Joint Pub 2-02

National Intelligence Support to Joint Operations

28 September 1998

PREFACE

1. Scope

This joint publication describes national intelligence organizations and their support to joint military operations. Also addressed is the special support and augmentation available for joint operations by national joint elements such as the Military Intelligence Board, the National Military Joint Intelligence Center, and National Intelligence Support Teams. This joint publication covers Service intelligence organizations and centers, as well as nonmilitary agencies and nongovernmental organizations. The recommended target audience for this joint publication is commanders and intelligence staffs of combatant commands, subordinate unified commands, joint task forces, combat support agencies, and supporting Service components.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth doctrine to govern the joint activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for US military involvement in multinational and interagency operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders and prescribes doctrine for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the joint force commander (JFC) from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

3. Application

a. Doctrine and guidance established in this publication apply to the commanders and intelligence staff of combatant commands, subordinate unified commands, joint task forces, combat support agencies, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached to forces of another Service or when significant forces of one Service support forces of another Service.

b. The guidance in this publication is authoritative; as such, this doctrine (or JTTP) will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable.

For the Chairman of the Joint Chiefs of Staff:

DENNIS C. BLAIR
Vice Admiral, US Navy
Director, Joint Staff

Intentionally Blank

TABLE OF CONTENTS

FIGURE

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Describes the National-Level Intelligence Support to Joint Military Operations**
- **Describes the National Intelligence Community**
- **Discusses the Military Intelligence Community**
- **Outlines the Service Intelligence Organizations**

National-Level Intelligence Support to Joint Military Operations

The joint force intelligence officer relies on the support of national intelligence organizations in order to provide the joint force commander (JFC) with timely, relevant, and accurate intelligence.

National intelligence organizations operate extensive collection, processing, and dissemination systems. These intelligence organizations employ specialized resources and dedicated personnel to gain information about potential adversaries, events, and other worldwide intelligence requirements. Successful national support to joint force commanders (JFCs) depends upon efficient and effective cooperation and interoperability, not only vertically but also horizontally among national organizations. The accomplishment of the JFC's goals depends in part on the smooth interaction and contributions of the entire intelligence community, including the national intelligence organizations.

National Intelligence Community

National intelligence organizations must be committed to shared purpose and cooperation in order to provide comprehensive intelligence support to JFCs and joint operations.

The framework for the Intelligence Community (IC) was created under the National Security Act of 1947. The Act established the National Security Council (NSC), the Director of Central Intelligence (DCI), and the Department of Defense (DOD). There are four statutory members of the NSC, which include the President, Vice President, Secretary of Defense, and the Secretary of State, while the Chairman of the Joint Chiefs of Staff and the DCI serve as statutory advisors. **The IC refers in the aggregate to those Executive Branch agencies and organizations that are founded in the National Foreign Intelligence Program.** The responsibility for providing intelligence support to military operations, during peacetime or crisis, rests with the National Military Joint Intelligence Center (NMJIC) and the joint intelligence centers (JICs). There are also many nonmilitary intelligence agencies and organizations that can support joint operations by providing

intelligence used in developing strategy, determining objectives, planning operations, conducting operations, and evaluating the effects of operations.

Military Intelligence Community

The Department of Defense and joint intelligence agencies and organizations must support joint operations in a timely, pertinent, and adequate manner.

The Military Intelligence Community includes the Secretary of Defense, the Defense Intelligence Executive Board, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, and the Assistant to the Secretary of Defense, Intelligence Oversight. **The Secretary of Defense exercises full direction, authority, and control over the intelligence activities of the Department of Defense** and is responsible for collecting, processing, producing, and disseminating military and military-related foreign intelligence and counterintelligence. The Defense Intelligence Agency is responsible for the timely and accurate flow of military intelligence from the national level, through the JICs, to deployed forces during peacetime. **Within the Military IC the Military Intelligence Board (MIB) serves as the senior "Board of Governors,"** working to develop cooperation and consensus on cross-agency, Service, and command issues. The MIB has a key role in guiding and supporting DOD intelligence operations and provides a forum for the discussion of ongoing national-level issues.

The National Military Joint Intelligence Center is the focal point for all defense intelligence activities in support of joint operations.

The Joint Staff Director for Intelligence develops joint intelligence doctrine and architecture, and manages intelligence for joint warfighting assessments while assisting the commands in passing critical, time-sensitive requirements to the NMJIC and the Defense Indications and Warnings System. **NMJIC supports the Joint Staff Director for Intelligence with all-source intelligence functions** and is the single point of entry for crisis requests for information as well as the point-of-contact for combatant commands to interface with elements of the National IC.

Service Intelligence Organizations

The Chiefs of the Military Services provide intelligence support for departmental missions related to military systems, equipment, training, and national intelligence activities.

Intelligence support comes from many different agencies and organizations throughout the Military Services. The missions and responsibilities of the Service intelligence centers, including the unique capabilities and products of these centers, provide support to the overall DOD intelligence effort and allow for comprehensive intelligence support to JFCs and joint operations.

CONCLUSION

This joint publication describes national intelligence organizations and their support to joint military operations. Also addressed is the special support and augmentation available for joint operations by national joint elements such as the MIB, the NMJIC, and national intelligence support teams. This joint publication covers Service intelligence organizations and centers as well as nonmilitary agencies and nongovernmental organizations.

Intentionally Blank

CHAPTER I
NATIONAL INTELLIGENCE SUPPORT: AN OVERVIEW

"One should know one's enemies, their alliances, their resources and nature of their country, in order to plan a campaign. One should know what to expect of one's friends, what resources one has, and foresee the future effects to determine what one has to fear or hope from political maneuvers."

Frederick the Great
Instructions for His Generals, 1747

1. Introduction

The Intelligence Directorate of a joint staff (J-2) will have to rely on national intelligence organizations for support in order to provide the joint force commander (JFC) with timely, relevant, and accurate intelligence. The J-2 will not be capable of satisfying all the commander's requirements using joint force, component, or even theater-level intelligence resources. The J-2 will have to rely upon or reach back to national intelligence organizations to provide a comprehensive intelligence support effort. The J-2 must understand how the national intelligence organizations are organized and how they operate in order to best exploit their capabilities.

2. Overview

This publication describes national intelligence support to joint operations and provides understanding for use by the military in preparing their plans, and outlines the national roles within this environment. **National intelligence organizations operate extensive collection, processing, and dissemination systems.** These intelligence organizations employ specialized resources and dedicated personnel to gain information about potential adversaries, events, and other worldwide intelligence requirements. The J-2 should take advantage of the extensive capabilities provided by these organizations. This publication is to be used in conjunction with Joint Pub 2-0, "Doctrine for Intelligence Support to Joint Operations," and Joint Pub 2-01, "Joint Intelligence Support to Military Operations." Joint Pub 2-0, "Doctrine for Intelligence Support to Joint Operations," describes the joint intelligence architecture and forms the doctrinal basis for US military intelligence involvement in multinational and interagency intelligence operations. Joint Pub 2-01, "Joint Intelligence Support to Military Operations," provides the fundamentals of joint intelligence responsibilities and command relationships and detailed information on the intelligence cycle, seen in Figure I-1. A summary of the intelligence cycle follows.

General:

Intelligence provides multidiscipline support to the combatant command, the subordinate Service and functional component commands, and subordinate joint forces.

Planning and Direction:

Conducted continuously, intelligence planning involves task-organizing intelligence assets; developing a collection plan; issuing requests for collection and production; and monitoring the availability of collected information.

