS

Nuclear operations require focused and detailed intelligence that can survive in pre- and post-strike environments. Intelligence provides commanders with information needed to make timely decisions and enables civilian leaders to send clear messages and signals to deter adversaries and assure allies.[6]

CYBERSPACE OPERATIONS

Cyberspace operations that support air operations are usually provided to the air component through reachback and are broken down into three subsets: offensive (OCO), defensive (DCO), and Department of Defense Information Network (DoDIN) operations. Intelligence support to each of these subsets is technologically focused and requires significant technical understanding of the domain. Cyberspace intelligence analysts integrate as closely as possible with cyberspace personnel.

Intelligence for OCO identifies access vectors to gain entry into adversarial target networks, detail target network characteristics, and identify network vulnerabilities for further attack vectors. Intelligence analysts supporting DCO and DoDIN operations consider the perspective of potential adversaries that may attack air component networks to understand threats to those systems, whether from state or non-state actors.[7]

FORCE PROTECTION

Intelligence provides vital support and capabilities to force protection and point defense functions and activities to defeat threats to airfields and air bases and prevent mission degradation. If tasked to defend assets and personnel at air component installations, the air component commander should consider designating organic ISR assets to support the Air Force Office of Special Investigations (AFOSI) counterintelligence (CI) activities.

Force protection forces rely on the unique capabilities of various sensors to develop a comprehensive understanding of the OE and enhance their ability to identify and track

[5] See Air Force Doctrine Publication (AFDP) 3-27, *Homeland Operations,* for additional information.
[6] See AFDP 3-72, *Nuclear Operations,* for additional information.
[7] See AFDP 3-12, *Cyberspace Operations,* for additional information.

potential threats. Intelligence support to force protection operations should identify threats and focus on ways to mitigate or eliminate them. Achievement of JFC and air component commander force protection objectives can be aided by the proper combination of complementary ISR and force protection activities and capabilities.[8]

CONTRIBUTIONS TO LONG-RANGE KILL CHAINS

Long-range kill chains are becoming essential for future conflicts because adversaries are investing in anti-access and area-denial systems, long-range fires, and distributed operations that demand we sense, decide, and act from far beyond traditional engagement distances. As threats grow more mobile, more concealed, and more geographically dispersed, the ability to execute a seamless chain of sensing, sense-making, and engagement across domains becomes the only way to maintain decision advantage. Future fights will unfold at machine speed, over vast distances, and under constant threat of disruption, which means forces should be able to detect targets early, validate them with confidence, and pair them to the right shooter without delay. As the force moves toward more contested, multi domain environments, the integration of advanced ISR, resilient C2, and precision fires makes long-range kill chains not just useful, but foundational to deterrence and combat credibility.

Long-range kill chains function when the strategic, operational, and tactical levels of intelligence operate as a single, synchronized enterprise. Long-range engagements demand rapid cycles of sensing, sense-making, and shooting, and none of those phases can succeed in isolation. The DCGS provides the fused intelligence picture and manages the theater's DOF, the AOC ISRD transforms that picture into operational direction, tasking, and timing, the IC supplies the global context, strategic warning, and specialized expertise that sharpen every decision. Together, they create a seamless architecture where sensors are positioned deliberately, targets are validated with confidence, and shooters receive precise, time-dominant intelligence. Without this triad working in concert, long-range kill chains would be slow, fragmented, and vulnerable to adversary disruption.

[8] See AFDP 3-10, *Force Protection,* for additional information.

CHAPTER 2: COMMAND AND CONTROL, FORCE PRESENTATION, AND ORGANIZATION

Air component intelligence forces provide the foundation for a commander's ability to understand, anticipate, and shape the OE. They generate decision-quality intelligence, integrate seamlessly with joint and IC partners, and execute a spectrum of activities that include indications and warning, targeting, characterizing the threat environment, performing collection, and assessment. These forces operate through a mix of assigned and attached elements, with authorities and support responsibilities shifting based on command relationships. Their effectiveness is amplified through robust support networks, federated production centers, national level agencies, and other reachback organizations. These extend analytic capacity and ensure the air component maintains a persistent, comprehensive understanding of the adversary.

ROLES AND RESPONSIBILITIES

Command relationships delineate the degree of authority commanders have over forces. Understanding these authorities and how they fit into the planning and direction portion of the intelligence process is critical for intelligence operations.

DEPARTMENT OF WAR

The SecWar apportions national, strategic, and theater ISR assets to best meet all CCDR requirements. Approved apportionment decisions are delivered to the joint force in a monthly allocated directive (MAD), which identifies assets, units, and sortie rates for that theater. These allocation tables are then used to identify what ISR assets are available for tasking, which ultimately supports the development of the ISR Operations Strategy.

COMBATANT COMMANDER

A combatant commander (CCDR) employs assigned and attached intelligence forces to achieve national and theater objectives. When additional forces are required, CCDRs submit a request for forces (RFF) through the global force management (GFM) process. When authorized, CCMDs may also coordinate to enable the cooperative use of assets not regularly assigned to them to improve coverage. Based on guidance and direction from the CCDR, intelligence (J2) and operations (J3) staffs develop an overall theater collection strategy and posture to execute intelligence operations.

The CCDR establishes priorities for intelligence operations that align with national and theater objectives and ensures theater planning efforts support the fulfillment of crisis intelligence requirements. High-priority, time-sensitive requirements are identified and pre-validated by the JFC for the air component commander to consider for dynamic retasking during the execution of intelligence operations. When theater requirements exceed the capacity of assigned and attached forces, the JFC or air component commander may submit requests for additional ISR capabilities (personnel, platforms) through the CCMD. Taskings involving ISR assets supporting more than one JFC are coordinated and deconflicted by a common superior commander.

The CCDR may delegate operational control (OPCON) or tactical control (TACON) over theater ISR assets to appropriate subordinate commanders. However, the CCDR retains the authority to validate and prioritize requirements for collection by theater ISR assets. At the theater level, CCDRs exercise collection management authority (CMA) for collection operations within their area of responsibility (AOR).[9]

Collection Management Authority (CMA). CMA is the authority to establish, prioritize, and validate theater collection requirements, establish sensor tasking guidance, and develop theater-wide collection policies. Commanders exercising OPCON over intelligence forces may assume CMA of tasked ISR assets as part of the delegation of authority. The theater J2 usually retains CMA to validate, modify, or non-concur theater intelligence requirements through the CCDR's joint intelligence operations center (JIOC).

CMA usually includes the authority to task geospatial-intelligence sensors and lower-echelon signals intelligence (SIGINT) collection systems with more localized collection capabilities. The National Security Agency (NSA) retains CMA over strategic-capable SIGINT ISR systems. In addition, CCDRs may request, and subsequently receive, temporary SIGINT operational tasking authority (SOTA) over theater-wide capable platforms and sensors. The delegation of SOTA to a CCDR and subsequent delegation of this authority to the JFC ensures the theater can prioritize requirements and focus SIGINT collection where needed to carry out assigned missions. Collection management includes two complementary functions: collection requirements management (CRM) and collection operations management (COM).

- **Collection Requirements Management (CRM).** CRM is the authoritative development and control of collection, processing, exploitation, and information reporting requirements. CRM defines what intelligence systems should collect.

- **Collection Operations Management (COM).** COM is the authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and information reporting resources. The COM process specifies how to satisfy the requirement and provides details on how the collection occurs.