Collection:

Collection operations acquire information about the adversary. Collection managers convert

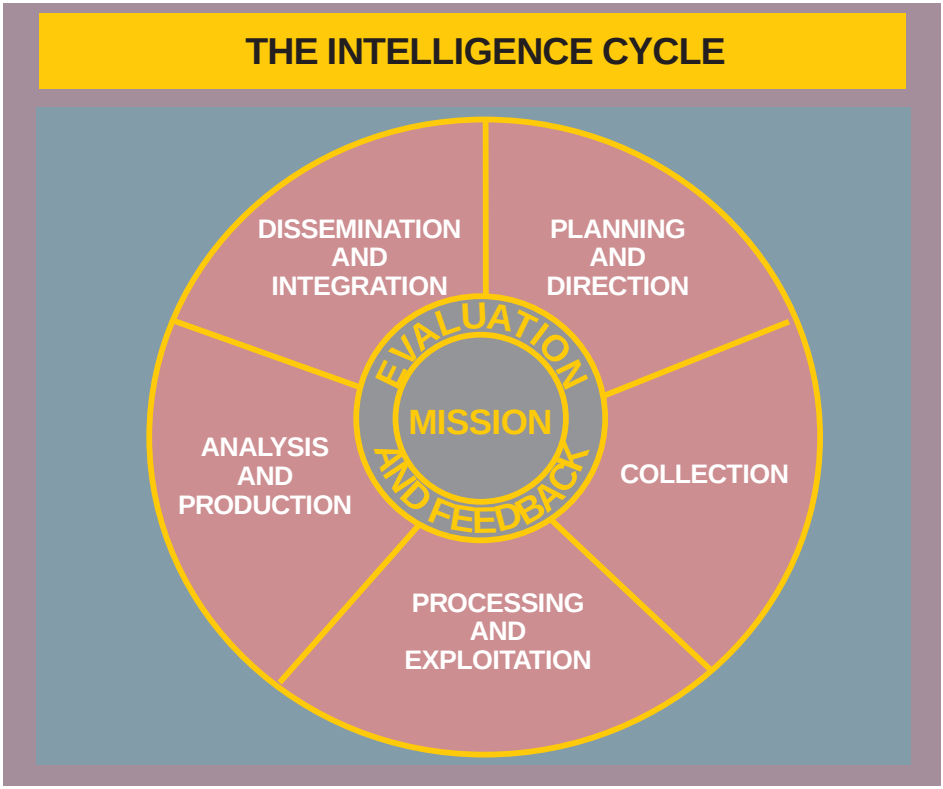


Figure I-1. The Intelligence Cycle

information requirements into collection requirements; establish, task or coordinate actions with appropriate collection sources or agencies; and monitor results in close coordination with the original requester and retask. Collection management officers (CMOs) develop collection plans based on the intelligence requirements of commanders, decision makers, and analysts. Components submit collection requests for management and validation to the theater CMO (or joint task force [JTF] CMO during contingencies), who tasks available collection assets against all collection requirements.

Processing and Exploitation:

Collected data is correlated and converted into forms suitable for analysis and production.

Analysis and Production:

Production changes information collected from single or multiple sources into finished intelligence. Production for joint operations is accomplished by organizations at every echelon, from national to joint force level. Production elements at all levels are assigned clearly delineated areas of analytical responsibility across the range of military operations.

Dissemination and Integration:

Dissemination consists of both "push" and "pull" intelligence concepts. The "push" concept allows the higher echelons to push intelligence down to satisfy existing lower echelon requirements or to relay other relevant intelligence to the lower level. The "pull" concept involves direct electronic access to data bases, intelligence files, or other repositories by intelligence organizations at all levels.

Evaluation and Feedback:

Intelligence personnel at all levels evaluate the intelligence process and provide feedback to improve support to the requester.

3. The Role of National Intelligence Organizations

a. The national intelligence organizations can and will provide support to the JFC and continue to support national decision makers. **The focus of these national organizations is not evenly split among intelligence customers and varies according to the situation.**

b. Successful national support to JFCs depends upon efficient and effective cooperation and interoperability not only vertically (among national and subordinate echelons) but also horizontally (among national organizations). Each agency is assigned clearly defined missions and areas of responsibility to minimize duplication of effort and questions over functional responsibilities.

c. **National intelligence organizations** (Central Intelligence Agency [CIA], Defense Intelligence Agency [DIA], National Security Agency [NSA], National Imagery and Mapping Agency [NIMA], and the State Department) **support the combatant commanders on a full-time basis through representatives.** Some of these representatives are located full-time at the command headquarters. These representatives serve as the combatant commander's advisors on how to best employ their organization's capabilities and provide liaison with their parent organizations. The commands should utilize these representatives

Intelligence representatives serve as both advisors to combatant commanders and liaisons to their parent organizations.

in conjunction with this publication to ensure that the command is familiar with the current responsibilities, capabilities, and operations of each organization.

d. US military planning and operational deployments have become increasingly complex in recent years. They are characterized by multi-Service and interagency involvement and are frequently multinational in nature. **The accomplishment of the JFC's goals depends in part on the smooth interaction and contributions of the entire intelligence community, including the national intelligence organizations.**

NATIONAL INTELLIGENCE IN THE PERSIAN GULF WAR

Coinciding with the release of Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), and Central Command (CENTCOM) warnings of possible Iraqi military action against Kuwait [issued on 1 August 1990], DIA activated an Intelligence Task Force (ITF) in the National Military Intelligence Center (NMIC) at the Pentagon, and augmented the Operational Intelligence Crisis Center (OICC) at the Defense Intelligence Analysis Center on Bolling Air Force Base, Washington, DC. The ITF mission was to provide direct support to the JCS operations and planning staffs, and to serve as a clearinghouse for the flood of requests for information (RFIs) pouring into the NMIC from commands worldwide. The OICC was augmented to coordinate and manage all DIA research and analytical efforts to provide responses to RFIs, and to produce specialized targeting packages.

Concurrent with CENTCOM's initial force deployments on 7 August 1990, DIA deployed a National Military Intelligence Support Team (NMIST) to Riyadh. NMIST have self-contained satellite communications equipment providing direct connectivity to DIA for the submission of RFIs and the direct dissemination of intelligence information and imagery to the theater. Eleven NMISTs eventually were deployed to support forces involved in Operations DESERT SHIELD and DESERT STORM. The NMIST network was to prove crucial to the CENTCOM J-2 since it eventually would be the sole dedicated intelligence communications capability between the CENTCOM J-2, the component and subunified command intelligence staffs, and the information, to include imagery, especially when the existing communications circuits between the United States and the theater became saturated with operational message traffic.

SOURCE: Final Report to Congress
Conduct of the Persian Gulf War, April 1992

CHAPTER II
THE INTELLIGENCE COMMUNITY

"The times we live in are times of profound change, dramatic and fundamental change — political, idealogical, and technical. We must adapt to that change, and we must grow."

GEN Gordan R. Sullivan, 23 May 1993

1. Introduction

This chapter provides information about the national-level intelligence organizations that could provide support to joint operations. National intelligence organizations should be committed to cooperation and a shared purpose in order to provide comprehensive intelligence support to JFCs and joint operations.

2. Management and Oversight of the Intelligence Community

a. **National Security Act.** The National Security Act of 1947 created the framework for the Intelligence Community (IC). The Act established the National Security Council (NSC), the Director of Central Intelligence (DCI), and the Department of Defense (DOD), and identifies the organizations that make up the IC.

b. **National Security Council.** The NSC is the principal forum to consider national security issues that require Presidential decision (See Figure II-1). There are four statutory members: the President, the Vice President, the Secretary of Defense (SecDef), and the Secretary of State (SECSTATE). The Chairman of the Joint Chiefs of Staff (CJCS) and the DCI serve as statutory advisors. The DCI attends NSC meetings as its Intelligence Advisor. The Assistant to the President for National Security Affairs (the National Security Advisor) is responsible for the NSC's day-to-day operations. Council functions are supported by the NSC staff that includes the White House Situation Room and regional and functional desks.

c. **Director of Central Intelligence.** The DCI serves in four roles:

- as the principal intelligence advisor to the President;
- as the director of the CIA;
- as the head of the entire US IC; and
- as a statutory advisor to the NSC.

As the top policymaker for the IC, the DCI develops policies for and provides guidance on future intelligence needs and capabilities. The DCI is authorized to establish committees and boards for advice and is charged with producing and disseminating national foreign intelligence. The DCI tasks major collection systems that can be employed to satisfy strategic, operational, and tactical intelligence requirements. The DCI also is responsible for coordinating the relationships between elements of the intelligence community and the intelligence or security services of foreign governments on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means; providing overall direction for the collection of national intelligence through human sources by elements of the intelligence community and coordinating with other agencies which are authorized to undertake collections; and conducting counterintelligence activities outside the United States and coordinating the counterintelligence activities of other government agencies outside the United States.

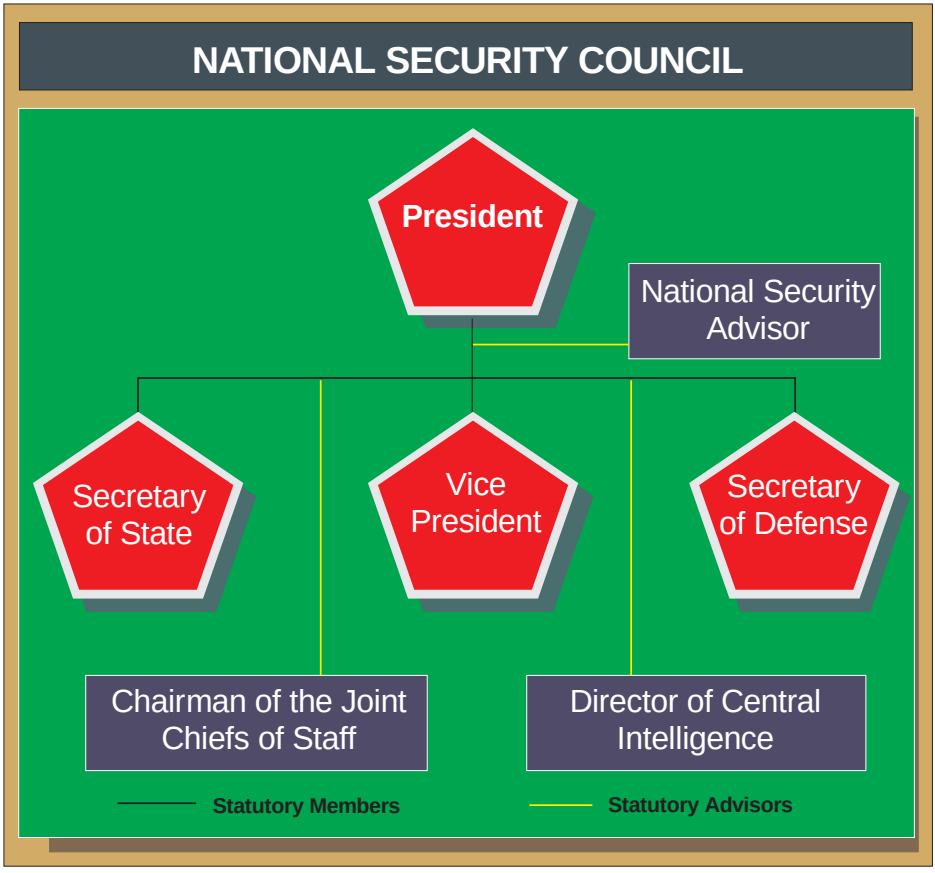


Figure II-1. National Security Council

d. **Intelligence Community.** The IC refers in the aggregate to **those Executive Branch agencies and organizations that are founded in the National Foreign Intelligence Program** (NFIP). (The Intelligence Management Programs, including the NFIP, are discussed in Appendix D, "Intelligence Resource Programs.") The Community currently includes the CIA, the NSA, the DIA, the NIMA, the National Reconnaissance Office (NRO), the Bureau of Intelligence and Research (INR) of the State Department, the counterintelligence (CI), cryptologic, and some of the foreign intelligence elements of the Military Services (Army, Navy, Air Force, and Marine Corps), and foreign intelligence and/or CI elements of the Federal Bureau of Investigation (FBI) and the Treasury and Energy Departments (See Figure II-2). The nonmilitary organizations and their responsibilities are detailed in Chapter III, "Nonmilitary Members of the Intelligence Community."

- **IC Management.** Two key officials directly support the DCI to implement the DCI's community responsibilities.

  •• **Chairman, National Intelligence Council (NIC).** The Chairman of the NIC **oversees IC production and analysis,** including National Intelligence Estimates and NIC Memorandums.

  •• **Executive Director for Intelligence Community Affairs (EXDIR/ICA).** The EXDIR/ICA is **the DCI's principal advisor on IC matters** and assists the

Figure II-2. Intelligence Community Membership

DCI in planning and implementing national foreign intelligence production responsibilities. As the Director of the Community Management Staff (CMS), the EXDIR/ICA is responsible for developing, coordinating, and overseeing implementation of DCI policy in resource management, systems analysis, and requirements and evaluation.

- **Community Management Staff.** The CMS is responsible for oversight of IC responsiveness to the DCI's guidance. **The CMS oversees all Community-wide programming and budgeting activities and controls the overall requirements tasking process.** The two principal CMS offices, and the contribution each makes in promoting the overall effectiveness of the IC, are as follows:

•• **Program Evaluation and Budget Office.** This office, composed of four groups, enhances CMS' program review capability by providing resource information, program budget oversight, and program analysis and evaluation. The Resources Management Group is responsible for resource information and guidance and program budget oversight of component programs of the NFIP. The Program Assessment Group performs analysis and evaluation of programs. The Advanced Technology Group oversees the IC's Advanced Research and Development programs. The Quality

Council Secretariat reviews IC quality management and performs the National Performance Review.

•• **Requirements, Plans, and Policy Office.** This office consists of three groups. The Requirements and Plans Group is responsible for planning, requirements, management, and performance evaluations. The Policy and Special Issues Group provides policy guidance, evaluates IC management issues, and provides the CMS with legal counsel. The Foreign Language Coordinator serves as the Foreign Language Committee Secretariat for the IC.

- **National Foreign Intelligence Advisory Groups**

•• **The President's Foreign Intelligence Advisory Board (PFIAB). The PFIAB consists of 16 members, appointed by the President, who are senior civilian and former military leaders.** The Board reports directly to and advises the President on the performance of all government agencies engaged in the collection, analysis, or production of intelligence or in the execution of intelligence policy. Additionally, the Board advises the President concerning the objective, conduct, and coordination of the activities in these agencies. The Board is specifically charged to make appropriate recommendations for actions to improve and enhance the performance of intelligence efforts.