The CCDR's staff is responsible for developing a collection strategy and execution posture for ISR missions and coordinating with national agencies. The theater J2 reviews, validates, and prioritizes all outstanding intelligence requirements, whether originating with the J2 staff or subordinate components. In conjunction with component staffs, the JFC's staff is responsible for developing a shared production architecture that leverages reachback, distributed, and federated partners for intelligence exploitation and analysis. This shared production architecture also leverages support from organic capabilities at the component and JTF levels, the Services, other CCDRs, foreign partners, and national agencies. This helps maximize coverage of intelligence requirements.

Control of Assets vs Control of Intelligence. A critical distinction for commanders at all echelons is the separation of authority between controlling an ISR asset and control of the intelligence it gathers. The CCDR's delegation of OPCON and TACON over an ISR

[9] For additional information on collection management, see JP 2-0, *Joint Intelligence*.

asset provides the subordinate commander with authority over the platform's employment, but it does not automatically grant authority over the raw intelligence it collects. SIGINT serves as a primary example. Regardless of the air component platform collecting the data (e.g., MQ-9, RQ-4, RC-135V/W), the raw SIGINT is owned by and routed through the NSA for processing, exploitation, and dissemination (PED).

With any command relationship involving intelligence forces, care should be taken to know, understand, and align with the appropriate authorities. Intelligence and intelligence-related activities must be conducted in accordance with DoDD 5240.01, applicable laws, Executive Orders, including EO 12333, as amended, Presidential Directives, DoDD 5148.13, DoD Manual (DoDM) 5240.01, Secretary of War memoranda and other DoW policies, and applicable DoW and DAF policies implementing ICDs.

Joint Intelligence Operations Center (JIOC). Each CCMD and some subordinate unified commands have assigned JIOCs to integrate intelligence capabilities in support of their mission. The JIOC supports joint planning and conducts intelligence operations in support of the CCDR and staff, subordinate component commands, and JTFs. The JIOC integrates intelligence from external DoW and national intelligence organizations, Partner Nations, and law enforcement to ensure accurate, timely, and complete intelligence is available to support CCMD joint planning, execution, and assessment.

AIR COMPONENT COMMANDER

The USAF organizes, trains, and equips forces to be an air component to a CCDR. The air component commanders' administrative authorities are derived from Title 10 and exercised as the COMAFFOR. The air component commander's operational authorities are delegated by the CCDR and exercised as both the COMAFFOR, and as the Joint Forces Component Commander (JFACC), over joint air forces made available for tasking.[10]

The air component commander is typically the supported commander for theater ISR and is often delegated OPCON for assigned or attached airborne ISR assets as well as serving as the principal agent for executing COM in accordance with CMA. To prevent CCMD J2 from overstepping its authority, clear distinction is drawn between the strategic oversight of the CCDR and the tactical execution of the JFACC and ISRD. The CCDR often retains CRM, but as the supported commander for theater ISR, the air component commander leverages the AOC to integrate CRM and COM.

USAF Service Component Intelligence (A2). The air component commander's A2 guides Service component intelligence forces by recommending policy and guidance and ensuring coordination among various intelligence functions. The A2's dedicated intelligence manpower is provided within the AOC and Air Force forces (AFFOR) staff. The A2 is responsible for intelligence plans and programs, sensitive compartmented information management, intelligence liaison, foreign disclosure, and intelligence information management functions. The A2 is responsible for intelligence support to the air component commander and assigned or attached Service component forces. This

[10] For additional information on commander, Air Force forces and JFACC, see AFDP-1 *The Air Force*.

includes the following:

- Serves as the Service component SIO. Advises the air component commander on all intelligence matters impacting mission accomplishment.
- Recommends USAF intelligence policy and guidance for operations within the joint operations area in coordination with the JFC J2.
- Establishes, coordinates, and monitors Service component intelligence requirements and capabilities to support operations.
- Coordinates and monitors JFC intelligence requirements.
- Coordinates with the JFC staff to establish joint and foreign partner relationships governing federated intelligence operations and distributed operations in theater.
- Validates unit intelligence and systems requirements and manages fielding and operation of automated intelligence systems.
- Participates in contingency planning processes and development of Service annexes to contingency plans, operational plans (OPLANs), planning orders, and operation orders.
- Assists the USAF Service Component Operations, Plans and Requirements (A3/5) in developing the air component commander's critical information requirements (CCIRs) and ensures the CCIRs are communicated to the J2 for action.
- Plans and develops instructions to implement wartime intelligence support, including augmentation of joint forces.
- Plans intelligence architecture support to satisfy Service-specific weapon system employment requirements in accordance with OPLANS.
- Establishes procedures for and manages theater production requests and RFIs.

ASSIGNED AND ATTACHED AIR COMPONENT INTELLIGENCE FORCES

Air Force Intelligence Forces. USAF intelligence forces are normally presented to JFCs through an AOC or air expeditionary task force (AETF) structure. USAF intelligence forces are sometimes employed in support of other components through joint expeditionary taskings. These taskings are Service-specific and allocated based on requests for forces submitted by a CCDR. Similarly, the USAF conducts many peacetime intelligence operations in support of CCMDs or interagency customers that do not support a JTF and do not fall under an AETF construct. When Airmen are tasked to augment another Service, the AETF model should be applied as a template.

Most USAF ISR assets are considered high-demand, low-density (HD/LD) and are often tasked to perform a range of missions across the globe. The Joint Staff coordinates with the military departments/services, CCDRs, and intelligence agencies to identify and recommend joint global platform- and sensor-based ISR along with associated PED

capability sourcing solutions. Some assets may be theater assigned. When emergent requirements exceed the capabilities or capacity of assigned forces, SecWar can allocate additional forces to CCMDs through the Global Force Management Allocation Plan (GFMAP). For both assigned and allocated forces, SecWar specifies the command relationship authorities.

Intelligence, Surveillance, Reconnaissance Division (ISRD). The ISRD, in conjunction with the other AOC divisions, plans and executes airborne ISR operations and provides combat ISR support to air component planning, execution, and assessment activities. The ISRD serves as the central node and fusion center for all air component intelligence operations. Its primary mission is to provide the air component commander an understanding of the adversary and the OE. The ISRD is fundamentally responsible for orienting the commander to enemy capabilities, threats, and COG by directing and managing the air components intelligence operations. It accomplishes this by seamlessly integrating intelligence functions, including analysis, collection management, and targeting support within the air tasking cycle. Key responsibilities include producing a common intelligence picture for all staff, providing IPB, managing the targeting process from target development and nomination to post strike battle damage assessment (BDA), and re-strike recommendations.

- **Analysis.** Within the ISRD, analysis functions support the joint intelligence preparation of the operational environment (JIPOE), intelligence preparation of the battlespace (IPB),[11] and developing assessments that enhance friendly understanding of the OE and adversary intentions and behaviors. Intelligence analysts synthesize intelligence and data, apply critical thinking, identify, assess, and fill intelligence gaps, and conduct predictive analysis. This is primary coordinated through the Analysis, Correlation, and Fusion Team.

- **ISR Operations and Collection Management.** The ISR operations team conducts collection management for theater airborne ISR requirements, planning theater airborne ISR operations, and associated PED. The ISRD is the optimal entity for COM of theater airborne ISR operations. To ensure ISR operations align with air component commander objectives, intelligence operations planners and collection managers attend joint collection working groups and management boards to advocate for air component collection priorities based on PIRs, RFIs, targeting requirements, and other intelligence needs.

- **Target Development and Battle Damage Assessment.** The ISRD is responsible for target development and battle damage assessment (BDA) primarily done through the targeting and tactical analysis team. Target development includes evaluating and nominating potential adversary targets based on commander's guidance and intended effects. In addition, BDA facilitates reporting on physical and functional damage and change assessments post-strike. The ISRD also supports munitions

[11] The term intelligence preparation of the battlespace has been removed from the DoD Dictionary. Content related to the term has been moved to the *Joint Guide for Joint Intelligence Preparation of the Operational Environment*.

effectiveness assessments and restrike recommendations.

- **Unit Support.** The ISRD provides USAF unit support by liaising with wing-level CINs. Unit support functions include oversight of theater intelligence reporting procedures, the RFI process, and additional unit intelligence requirements. These functions include receiving and processing mission reports and RFIs from USAF units.

Air Expeditionary Task Force (AETF). The AETF is the USAF's primary warfighting organization and how the USAF presents forces to a JFC. The AETF presents a JFC with a task-organized, integrated package that balances force, sustainment, control, and force protection. When established, AETFs usually stand up under the designated USAF component-numbered air force (C-NAF) headquarters and coordinate with the air expeditionary wings.[12]

Air Expeditionary Wing (AEW). Intelligence forces within the AEW are organized to provide the wing commander with a comprehensive understanding of the OE, enabling effective mission generation. This role is executed through the wing's intelligence SIO, which manages the Contingency Intelligence Network (CIN) comprised of the Combat Intelligence Cell (CIC), Mission Planning Cell (MPC), and squadron level intelligence elements. These forces are responsible for mission planning, executing, and debriefing, and ensuring that aircrew are equipped with timely and accurate threat data. They serve as the conduit between the theater AOC ISRD and the wings' tactical operators, disseminating threat warnings, managing RFIs, and providing intelligence support crucial for force protection and agile combat maneuvers.[13]

SUPPORT RELATIONSHIPS

Air component intelligence operations are critically dependent on a robust network of external support, primarily through reachback. Reachback is the process of obtaining products, services, applications, forces, equipment, or material from organizations that are not forward deployed. This structure is essential as forward deployed intelligence elements often have limited organic, analytical, and collection capabilities.[14]

UNITED STATES AIR FORCE

Deputy Chief of Staff of the Air Force for ISR (AF A2). The Deputy Chief of Staff of the Air Force for ISR Operations (AF A2) is the Service's head of the intelligence community element (HICE) and senior intelligence officer (SIO). AF A2 represents the USAF to the national IC (NIC) and is the principal USAF advisor to national and DoW executives for programs and capabilities integration. As the USAF HICE, AF A2 is responsible for leveraging and integrating USAF and national capabilities, collaborating with allies and partners, developing intelligence foreign disclosure policy, disseminating intelligence sharing guidance, intelligence analysis, targeting tradecraft, and data standards policy, formulating the USAF ISR strategy, and establishing the necessary linkages between

[12] For additional information on the AETF structure, see AFDP 3-0, *Operations.*
[13] For additional information on the CIN, see AFTTP 3-4.14.*CIN.*
[14] For additional information on reachback, see JP 3-30, *Joint Air Operations.*

planning and execution to integrate USAF and IC capabilities.[15]

Air Combat Command (ACC). ACC provides combat-ready intelligence forces, support, and equipment to CCMDs when directed. ACC meets this responsibility as the ISR global force manager and the lead Major Command (MAJCOM) for managing and modernizing numerous ISR capabilities. These ISR capabilities include the geospatial intelligence, cyberspace intelligence, science and technology intelligence, measurement and signature intelligence, signals intelligence, and all-source analysis, targeting, and associated intelligence products.

Sixteenth Air Force (16 AF). Subordinate to ACC, 16 AF is the principal Numbered Air Force (NAF) for organizing, training, and equipping intelligence personnel to execute ISR responsibilities in support of CCMDs and combat support agencies. The USAF intelligence enterprise retains the preponderance of military manpower within 16 AF subordinate wing-level intelligence organizations to provide services to all theaters.

Air Force Wing-Level Intelligence. USAF intelligence at the wing level through their subordinate squadrons provides a comprehensive spectrum of support, delivering critical analysis and production that spans every level of warfare. At the strategic level, service intelligence centers produce foundational intelligence on adversary capabilities and future threats, informing national policy, long-term defense planning, and weapon system acquisition. This strategic foundation enables the operational efforts of other specialized intelligence wings, which provide direct support to air component and joint force commanders through missions like real-time ISR analysis, precision targeting, and cryptologic operations. This support is further refined at the tactical level, where intelligence personnel organic to flying wings and squadrons provide direct mission planning, threat analysis, and debriefing for aircrews. This unit-level function ensures warfighters have an immediate, detailed understanding of the environment and adversary actions relevant to their specific sorties.

Many of the intelligence wings function as service-retained forces, meaning they are managed and allocated by the USAF to support joint force requirements. Through the GFM process, ACC works with component commanders to align intelligence manpower against their most pressing analytical and targeting needs. This support is formalized through specific tasking orders, such as the Analytic Support Tasking Request Order (ASTRO) for analytical efforts, or the Targeting Support Tasking Request Order (TSTRO) for targeting needs. This model allows the USAF to retain stewardship of its specialized intelligence capabilities while ensuring they remain responsive to the needs of the warfighter.

[15] For additional information on Air Force Intelligence policy, see Department of the Air Force Manual (DAFMAN) 14-401, Intelligence Analysis And Targeting Tradecraft/Data Standards.

INTELLIGENCE COMMUNITY SUPPORT



The USAF is one of the eighteen members of the IC. Air component intelligence integrates both foundational and operational products, fusing long term analytic baselines with time-sensitive reporting. This integration ensures commanders benefit from the depth of national level expertise and the immediacy of operational intelligence, enabling more accurate assessments, faster decisions, and more effective employment of airpower. The USAF intelligence enterprise works with all IC partners across the competition continuum.

CHAPTER 3: INTELLIGENCE PROCESS

THE INTELLIGENCE PROCESS

The joint intelligence process provides the basis for common intelligence terminology and procedures. It consists of six interrelated categories of intelligence operations and serves as a comprehensive framework to guide intelligence activities of the joint services and broader IC. This joint process feeds analytical efforts via the joint intelligence preparation of the operational environment (JIPOE), a four-step analytical process used by joint intelligence organizations to produce estimates and other intelligence products in support of the JFC's decision-making process. In contrast to JIPOE, Services use the intelligence preparation of the battlespace (IPB). IPB mirrors the four-step process of JIPOE, but differs in the purpose, focus, and level of detail. Service component intelligence personnel provide force specific, detailed analysis via IPB that supports component operations and complements the broader JIPOE. The USAF intelligence enterprise contributes to every step of the JIPOE, IPB, and the joint intelligence process. The USAF is the only service to refer to the joint intelligence process as an acronym (PCPADE).[16]

Planning and Direction. Planning and direction set the foundation for the entire intelligence process. Leaders identify what they need to know, establish priorities, and issue guidance that shapes all subsequent intelligence activities. This phase ensures that limited resources are focused on the most important questions, aligning intelligence efforts with operational goals and strategic objectives.

Collection. Collection involves gathering raw information from a wide range of sources: human, signals, imagery, open source, and more. The goal is to acquire relevant data that can answer the requirements established during planning. Effective collection balances speed, accuracy, and risk while ensuring coverage across all required domains.

Processing and Exploitation. Once information is collected, it must be converted into usable form. Processing and exploitation include translating, decrypting, organizing, and filtering raw data so analysts can work with it. This step transforms large volumes of unrefined material into structured information, enabling the identification of patterns, anomalies, or actionable details.

Analysis and Production. Analysts evaluate processed information, integrate data from multiple sources, and produce assessments that explain what is happening and why it matters. They apply critical thinking, contextual knowledge, and analytic methodologies to turn information into insight. The final products: reports, briefings, and estimates, providing decision-makers with clear, relevant, and timely intelligence.