•• The National Foreign Intelligence Board is **the senior IC advisory body to the DCI** and includes senior representatives from all organizations involved in the collection, processing, and analysis of intelligence. The intelligence chiefs of the military Services are observers. The Board is chaired by the DCI and reviews all substantive intelligence matters, including production, review, and coordination of all national foreign intelligence; arrangements with foreign governments on intelligence matters; and protection of intelligence sources and methods.

•• **Intelligence Community Executive Committee (IC/EXCOM).** The IC/EXCOM **advises the DCI on priorities and objectives for the NFIP budget, national intelligence policy and planning, and IC management and evaluation.** The IC/EXCOM is chaired by the DCI or the Deputy DCI (DDCI), or, in their absence, by their designated representative. Permanent members include the DCI; DDCI; Vice Chairman, Joint Chiefs of Staff; Director, NSA; Director, DIA; Assistant SECSTATE and INR; Director, NRO; Director, NIMA; Chairman, NIC; Assistant Secretary of Defense, Command, Control Communications and Intelligence (ASD [C3I]); and EXDIR/ICA.

3. Request for Information from National Agencies

a. **The responsibility for providing intelligence support to military operations rests with the joint intelligence centers** (JICs). (This section should be used in coordination with Chapter III of Joint Pub 2-01, "Joint Intelligence Support to Military Operations," in which the organizations and responsibilities are discussed in detail.) The flow of the request for information (RFI) from national agencies differs only slightly from peacetime to crisis.

b. **The DIA ensures the expeditious flow of military intelligence from the national level through the JICs to deployed forces during peacetime.** RFIs are forwarded from the JIC to the DIA and/or production agency (See Figure II-3).

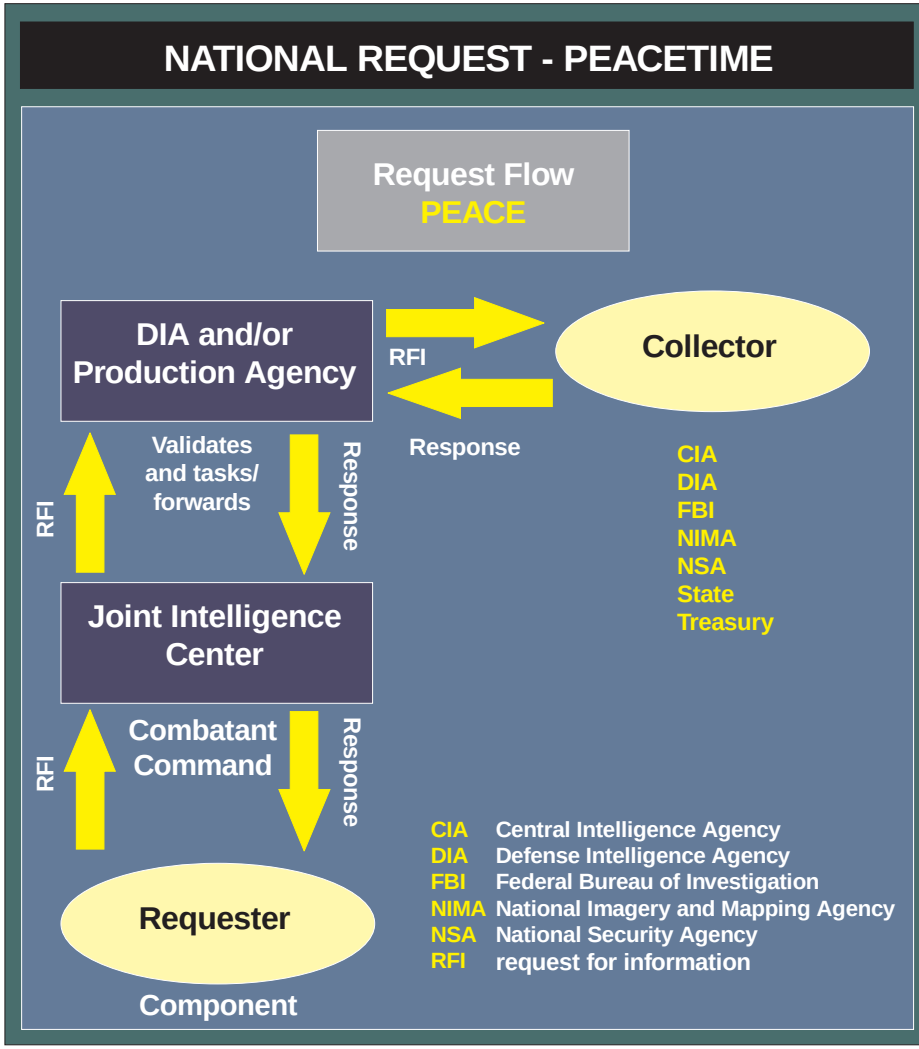


Figure II-3. National Request - Peacetime

c. **The Joint Staff J-2 National Military Joint Intelligence Center (NMJIC) is the national focal point for crisis intelligence in support of joint operations.** (The NMJIC's functions and structure are discussed in detail in Chapter V, "Joint Staff J-2," of this publication.) **The NMJIC is the single point of entry at the national level for crisis RFIs** (See Figure II-4).

d. The Joint Staff J-2 national intelligence support team (NIST) will serve as a direct link to the NMJIC RFI desk when the JTF J-2 determines that **time-sensitive** RFI require national **"reachback"** support. The JIC and/or Joint Analysis Center (JAC) will receive a simultaneous copy for tracking purposes (See Figure II-4).