Dissemination and Integration. This phase ensures intelligence reaches the right people at the right time and is incorporated into planning and operations. This includes distributing reports, coordinating with partners, and maintaining feedback loops to refine

[16] For additional information on the joint intelligence process, see JP 2-0 Joint *Intelligence*; to review the steps and differences between JIPOE and IPB, see the *Joint Guide for Joint Intelligence Preparation of the Operational Environment*.

intelligence.

Evaluation and Feedback. Evaluation and feedback are continuous, collaborative parts of the intelligence process involving planners, collectors, analysts, and consumers. This ongoing dialogue aims to identify and correct deficiencies, such as by re-tasking a sensor or revising a report, to ensure intelligence requirements are met.

PLANNING AND DIRECTION

Air component intelligence plays a pivotal role in meeting the CCDR and JFACC's most pressing information needs, as formally expressed in Commander Critical Information Requirements (CCIRs). The subset of these requirements related to the adversary and the OE are known as priority intelligence requirements (PIRs), and they serve as the primary drivers for all intelligence activities. To effectively answer these high-level PIRs, the intelligence enterprise breaks them down into more specific, manageable questions called essential elements of information (EEIs). These EEIs guide the detailed planning and execution of intelligence collection and analysis. When an intelligence question cannot be answered with organic assets or available information, the formal RFI process is initiated, tasking the broader IC to leverage its vast resources. This process ensures that the entire intelligence apparatus, from tactical collection assets to national level analytical centers, is synchronized and focused on providing the specific intelligence the commander needs to make critical decisions.

Commander Critical Information Requirements (CCIR). Owned by the commander, CCIRs are composed of PIRs and Friendly Forces Information Requirements (FFIR). To focus the staff and prioritize resources on information that directly impacts the commander's decision.

Intelligence Requirement (IR). Any subject, general or specific, upon which there is a need for the collection of information or the production of intelligence. Results in RFI, a collection requirement (CR), or a production requirement.

Priority Intelligence Requirement (PIR). Owned by the commander but developed by the staff. The intelligence component of commander's CCIRs focused the employment of limited intelligence assets and resources against competing demands for intelligence support. These are used to drive intelligence collection and analysis against the most critical adversary related knowledge gaps. These are the foundation of the ISR strategy.

Essential Elements of Information (EEI). Produced by intelligence staff, these are the most critical information requirements regarding the enemy or adversary, and the environment needed by the commander at a particular time, to be used in conjunction with other relevant information and intelligence to assist in reaching a logical decision. These translate the commanders' broad questions into specific questions for tasking assets and analysts.

Request for Information (RFI). Produced by any staff element, these are any specific, time-sensitive, ad hoc requirements for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled

intelligence production. They are normally the action oriented mechanism for seeking answers to EEIs and other information needs from the intelligence enterprise.

Collection Requirement (CR). A valid need to close a specific gap in intelligence holdings in direct response to a RFI.

Production Requirement (PR). An intelligence requirement that cannot be met by current analytical products, resulting in tasking to produce a new product that can meet this intelligence requirement.

SUPPORT TO THE AIR PLAN

Joint Planning Process for Air (JPPA). JPPA is driven by clearly defined information requirements, and intelligence is the element that gives those requirements meaning. JPPA translates the JFC's strategic aims into executable operational airpower, and intelligence underpins every decision within that process. Intelligence professionals are embedded throughout, ensuring commanders and planners understand the adversary, the environment, and the opportunities and risks inherent in each COA.[17]

Intelligence analysts enter planning with a detailed understanding of the adversary's capabilities, vulnerabilities, order of battle, decision-making processes, and likely/most dangerous COA. This understanding shapes the commander's operational approach and informs the development of feasible, acceptable, and effective airpower options. **All source analysts** develop the adversary picture, assess intent, identify critical vulnerabilities, and anticipate adversary reactions across the range of potential friendly actions. **Collection strategists** integrate sensor capabilities into planning by recommending collection allocations, conducting feasibility assessments, estimating ISR gain-loss, and ensuring alignment with component requirements and available capabilities. **Targeting strategists** guide the development of the operational targeting strategy, ensuring target systems are understood, desired effects are achievable, and analyst teams can match the right targets to the commanders' objectives. Together, these intelligence roles ensure that JPPA is grounded in a realistic understanding of battlespace and that airpower options are aligned with both strategic aims and operational realities.

Normally developed by the AOC Strategy Division (SRD) or air component A5, the joint air operations plan (JAOP) is the comprehensive plan that translates the JFC and JFACC guidance into a coherent strategy of the air, and cyberspace operations. The ISR operations strategy is a key component of the JAOP, ensuring that collection and analysis are synchronized with theater and national efforts to support the overall campaign.[18] The AFFOR A2 staff provides intelligence inputs to the operations order (OPORD), which identify forces, functional support, and resources and their flow into theater in support of the mission. Both documents include Annex B, developed by ISR strategists and planners, which details how intelligence will support the larger air plan, and identifies critical obstacles and shortfalls. Both plans follow the standard "SMEAC" format. These planning efforts culminate in operational directives and strategies such as the Air

[17] For additional information on JPPA, see AFDP 5-0 *Planning*.
[18] For additional information about the JAOP, see JP 3-30, *Joint Air Operations*, and AFDP 5-0, *Planning*.

Operations Directive (AOD), ISR Operations Strategy, and ISR Allocation Plan.

Air Operations Directive (AOD). The AOD is a near-term directive that translates the broader JAOP into daily operational guidance for the air tasking order (ATO). It refines and prioritizes operational tasks, including specific guidance for ISR operations. The AOD details the JFACC's intent for a specific ATO or time period, lists PIRs, specifies employment of certain ISR platforms and intelligence disciplines (INTs), and provide PED guidance.[19] This guidance is crucial for the daily development of the ISR plan, including the component prioritized collection list (CPCL) and the final reconnaissance, surveillance, and target acquisition (RSTA) Annex.

ISR Operations Strategy. The air component ISR strategy is driven by overarching J2 guidance and priorities, and commander PIRs help focus this effort. ISR strategists integrate a wide range of capabilities into the plan: national, theater, and other service platforms, and understand the PED architecture. Strategists also work with AFFOR staff planners to identify platform, sensor, PED, communications availability, force flow, timing, bed down, and sustainment matters. Other components' tasks have implications for the air component's ISR capabilities, so ISR shortfalls and limitations with broad implications for the joint force should be communicated clearly and early in venues such as the joint collection working group (JCWG) or joint collection management board (JCMB).

ISR Apportionment and Allocation Plan. Air apportionment is the determination and assignment of the total expected effort by percentage and/or by priority that should be devoted to various air operations for a given period of time. The JFACC apportions air to the CCDR or JTF, who serves as the approval authority. Air allocation is the translation of the air apportionment decision into the total number of sorties or missions by weapons system type available for each operation or task.

COLLECTION

Collection operations acquire raw data about the OE and provide it to intelligence processing elements. This involves the detailed tasking and synchronization of ISR sensor platforms and exploitation resources to characterize the OE, adversary activities, and infrastructure, and to support the targeting cycle. The overarching purpose of collection operations is typically driven by the need for battlespace characterization, targeting, test assumptions, confirm knowledge, identify intelligence gaps, and enhance the commander's decision advantage. This is done through collection management, which is the process of converting intelligence requirements into collection requirements (CRs), establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required.