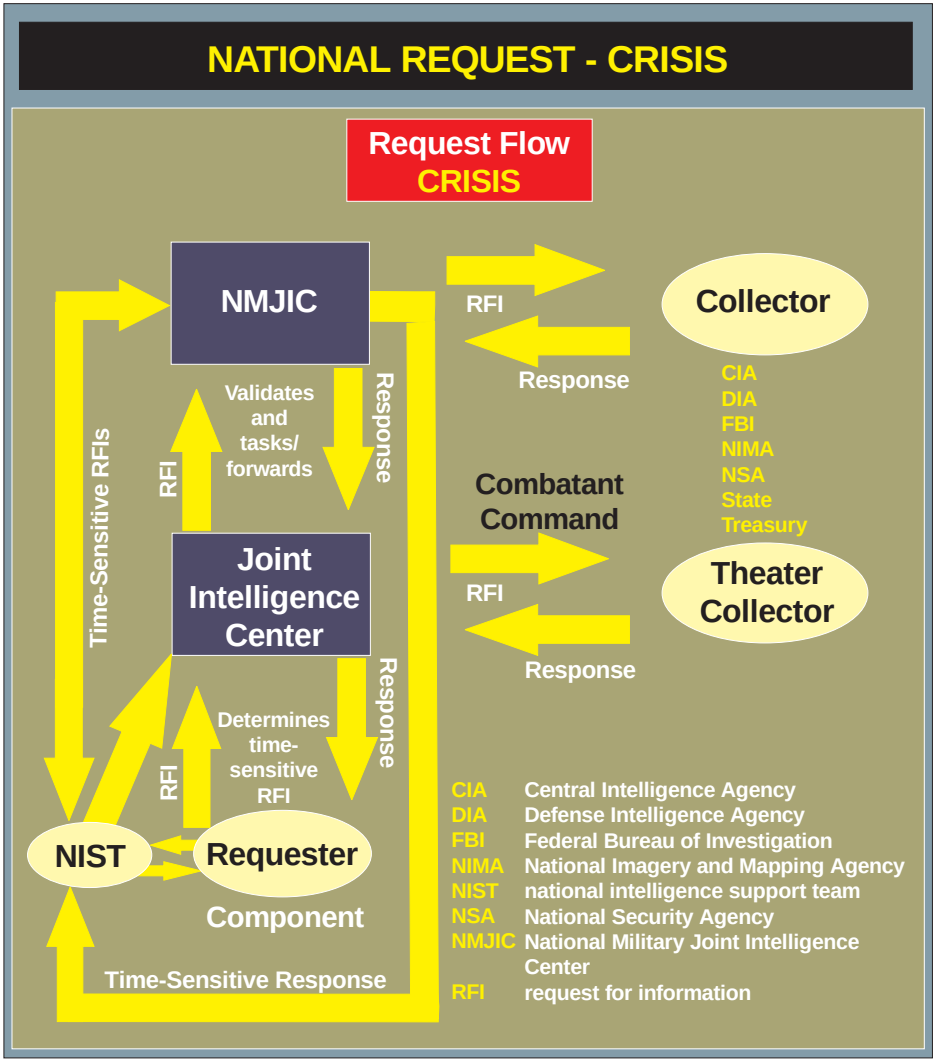


Figure II-4. National Request - Crisis

CHAPTER III
NONMILITARY MEMBERS OF THE INTELLIGENCE COMMUNITY

"In total war it is quite impossible to draw any precise lines between military and nonmilitary problems."

Winston Churchill
Their Finest Hour, 1949

1. Introduction

This chapter identifies responsibilities for nonmilitary intelligence agencies and organizations that can support joint operations. A part of the responsibility of these agencies is support of military policy. These nonmilitary agencies and organizations contribute to the support for joint operations in a significant manner by providing intelligence used in developing strategy; determining objectives; planning operations; conducting operations; and evaluating the effects of operations. A primary responsibility is to assist in identifying potential intelligence requirements that may be addressed through tailored analytical and operational support provided by the respective agency and organization.

2. Non-DOD Members Support

The non-DOD members efforts will primarily focus on strategic intelligence and support to the National Command Authorities (NCA). These agencies identify global and regional issues and threats to the NCA, military leadership, and combatant commanders. This responsibility includes assessing potential issues and situations that could impact US national security interests and objectives. Intelligence provided by these agencies is essential in support of some military operations. These non-DOD members are detailed in paragraph 3 of this chapter. In military operations other than war (MOOTW) involving the use or threat of force, the intelligence provided by the non-DOD members include support to the operations shown in Figure III-1. The intelligence tasks associated with these type of operations are addressed in Joint Pub 2-0, "Doctrine for Intelligence Support to Joint Operations."

3. Non-DOD Members

See Figure III-2.

a. **Central Intelligence Agency**

- **CIA's primary areas of expertise are in human intelligence (HUMINT) collection, imagery, all-source analysis, and the production of political and economic intelligence.** The CIA has four Deputy Directors: Deputy Director for Operations; Deputy Director for Intelligence; Deputy Director for Science and Technology; and Deputy Director for Administration. The DCI is also the head of the CIA, but there is an Executive Director who handles the day-to-day activities of the agency.

- **Office of Military Affairs (OMA).** The OMA falls under the Associate Director of Central Intelligence for Military Support, a flag rank military officer. OMA is staffed by CIA and military personnel. As the agency's single point of contact for military support, **OMA negotiates, coordinates, manages, and monitors all aspects of agency support for military operations.** This support is a continuous process that can be enhanced or modified

Figure III-1. Intelligence Support to MOOTW Operations

to respond to a crisis or developing operation. Interaction between OMA and the DCI representatives to the Office of the Secretary of Defense (OSD), the Joint Staff, and the combatant commands facilitates the provision of national-level intelligence in support of joint operations,

Figure III-2. Nonmilitary Members of the Intelligence Community

contingency and operation planning, and exercises.

- **Foreign Broadcast Information Service (FBIS)**

  •• The FBIS is the primary collector of foreign open-source information for the IC. The FBIS collects comprehensive foreign open-source information on developing world events and trends for

the President, Cabinet, senior US policymakers, and government agencies.

•• FBIS brings the latest foreign political, military, economic, and technical information to the intelligence analysis, warning, and operations processes. FBIS monitors approximately 2,350 publications, 331 radio stations, 153 television stations, 112 news agencies, 70 Internet sources, and 40 data bases in 210 countries and 73 languages.

•• FBIS administers the continental United States (CONUS) and outside the continental United States (OCONUS) installations in support of its mission to collect, translate, analyze, and disseminate information responsive to US policy interests from the world's open-source media, including radio, television, press agencies, newspapers, periodicals, journals, books, maps, data bases, gray literature, and the Internet.

•• In support of and supplementary to the field collection effort, foreign language area specialists at FBIS headquarters systematically review newspapers, journals, and other open-source publications for information of interest to US Government (USG) customers and select the appropriate material for translation and dissemination. Specialist language support is available on a limited basis.

•• The FBIS accepts formal open-source collection tasking from the IC through the HUMINT process. IC customers that want to levy standing open-source collection need to identify their requirements to the National HUMINT Requirements Tasking Center during the formulation or revision of collection directives. Additionally, FBIS accepts formal tasking from the CIA's Directorate of Intelligence Production through the Directorate's Collection Requirements and Evaluation Staff.

•• On a case-by-case basis, FBIS will consider ad-hoc collection tasking requests from IC organizations and agencies (including CIA), depending on available resources. Requests for ad-hoc collection efforts by FBIS should be addressed to the FBIS Information Center, located in Reston, Virginia, for proper referral.

•• FBIS makes available to the IC and other USG agencies the following products and services derived from foreign open-sources: (1) **FBIS Reporting.** FBIS, through its worldwide access to foreign media and other publicly available materials, provides political, military, economic, and technical information. Translation and translations of the information are collectively referred to as FBIS "reporting." FBIS data bases of reporting are accessible either from several worldwide electronic information handling systems that function via the Internet or similar technology, or from one of FBIS' own proprietary mechanisms such as compact disc-read only memory (CD-ROM). (2) **FBIS Observations and Analysis.** FBIS analyzes the content and behavior of the media of countries posing a significant policy interest to the USG's foreign affairs community. (3) **FBIS Video Products.** FBIS provides television program summaries and selected video programs to a limited set of customers. (4) **Foreign Language Glossaries.** FBIS officers skilled in foreign languages produce on an ad-hoc basis glossaries or guides to foreign language terminology, which the National Technical Information Service hosts on its FedWorld service on the Internet (URL: http://www.fedworld.gov/fbis).

(5) **World Wide Guides.** FBIS foreign media experts compile catalogs of information about the electronic and print media of a specific country or region, providing broadcast and circulation figures as well as political affiliations and policy positions. (6) **Maps.** FBIS supports USG analysis, operations, and decision making by providing unclassified reference maps and geographic information. (7) **Publications Procurement.** FBIS procures foreign media and other forms of open-source information, including newspapers, journals, books, newsletters, commercial annual reports, telephone directories, CD-ROMs, and data bases for USG components participating in the Foreign Publications Procurement Program. (8) **Gray Literature Procurement.** FBIS obtains gray literature (publicly available material that cannot be obtained by commercial subscription) in response to specific customer requests and standing collection directives. FBIS maintains the Gray Literature Tracking Data Base, which is available on the Intelink-TS and Open-Source Information System network. (9) **FBIS Operations Center.** The FBIS Operations Center is a 24-hour watch office that serves as a major conduit between FBIS Headquarters, FBIS OCONUS installations, and numerous USG operations centers. (10) **Linguistic Support.** On a fee-for-service basis, FBIS selectively provides a variety of linguistic services to its USG customers, including reverse translations, emergency translations, foreign language instruction, translations from audio and

PROLOGUE TO THE GULF WAR

Although relations between Iraq and Kuwait had, in the past, been affected by the unresolved border issue and the question of ownership of Warbah and Bubiyan islands, Kuwaiti leaders nevertheless were surprised at the antagonism of Saddam Hussein's 17 July 1990 speech commemorating the 22nd anniversary of the 1968 Iraqi revolution. In his speech, Saddam accused Kuwait and the United Arab Emirates of complicity with the United States and Israel in a plot to cheat Iraq out of billions of dollars of oil revenue. The ferocity of the speech caused concern among the Intelligence Community, as did detection of movements of Republican Guard Forces Command units from the Baghdad area towards the Kuwaiti border.

Central Command (CENTCOM), the Defense Intelligence Agency (DIA), the Central Intelligence Agency (CIA), and the National Intelligence Officer for Warning all were monitoring events closely and reporting on their significance. On 23 July 1990, DIA began twice-daily production of Defense Special Assessments on the developing situation. All US intelligence agencies provided detailed reporting on the continuing Iraqi military buildup, and issued warnings of possible Iraqi military action against Kuwait. By 1 August 1990, Iraqi forces between Al-Basrah and the Kuwaiti border included eight Republican Guard divisions supported by at least 10 artillery battalions. This force consisted of almost 150,000 troops, with more than 1,000 tanks and required support forces. That same day, CIA, DIA, and CENTCOM issued warnings that an Iraqi invasion of Kuwait was likely, if not imminent.

SOURCE: Final Report to Congress
Conduct of the Persian Gulf War, April 1992

videos, classified translations, and assistance to treaty monitoring efforts.

b. **Department of State (DOS)**

- **Bureau of Intelligence and Research.** The INR coordinates programs for intelligence, analysis, and research and produces intelligence studies and current intelligence analyses essential to foreign policy determination and execution.

- **Bureau of Politico-Military Affairs.** The Bureau originates and develops policy guidance and provides general direction on issues that affect US security policies, military assistance, nuclear policy, nonproliferation policy, and arms control matters. This office maintains political and military liaison with the Department of Defense and other Federal agencies on a wide range of affairs.

- **Bureau of International Narcotics Matters.** The Bureau develops, coordinates, and implements international narcotics control assistance activities. It is the principal point of contact and provides policy advice on international narcotics control matters for the Office of Management and Budget, the NSC, and the White House Office of National Drug Control Policy (ONDCP). The Bureau also oversees and coordinates the international narcotics control policies, programs, and activities of US agencies.

- **Foreign Service.** Ambassadors are the personal representatives of the President and report to him through the SECSTATE. The President gives the chief of the diplomatic mission, normally an Ambassador, direction and control over all US in-country government personnel except those assigned to an international agency or to a combatant commander.

c. **Department of Energy.** The Office of Nonproliferation and National Security directs the development of the Department's policy, plans, and procedures relating to arms control, nonproliferation, export controls, and safeguard activities. Additionally, this office is responsible for managing the Department's research and development program for verifying and monitoring arms implementation and compliance activities, and for providing threat assessments and support to headquarters and field offices.

d. **Department of Justice (DOJ)**

- **Attorney General.** The Attorney General, as head of the DOJ and chief law enforcement officer of the Federal Government, represents the United States in legal matters and gives advice and opinions to the President and to the heads of the executive departments. The Attorney General is delegated the power to approve the use of any technique for intelligence purposes, within the United States or against a US person abroad, for which a warrant would be required if undertaken for law enforcement purposes.

- **Federal Bureau of Investigation.** The FBI, the principal investigative arm of the DOJ, **has primary responsibility for CI and counterterrorism operations conducted in the United States.** CI operations contemplated by any other organizations in the United States must be coordinated with the FBI. Any overseas CI operation conducted by the FBI must be coordinated with the CIA.

- **Internal Security Section.** This section investigates and prosecutes cases affecting national security, foreign relations, and the export of military and strategic commodities and technology. DOJ has exclusive prosecution responsibility for criminal statutes

regarding espionage, sabotage, neutrality, and atomic energy.

e. **Department of the Treasury.** Intelligence-related missions include the production and dissemination of foreign intelligence relating to US economic policy and participation with the DOS in the overt collection of general foreign economic information.

CHAPTER IV
MILITARY INTELLIGENCE COMMUNITY

"If I always appear prepared, it is because before entering on an undertaking, I have meditated for long and foreseen what may occur."

Napoleon Bonaparte, 1769-1821

1. Introduction

This chapter identifies responsibilities for DOD and joint intelligence agencies and organizations in support of joint operations. There must be a commitment to cooperation and shared purpose based on requirements and capabilities, with the objective of providing timely, relevant, accurate, and predictive all-source intelligence to combatant commanders and subordinate JFCs. This chapter defines Military Intelligence Community responsibilities for any intelligence officer on a staff to use to identify and determine objectives and strategy, assist staff and forces in planning operations, support the conducting of operations, and evaluate the effects of the operations.

2. Responsibilities of the Office of the Secretary of Defense

a. **Secretary of Defense.** As shown in Figure IV-1, **the Secretary of Defense exercises full direction, authority, and control over the intelligence activities of the Department of Defense.** The Secretary of Defense is responsible for collecting, processing, producing, and disseminating military and military-related foreign intelligence and counterintelligence. As a member of the NSC, the Secretary of Defense participates in the development of national-level policy. The Secretary of Defense has a major responsibility to ensure timely development and submission of proposed national programs and budgets.

b. **Defense Intelligence Executive Board (DIEB).** The DIEB is the senior corporate advisory body to the Secretary of Defense for review and oversight of defense intelligence programs and activities. Further, the DIEB is the senior management body providing fiscal and programmatic guidance to the Joint Military Intelligence Program (JMIP). Upon the establishment of the JMIP, the Secretary of Defense created the DIEB as a management mechanism to "...provide effective oversight of Defense Intelligence programs and to make key decisions for efficient allocation of available resources to address Department needs." The DIEB is chaired by the Deputy Secretary of Defense, with the ASD (C3I) serving as its executive secretary. Additional members include the DCI; representatives of the Military Services; a number of senior OSD officials; the Vice Chairman of the Joint Chiefs of Staff; the Director of the Joint Staff; and the directors of all Defense agencies involved in the JMIP.

- **DIEB Issues.** The DIEB provides a forum for discussion and review of existing and emerging issues and challenges for intelligence in support of defense needs and develops immediate solutions when necessary. The composition of this board ensures significant issues are identified and addressed. Through careful corporate examination of defense intelligence capabilities, **the DIEB develops alternatives and recommendations that foster the most effective allocation of these resources.** The board meets not less than twice a year to provide advice and counsel on defense intelligence issues.

- Discussions and advisory guidance focus on requirements, policy, interoperability, resources, priorities, and goals.