Collection operations orchestrate three distinct but related functions: collection management authority (CMA), collection requirements management (CRM), and collections operations management (COM). At the operational level, the ISRD is central to this process and is considered the most suitable entity for conducting COM for theater

[19] For additional information on AOD, apportionment, and ISR Strategy in the AOC, see AFTTP 3-3, *AOC.*

airborne ISR. Chapter 2 included discussion about CMA, CRM, and COM.

COLLECTION PRIORITIZATION

Component Prioritized Collection List (CPCL). The ISRD is responsible for developing the JFACC's CPCL. This list includes collection tied to target nominations and other CRs from various entities within the AOC and subordinate units. These component CPCLs are coordinated with the theater J2 collections team via a JCWG, then consolidated into a draft joint integrated prioritized collection list (JIPCL), which aligns with component target nominations.

Joint Collection Working Group (JCWG). The JCWG is the primary forum used by a Joint Force Commander's staff to synchronize and prioritize intelligence collection requirements from all subordinate components. The group deconflicts competing requests for limited ISR capabilities and develops the draft joint integrated prioritized collection list (JIPCL) to task these assets effectively.

Joint Integrated Prioritized Collection List (JIPCL). The JIPCL is a comprehensive, prioritized list of all CPCL CR that guides the tasking of both theater and national ISR assets. This consolidated list is then presented at the JCMB and approved by the theater J2.[20] The purpose of the JIPCL is to integrate with the joint integrated prioritized target list (JIPTL).

Joint Collection Management Board (JCMB). The JCMB is a key body that oversees and coordinates intelligence collection activities across a joint force, serving as the senior review for the joint collection working group (JCWG). It resolves conflicts in collection priorities, ensures efficient use of ISR assets and formalizes the JIPCL.

Reconnaissance, Surveillance, and Target Acquisition (RSTA) Annex. The RSTA serves as the ISR annex to the ATO. Managed by the ISRD, the RSTA synchronizes and directs the employment of all available ISR assets from national systems to theater and tactical platforms to collect information that answers the commanders' PIRs and fills critical intelligence gaps. The data gathered through RSTA missions feeds PED activities, where it is transformed into actionable intelligence. To build the RSTA, the ISRD coordinates with the theater J2 staff to determine asset availability, evaluates sensors using the AFAT methodology (access, fidelity, accuracy, timeliness) for imagery or signals requirements, and supports targeting and BDA priorities.

COLLECTION PLATFORMS

Airborne Systems. Airborne ISR platforms provide commanders with a taskable and often visible presence, capable of collecting and disseminating large volumes of real-time information across a wide area. To mitigate threats or political sensitivities, these platforms may operate in a standoff capacity, which can limit the range and depth of sensor coverage. A critical consideration for all airborne ISR is the significant PED support required to turn collected data into usable intelligence, which can be

[20] For additional information on JIPCL, see JP 2-0 Joint *Intelligence*.

accomplished via reachback to specialized ground stations.

When dedicated ISR assets are insufficient, planners should integrate non-traditional ISR (NTISR) platforms, such as strike aircraft, to supplement collection. This tactic, sometimes called operations reconnaissance (ops recce), leverages the advanced sensors on multi-role aircraft to increase battlespace awareness. The successful use of NTISR requires clear, pre-defined mission authorities that distinguish between aircraft control, which remains with the pilot-in-command, and the separate authorities for sensor control and sensor tasking. This ensures that even when an aircraft is performing multiple roles, the C2 of its intelligence collection function is unambiguous and effectively integrated into the broader ISR plan.

Space-based Systems. Space-based intelligence systems are integral to modern military operations, offering the primary advantage of persistent, wide-area coverage over denied areas where airborne or ground assets cannot operate. Their longevity and reduced vulnerability provide commanders with critical information to assess situations and develop plans. However, these systems are a limited resource, as demand often exceeds capacity, and their orbital mechanics can create coverage gaps. Furthermore, they can be susceptible to adversary denial and deception techniques, necessitating a clear understanding of their capabilities and limitations during planning.

The US employs a variety of military, national, and non-military space systems to support its objectives. Military and national satellite systems, controlled by the DoW and IC respectively, provide a broad range of capabilities from environmental monitoring to detailed imagery intelligence. Access to these high-demand assets requires detailed justification and must be coordinated well in advance through the appropriate command channels. To augment these limited resources, commanders can also leverage non-military systems, including allied or commercial assets, though access often requires pre-negotiated legal arrangements that should be established prior to the start of operations.

Ground-based Systems. Ground-based intelligence systems are critical components of the collection architecture, tasked worldwide to gather information for disciplines such as SIGINT and Measurement and Signature Intelligence (MASINT), fulfilling national, theater, and local requirements. These systems include air surveillance and target acquisition radars, which, while primarily for air control, also provide valuable threat warning within designated areas. However, these radar systems are limited by atmospheric conditions, electronic jamming, and line-of-sight constraints.

Beyond tactical air surveillance, significant ground-based ISR resources are dedicated to missile warning and space surveillance. Ground-based missile warning sensors primarily identify and characterize ballistic missile attacks, while also contributing to space surveillance. The Space Surveillance Network (SSN) actively tracks and characterizes artificial objects in space, providing crucial data on adversary space order of battle, overflight warnings, and spacecraft status. This information offers theater commanders early warning and supports denial and deception efforts against potential threats.

Cyberspace-based Systems. Cyberspace-based ISR capabilities are integral to military forces and enable operations across the competition continuum. Cyberspace-focused ISR includes digital network analysis and intelligence support to USAF cyberspace missions. Additionally, specialized units provide timely and actionable all-source ISR services and products supporting national cyberspace operations. This support is generally characterized by five cyberspace focused ISR areas: current intelligence and reporting, indications and warning, threat attribution and characterization, JIPOE, and computer network exploitation under national intelligence and US Cyber Command authorities.[21]

PROCESSING AND EXPLOITATION

Intelligence collection operations are executed through several core intelligence disciplines, each employing unique methods and platforms to acquire raw data from a specific domain. Each discipline has an IC and DoW functional manager. Air component intelligence should coordinate upward with the JTF J2 through the CCMD J2 to IC agencies to ensure collection elements use appropriate reporting methods with a response time sufficient to meet air component commander requirements.[22]

GEOSPATIAL INTELLIGENCE (GEOINT)

GEOINT is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on or about the Earth. GEOINT consists of imagery, IMINT, and geospatial information. GEOINT data sources include commercial satellites, government satellites, aircraft, maps, commercial databases, census information, global positioning system waypoints, and utility schematics. GEOINT can synthesize intelligence and data into conceptualized geographic spatial content that can provide commanders key operational intelligence (e.g., best vantage point for shooters, most advantageous entry points, and spatial trends and patterns). The National Geospatial Intelligence Agency (NGA) serves as the IC and DoW functional manager for GEOINT.

IMINT is the technical, geographic, and intelligence information derived through interpreting or analyzing imagery and collateral materials. IMINT includes the exploitation of imagery data derived from electro-optical, radar, infrared, multi-spectral, and laser sensors. IMINT results from the processing and exploitation of raw imagery (information) to create an analyzed product (intelligence). IMINT is used for historical comparisons, to locate adversary military forces and facilities, and to provide insight into the adversary's capabilities. IMINT is also valuable for understanding the physical terrain and human aspects like significant cultural sites (e.g., government structures, historical sites, and schools), agriculture and urban infrastructure, water, and electrical grids. The air component should leverage the imagery support element (ISE) specialty team in the ISRD for imagery production, tailored analysis, and/or exploitation.

[21] For additional information on collection platforms, see joint publication JP 2-0, *Joint Intelligence*.
[22] For additional information on planning, executing, and assessing various intelligence disciplines, see AFTTP 3-2.88, *ISR Optimization*.