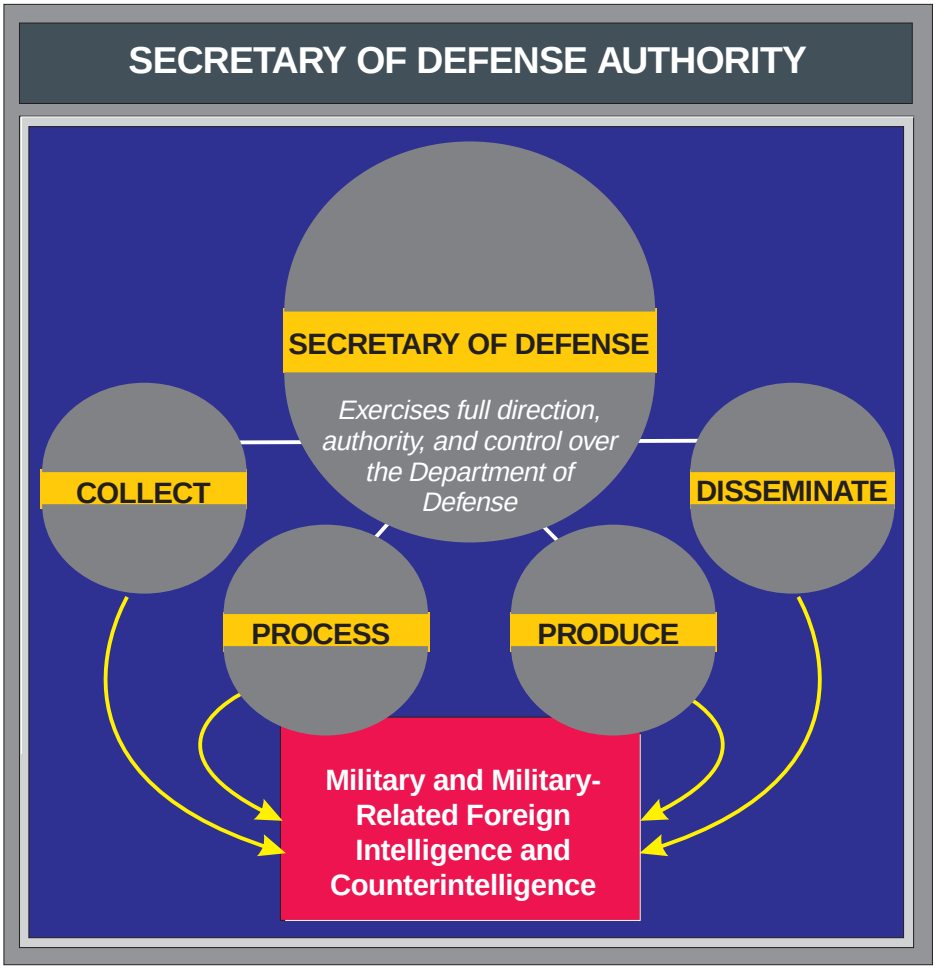


Figure IV-1. Secretary of Defense Authority

c. **ASD (C3I). The ASD (C3I) has as a principal duty the overall supervision of command, control, communications, and intelligence (C3I) affairs of the Department of Defense.** The ASD (C3I) is the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for C3I, information management, information warfare, CI, and security countermeasures matters, including warning, reconnaissance, intelligence and intelligence-related activities conducted by the Department of Defense.

d. **Assistant to the Secretary of Defense (Intelligence Oversight).** The Assistant to the Secretary of Defense (Intelligence Oversight) conducts independent oversight inspections of DOD intelligence and CI activities to ensure compliance with legal requirements and standards of propriety. This office also reviews all allegations that raise questions of legality or propriety involving intelligence or CI activities in the Department of Defense, to ensure that investigations are properly accomplished and appropriate corrective measures are implemented.

3. Military Intelligence Board

a. The Military Intelligence Board (MIB) serves as the senior "Board of Governors" for the

Military IC and works to develop cooperation and consensus on cross-agency, Service, and command issues. The MIB is chaired by the Director of DIA. The membership of the MIB is shown in Figure IV-2.

b. The MIB is a key element involved in guiding and supporting DOD intelligence operations. **The MIB coordinates intelligence support to military operations** and provides a forum for the discussion of issues going before the NFIP, CMS, and other national-level intelligence forums.

c. The MIB may assist in obtaining intelligence support to military operations during periods of crisis or contingency operations within a combatant command's area of responsibility. During Operations DESERT SHIELD and DESERT STORM, the MIB met almost daily to address theater intelligence shortfalls identified by combatant command J-2s and to coordinate the deployment of needed personnel, equipment, and systems to support operations.

Figure IV-2. Membership of the Military Intelligence Board

Intentionally Blank

CHAPTER V
JOINT STAFF J-2

"Great advantage is drawn from knowledge of your adversary, and when you know the measure of his intelligence and character you can use it to play on his weaknesses."

Frederick the Great,
Instructions for His Generals, 1747

1. Introduction

This chapter identifies the responsibilities of the Joint Staff J-2 in support of the Chairman of the Joint Chiefs of Staff and the combatant commands. Additionally, it identifies the responsibilities of the NMJIC in its role as the focal point for all defense intelligence activities in support of joint operations.

2. Joint Staff Intelligence Functions and Responsibilities

a. **The Joint Staff Directorate for Intelligence, J-2, is a unique organization, in that it is both a major component of DIA, a combat support agency, as well as a fully integrated element of the Joint Staff.** Joint Staff J-2 is composed of six deputy directorates, three of which make up the core of the NMJIC: Crisis Management (J-2M), Crisis Operations (J-2O), and Targeting Support (J-2T). The other three deputy directorates are Joint Staff Support (J-2J), Administration (J-2A), and Assessment, Doctrine, Requirements, and Capabilities (J-2P).

b. **Joint Staff J-2 provides all-source intelligence to the Chairman of the Joint Chiefs of Staff, OSD, Joint Staff, and combatant commands which requires it to draw deeply on DIA's broad range of capabilities to accomplish its mission and functions.** J-2 apprises the Chairman of foreign situations and intelligence issues relevant to current operational interests and potential national security policies, objectives, and strategy. This includes providing indications and warning (I&W) and crisis intelligence support, supporting combatant command intelligence requirements, developing joint intelligence doctrine, developing joint intelligence architecture, and providing targeting support to military operations. The Joint Staff J-2 serves as the single coordinating authority with the Department of Defense and IC for the deployment of national-level NISTs.

3. NMJIC

a. To accomplish assigned crisis intelligence functions, the Joint Staff J-2 operates the NMJIC, which is collocated in the Pentagon with the National Military Command Center (NMCC) and Defense Collection Coordination Center (DCCC) (See Figure V-1). The NMJIC is comprised of regional analysts, target analysts, and operations specialists from J-2M, J-2O, and J-2T as noted above. Additionally, the DIA has two elements assigned to the NMJIC; DCCC (from the Collection Requirements Division), and Terrorism Threat Warning Division. **The NIMA Pentagon Operations Center is also an integral component of the NMJIC, as are elements of CIA, NSA, representatives of the Services and, as required, other federal agencies. The mission of the NMJIC is to provide defense intelligence support and the earliest possible warning on developing situations which may threaten US interests for the NCA, OSD,**