HUMAN INTELLIGENCE (HUMINT)

HUMINT is an intelligence collection discipline that uses people in an area of interest to identify or provide insight into adversary plans and intentions, research and development, strategy, doctrine, and capabilities. Dedicated HUMINT collectors amplify, clarify, or verify information collected by other airborne, ground-based, or space-based assets. In many cases, HUMINT may be the best source regarding adversary intentions. The USAF has an organic HUMINT capability and works with DoW and other national-level agencies to collect on priority USAF operational and strategic requirements. The Director of the CIA serves as the National HUMINT Manager, and the Director of the DIA serves as the DoW functional manager.

SIGNALS INTELLIGENCE (SIGINT)

SIGINT is a category of intelligence comprised of COMINT, ELINT, and FISINT, that may consist of an individual element, or a combination. SIGINT uses intercepted electromagnetic emissions to provide information on adversary forces' capabilities, intentions, formations, and locations. SIGINT also includes collecting, processing, and exploiting data from information in cyberspace. The air component's link to the SIGINT enterprise is the National Tactical Integration (NTI) specialty team in the ISRD. The NSA serves as the IC functional manager for SIGINT.[23]

Communications Intelligence (COMINT). COMINT consists of information derived from intercepting and monitoring the adversary's communications systems. COMINT exploits an adversary's communications, revealing capabilities, intentions, perceived vulnerabilities, and, often, an adversary's perception of the US and multinational partners.

Electronic Intelligence (ELINT). ELINT is intelligence derived from interception and analysis of non-communications emitters, such as radars. ELINT includes both operational electronic intelligence (OPELINT) and technical electronic intelligence (TECHELINT). OPELINT focuses on operationally relevant information (location, movement, employment, tactics, and activity of foreign non-communications emitters and associated weapons systems). TECHELINT concentrates on the technical aspects (signal characteristics, modes, functions, associations, capabilities, limitations, vulnerabilities, and technology levels).

Foreign Instrumentation Signature Intelligence (FISINT). FISINT consists of technical information derived by intercepting electromagnetic emissions associated with testing and operational deployment of foreign air and space, surface, and subsurface systems. These emissions are typically generated by telemetry, electronic interrogators, and video data links. The technical details of foreign weapons system development derived from FISINT can provide insight into foreign capabilities, identify avenues for exploitation, and/or aid the employment of appropriate countermeasures. FISINT is accomplished by specialized, national-level Service and DoW organizations.

[23] For additional information on the role of NTI, see AFTTP 3-1.NTI, *National Tactical Integration*.

MEASUREMENT AND SIGNATURE INTELLIGENCE (MASINT)

MASINT is technically derived intelligence to detect, locate, and describe the physical measurements and signatures intrinsic to targets and events. MASINT collects and produces precise threat characteristics and performance information essential to support planning, development, and application of weapon systems, countermeasures, targeting, and battle damage assessment. MASINT is especially useful to monitor adversary technical developments and deployments, as well as emerging threats from weapons of mass destruction. DIA leads the IC effort for MASINT via senior science and technology officers (SSTOs) who integrate DIA efforts to meet operational intelligence requirements.

OPEN-SOURCE INTELLIGENCE (OSINT)

OSINT is intelligence derived from publicly available information (PAI) that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. PAI is information that has been published or broadcast for public consumption, available on request to the public, accessible online, could be seen or heard by a casual observer, or obtained by visiting a place or event open to the public. OSINT complements other intelligence disciplines and may cue collection and analysis, fill intelligence gaps, and supplement the accuracy and fidelity of classified information databases. Importantly, OSINT is susceptible to manipulation and deception and requires research expertise and OPSEC for internet-based activities. The Director of the CIA is the IC functional manager for OSINT, and the DIA Director is the DoW's functional manager.

TECHNICAL INTELLIGENCE (TECHINT)

TECHINT is intelligence produced by collecting, processing, analyzing, and exploiting data and information regarding foreign equipment to prevent technological surprise, assess foreign scientific and technical capabilities, and develop countermeasures to neutralize an adversary's technological advantages. TECHINT begins with the acquisition or recovery of a foreign piece of equipment or foreign scientific or technological information. This work is typically performed in a forward-deployed location by a joint captured materiel exploitation center (JCMEC) managed by DIA and OPCON to the CCMD.[24]

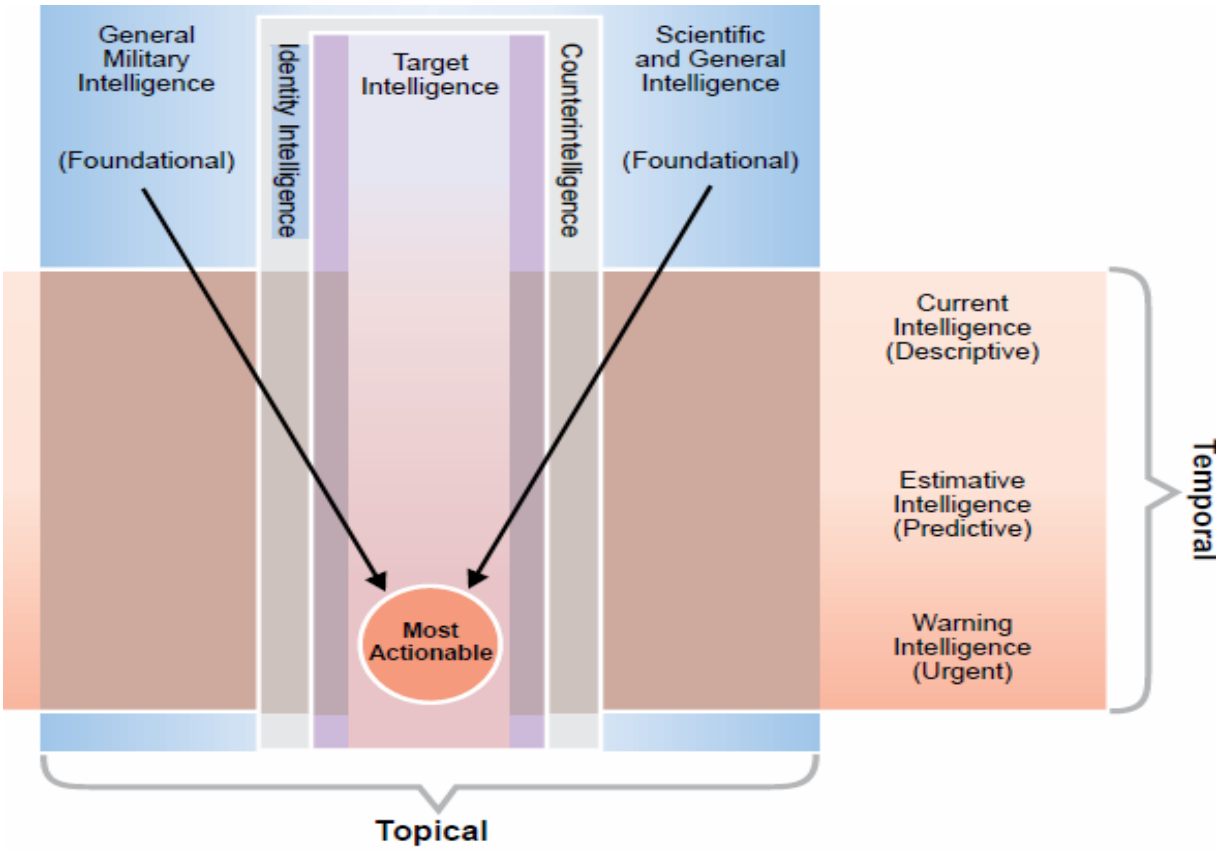
ANALYSIS AND PRODUCTION

Intelligence products generally span eight all-source categories: General Military Intelligence, Scientific and Technical Intelligence, Target Intelligence, Counterintelligence, Estimative Intelligence, Identity Intelligence, Current Intelligence, and Warning Intelligence. Each category is aligned to a distinct purpose and decision need. All-source intelligence analysis is inherently complex, supporting national, theater, and tactical consumers while simultaneously sustaining multiple production lines, including foundational, time-sensitive reporting, and tactical mission analysis. USAF intelligence professionals integrate contributions from all eighteen IC organizations,

[24] For additional information on intelligence disciplines, see JP 2-0, *Joint Intelligence*.

fusing national-level products with time-dominant reporting to generate decision-quality intelligence for the air component and the joint force.[25]

All-Source Topical and Temporal Relationships



General Military Intelligence (GMI). GMI is intelligence concerning foreign countries' military capabilities or topics affecting potential US or multinational military operations. Current intelligence and GMI form a symbiotic relationship. Information gained during the development of current intelligence forms the basis for the GMI effort and other analytical products. Conversely, GMI provides underlying threat information to produce accurate and meaningful current intelligence.

GMI focuses on a wide range of factors, including order of battle, organization, DOF, training, tactics, and overall strategy to determine a nation's military strength and effectiveness. GMI also analyzes critical supporting elements such as transportation networks, military materiel production, military and civilian communications systems, and military economics, including any foreign military assistance. Furthermore, it considers the potential use of asymmetric tactics or terror attacks and involves the detailed location, identification, and description of military-related installations. This analysis results in key products such as military-related infrastructure assessments, which detail an adversary's capabilities and warfighting sustainability, and military capabilities assessments, which determine an adversary's potential to employ force by evaluating their order of battle,

[25] For additional information on all-source production categories, see JP 2-0, *Joint Intelligence*.

readiness levels, and vulnerabilities.

Scientific and Technical Intelligence (S&TI). S&TI examines foreign developments in basic and applied sciences and technologies with potential for military use, particularly to enhance weapon systems. S&TI is a product that results from collection, evaluation, analysis, and interpretation of foreign scientific and technical information. It covers foreign developments in basic applied research and applied engineering techniques. S&TI also covers scientific and technical characteristics, capabilities, and limitations of foreign military systems. This analysis includes weapons, weapon systems, and materiel, the related research and development, and the methods used to manufacture the foreign military system. Example S&TI products include weapon system characteristics, capabilities, vulnerabilities, limitations, effectiveness, research and development, and related manufacturing information. S&TI products play a vital role in the acquisition process by allowing the procurement of systems or systems upgrades to meet current, developing, and future threats.

Acquisition Intelligence. Acquisition intelligence addresses future threats, specializing in S&TI to anticipate enemy capabilities in advance by one to five years. Acquisitions intelligence brings a focus on supportability issues associated with new ISR capabilities planned to be brought into theater. It is especially important for multinational operations.

Identity Intelligence. Identity intelligence results from the fusion of identity attributes (biologic, biographic, behavioral, and reputational information related to individuals), and other information and intelligence associated with those attributes, collected across various intelligence disciplines. The goal of identity intelligence is to discover unknown potential threat actors by connecting individuals to other persons, places, events, or materials, analyzing patterns of life, and characterizing the threat posed to US interests.

Target Intelligence. Intelligence operations play a prominent role in the targeting cycle by detecting, locating, and identifying targets and supporting mission planning and assessment. Target intelligence portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. Required products, such as target imagery, should be immediately available to support the air tasking cycle. ISR assets may be employed to detect and identify potential targets, changes to existing targets, or to conduct battle damage assessment. Multiple missions may be required to provide the level of detail necessary to support the precision engagement of specific targets. Target intelligence products include annotated target graphics, electronic target folders, target system analyses, and geospatial information to provide comprehensive data needed to plan and generate lethal and nonlethal effects.

Targeting within the air tasking cycle operates inside a compressed 72-hr window. Here, the focus shifts from foundational target development to the selection and prioritization of already developed targets from the restricted target list (RTL) or joint target list (JTL) for inclusion on the component target list (CTL). Intelligence analysts and targeteers attend joint targeting working groups (JTWG) and joint targeting coordination boards (JTCB) to approve targets for the JIPTL to meet commander’s objectives. Regardless of the cycle, intelligence personnel constantly evaluate the adversary and update target information, ensuring that targeting, whether deliberate or dynamic, is based on the most current and

accurate intelligence available.[26]

Current Intelligence. Current intelligence is produced by fusing data and intelligence products regarding the current situation in a particular area or the activities of specific groups. This type of intelligence is similar to warning intelligence in that both require continuous monitoring of world events and specific activities in an operational area. Information required to produce current intelligence products includes continuous assessments of adversary intentions, capabilities, and the will to use military force, as well as the identification of potential centers of gravity, operational plans, and vulnerabilities. It also encompasses geographic, environmental, and social analysis of the operational area, monitoring significant military and political events, and the status of strategic transportation nodes such as major airfields and seaports. A critical component of current intelligence is maintaining the adversary's DOF, a product of the DCGS enterprise that provides the precise geographic location and status of known units, directly enabling the Find, Fix, Track (F2T) phase of the dynamic targeting process.

Estimative Intelligence. Estimative intelligence provides forecasts of current or potential situations that may have bearing on the planning and execution of military operations, otherwise known as estimates. By employing pattern analysis, inference, and statistical probability techniques, intelligence personnel produce estimates describing relevant actors' capabilities and behavior.

Warning Intelligence. Warning intelligence products are derived from a worldwide system that analyzes and integrates information to assess the probability of hostile actions and provide sufficient warning to preempt or counter their effects. Warning intelligence systems rely on information and indications from sources at all levels. The focus of warning intelligence products varies at each echelon and is most specific at the operational and tactical levels. Warning intelligence products are specifically designed to alert decision-makers to emerging threats and potential crises, focusing on adversary intentions, capabilities, past behaviors, and doctrine. This includes monitoring foreign government responses to crises, analyzing significant political, economic, or social situations in both friendly and adversary states that could trigger instability, and tracking changes in adversary force dispositions, military activities, and mobilization status. Furthermore, warning intelligence examines adversary disinformation capabilities and observes civil or bureaucratic activities that might foreshadow subsequent military action, alongside continuously assessing the status of other military forces within an operational area.

Counterintelligence (CI). CI includes strategic analysis to identify and produce all-source finished intelligence on foreign intelligence threats to friendly operations. CI develops and implements strategies and action plans to counter the CI threat, tasks CI collection capabilities, and leverages all other intelligence disciplines to fill CI collection gaps.

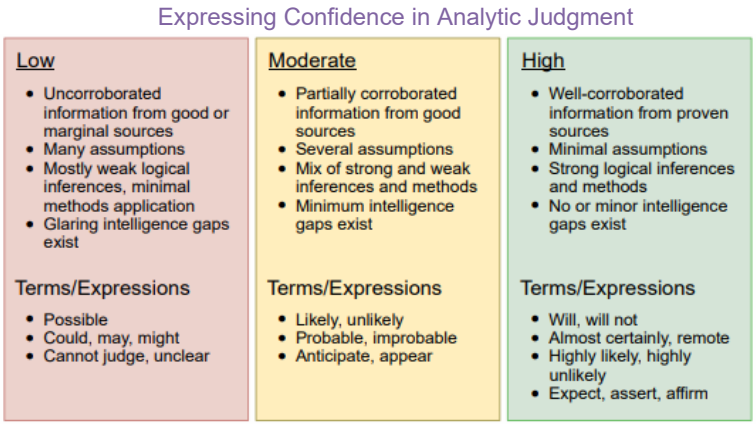
CI is critical to USAF operations, particularly force protection efforts. CI threat estimates and vulnerability assessments identify friendly weaknesses and vulnerabilities that may

[26] For additional information on the Air Force targeting process, see AFDP 3-60, *Targeting*.

be exploited by an adversary. CI supports friendly planning efforts through sociocultural analysis of enemy leadership characteristics. CI can also help assess enemy reactions to friendly deception efforts. Various classified CI databases maintain information on personalities, organizations, installations, and incidents. These databases can help provide indications of the motivations and ideology of potential adversaries.

AFOSI is the sole authorized executor of the CI mission for the DAF. No other DAF entities are authorized to conduct CI activities. AFOSI is a field operating agency under the administrative guidance and oversight of the Air Force Inspector General (SAF/IG). AFOSI forces normally operate in a Service retained status under the Commander, AFOSI. When attached to a CCMD, as specified by a military operation or operation order, the exercise of CI authorities may be under the OPCON of a CCDR providing a CI capability in support of CCDR PIRs. CCDR CI authority may limit AFOSI's ability to conduct Service CI activities. The Secretary of the Air Force (SecAF) retains administrative control (ADCON) for those USAF CI resources under OPCON of the CCDR.

CONFIDENCE IN ANALYTIC JUDGEMENT



USAF intelligence personnel adhere to analytical tradecraft standards common across the entire joint force and the IC to ensure rigor and clarity in their assessments. A fundamental aspect of this is the formal expression of confidence in analytical judgments. Confidence is the value placed on an analysis, "high confidence" in target identification, for example, increases combat effectiveness while reducing risks such as fratricide and collateral damage. Conversely, "low confidence" indicates a greater risk to the mission and friendly forces due to an incomplete understanding of the environment. These levels are not a guess, they are determined by systematically evaluating three factors: the number of key assumptions, the credibility and diversity of sources used, and the overall strength of the logical argument. Analysts then assign a confidence level of low, moderate, or high to their judgments, providing commanders with a clear and standardized measure of the certainty behind the intelligence they receive for decision-making.[27]

DISSEMINATION AND INTEGRATION

The dissemination and integration step involves the delivery to and use of intelligence. Dissemination ensures commanders, planners, and operational forces receive finished intelligence in time to make effective decisions and execute operations. The USAF's distributed operations capability provides timely and tailored intelligence across the globe

[27] For additional information on confidence, see JP 2-0, *Joint Intelligence*.

to multiple end-users.

Dissemination is accomplished through various means, each requiring continuous management (e.g., electronic transmission, hardcopy annotated imagery and maps, direct threat warnings, oral and written reports, briefings, and various servers allowing structured discovery and retrieval). When managed ineffectively, communications paths can become saturated by information retransmitted by numerous intermediate collection agencies, resulting in circular reporting. Advances in cyberspace capabilities and technologies should be leveraged to improve dissemination and reduce the information-to production timeline for delivery of intelligence products. Importantly, intelligence planning should include procedures for rapidly coordinating with public affairs for the public release of appropriately declassified intelligence.

Integration ensures disseminated intelligence is employed effectively. After intelligence products have been disseminated, intelligence organizations are responsible for continuing to support users as they integrate the intelligence into decision-making and planning processes. Continuous integration of intelligence and operations allow commanders and operational planners access to the most current information. This access optimizes intelligence support to operations planning, preparation, execution, and assessment functions.

Common Intelligence Feed/Picture (CIF/P): A flexible display of relevant, instructive, and contextual intelligence information regarding adversary, and neutral force disposition, and supporting infrastructures derived from all sources at any level of classification, shared by more than one command, which facilitates collaborative planning and assists all echelons to enhance situational awareness and decision-making.

The CIP/F represents the synthesized product of the entire intelligence enterprise. It is the authoritative, shared source of ground truth about the adversary, flowing up from the tactical edge and back down from the strategic level. This critical warfighting function is executed at each echelon: within the AOC, the ISRD develops and maintains the operational level picture, supported by the DGS. At the tactical level, the CIC is responsible for maintaining the intelligence picture for its wing, ensuring immediate relevance to aircrew and combat operations.[28]

EVALUATION AND FEEDBACK

All operations in the intelligence process are interrelated and should be evaluated to determine the degree to which they facilitate each other and succeed in meeting intelligence requirements. Importantly, evaluation and feedback are not an independent operation in the intelligence process. Rather, it should be conducted continuously to assess the intelligence process. The goal is to identify issues as early as possible to minimize information gaps, mitigate capability shortfalls, and ensure intelligence operations meet established analysis tradecraft and objectivity standards.

Evaluation and feedback require a collaborative dialogue between intelligence planners,

[28] For additional information on the CIP/F, see the Air Land See Space Application (ALSSA) Center *CIP/F Tactical Bulletin (TACBUL)*.

collection managers, collectors, and analysts to identify deficiencies within the intelligence process. Assessment of intelligence operations relies on product satisfaction, as determined by the user. As such, intelligence personnel and users should provide timely feedback regarding intelligence process successes and problems. A formalized process should be established to ensure feedback is provided consistently and analyzed systematically.

Assessment Methods. An ISR strategy is not complete unless it includes a qualitative and quantitative ISR assessment. Assessments provide leaders with information to reprioritize intelligence requirements, shift collection emphasis, change analytic levels of effort, and reallocate available ISR assets. To assess intelligence activities and operations, intelligence planners develop and document intelligence measures of performance (MOPs) and intelligence measures of effectiveness (MOEs).

- **Measurement of Performance (MOP).** An indicator used to measure a friendly action that is tied to measuring task accomplishment.

  MOPs are informed by quantitative indicators. They indicate whether a particular platform or sensor is performing as expected: e.g., the number of sorties conducted or number of images taken.

- **Measurement of Effectiveness (MOE).** An indicator used to measure a current system state, with change indicated by comparing multiple observations over time.

  MOEs gauge the impact of intelligence tasks performed within the intelligence process. MOE indicators tend to be qualitative and related to the value of the intelligence produced.

REFERENCES

All websites accessed 30 Apr 2026.

US AIR FORCE DOCTRINE: https://www.doctrine.af.mil/

- AFDP 1, *The Air Force*
- AFDP 3-0, *Operations*
- AFDP 3-10, *Force Protection*
- AFDP 3-12, *Cyberspace Operations*
- AFDP 3-27, *Homeland Operations*
- AFDP 3-60, *Targeting*
- AFDP 3-72, *Nuclear Operations*
- AFDP 5-0, *Planning*

JOINT DOCTRINE

- JP 2-0, *Joint Intelligence*
- JP 3-30, *Joint Air Operations*
- JP 3-60, *Joint Targeting*

TACTICAL DOCTRINE

ALSSA-Multi-Service Tactics, Techniques, and Procedures (MTTPs)

- AFTTP 3-1, *National Tactical Integration*
- AFTTP 3-2.88, *ISR Optimization*
- AFTTP 3-3, *AOC*
- AFTTP 3-4.14. *Contingency Intelligence Network*
- ALSSA Center, *CIP/F Tactical Bulletin*

MISCELLANEOUS PUBLICATIONS

- DAFMAN 14-401, *Intelligence Analysis And Targeting Tradecraft/Data Standards*
- Air Combat Command (ACC) A2 Disposition of Forces (DOF) Concept of Operations (CONOP)