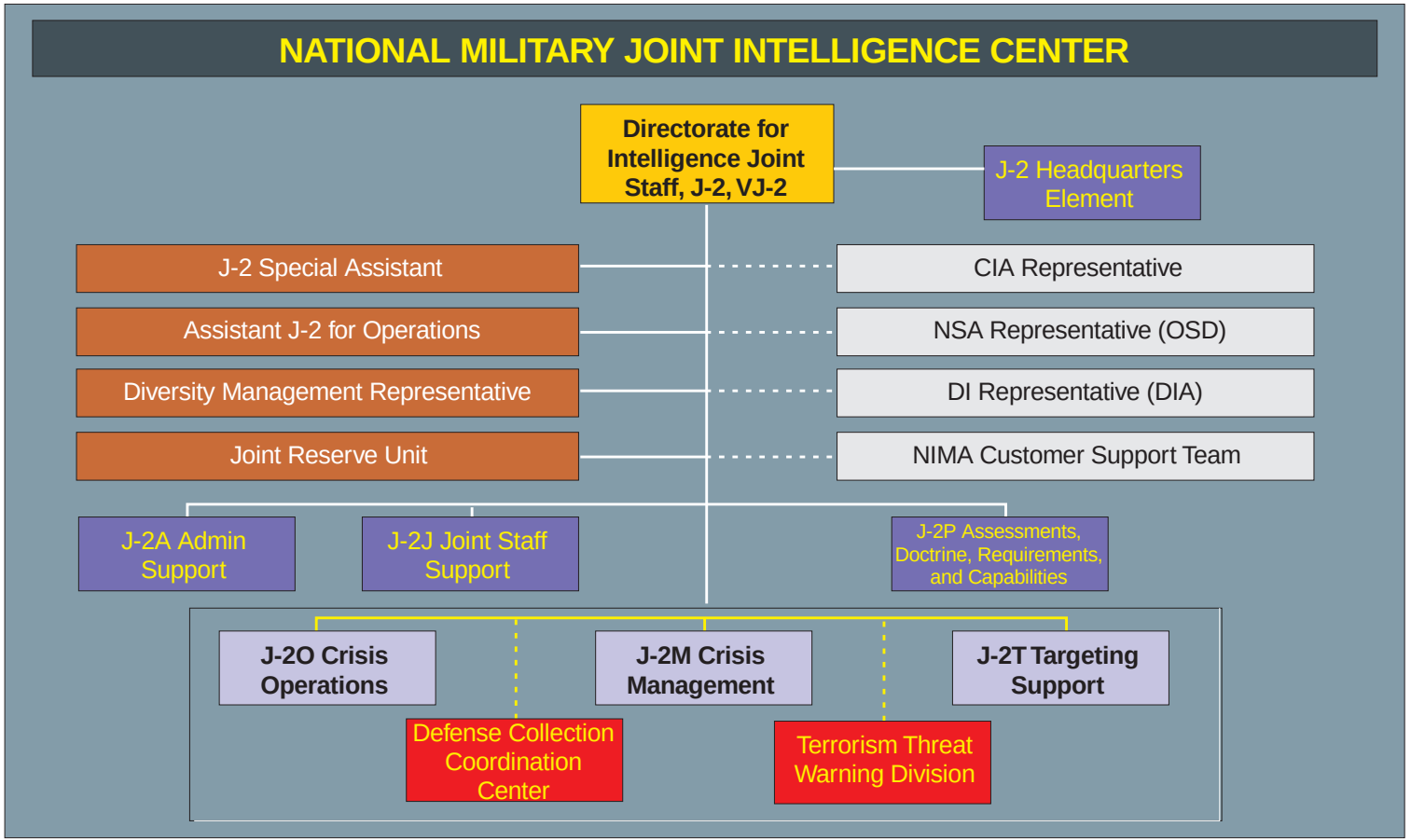


Figure V-1. National Military Joint Intelligence Center

Chairman of the Joint Chiefs of Staff, Joint Staff, combatant commands (through their JIC and/or JAC), and Military Service secretaries and chiefs during peace, crisis, and war. As such, the NMJIC is the permanent DOD Crisis Intelligence and I&W Center, a critical element in fulfilling the national intelligence community's priority mission of crisis support to military operations. The NMJIC orchestrates the responsiveness of all national sensors and collection assets to ensure complete, mutually supportive target coverage and immediate reporting of events. It supports the combatant commands and their subordinate joint forces in exercising their wartime missions and deploys special teams to facilitate national support during crises. As the DOD focal point for crisis intelligence, the NMJIC draws upon its centralized "all-Service, all-agency, all-source" resources and capabilities. Moreover, the NMJIC is recognized as the national focus for military intelligence issues for the entire IC, with particular emphasis on crisis management and operations. The current mission and configuration of the NMJIC reflects the changing nature of intelligence support to contingency operations in the dynamically evolving world environment. The mission of the NMJIC includes providing intelligence support to selected multinational organizations in situations where there is an imminent threat to the life and safety of multinational personnel worldwide, and in other prescribed situations. The NMJIC is also the focal point within the IC for military intelligence support to selected peacekeeping and humanitarian operations, and to civilian agencies involved in emergency and disaster relief operations.

b. **Deputy Directorate for Crisis Management, J-2M.** J-2M provides direct analytical and intelligence support to the NMCC through the NMJIC Alert Center, a 24-hour all-source, multi-discipline intelligence center which monitors and reports on current and emerging crisis situations. **The Alert Center Deputy Director for Intelligence represents the Director, J-2 and the DIA during non-duty hours** and provides military and crisis intelligence continuity for other intelligence producers and national-level decision makers. If a developing crisis situation escalates into a crisis, the relevant Alert Center regional desk officer is augmented with analytical support, or an intelligence working group (IWG) or intelligence task force (ITF) is formed. Thus, support may range from one additional analyst through an extended IWG to a 24-hour IWG or ITF.

- **Request for Information Desk.** The NMJIC Alert Center Desk **provides positive control and direct management of crisis-related and time-sensitive RFIs** requiring national-level intelligence products in support of warfighters, planners, and decision makers. The RFI Desk is responsible for validating and managing all crisis, emerging crisis, and time-sensitive (responses required within 24 hours) RFIs. The RFI Desk assigns requirements to the appropriate national producer in accordance with the DOD Intelligence Production Program (DODIPP) and/or direct coordination and ensures that products and responses are timely and satisfy the requester's needs.

- **Intelligence Working Group.** As a crisis develops an IWG may be established within the NMJIC Alert Center **to provide focused coverage of crisis requirements**. When established, an IWG is announced through worldwide message dissemination, complete with address identification and telephone numbers. Specifically the IWG:

  •• Is formed at the lowest level of response to a particular crisis situation;

  •• Provides all-source intelligence on the crisis situation to the NCA, Chairman

of the Joint Chiefs of Staff, Joint Staff, Services, combatant commands, and deployed operational forces; and

•• Is normally manned from J-2 and DIA with dedicated Reserve support.

- **Intelligence Task Force.** If a crisis situation continues to escalate, the Joint Staff J-2 may decide to form an ITF to provide stronger focused all-source intelligence support. **The size of the ITF depends on the severity, complexity, and duration of the crisis and may be formed using an IWG as its core.** Figure V-2 displays a basic ITF organization. NSA, NIMA, CIA, the Services, and other major government organizations generally augment an existing IWG to form an ITF. Like the IWG, an ITF is announced by message with worldwide distribution. While an IWG normally precedes the formation of an ITF, in a rapidly evolving crisis (e.g., a major military clash) an ITF may be formed immediately, bypassing the establishment of an IWG. **The ITF focuses intelligence resources, answers RFIs, expedites dissemination of intelligence, and provides rapid responses to special tasking.** Specifically, the ITF:

•• Is convened by the Joint Staff J-2 whenever a crisis action team (CAT) is convened by the Operations Directorate, Joint Staff (J-3) (An ITF may be convened by the J-2 without a CAT being convened if it is required to support the NMJIC. However, when the J-3 forms a CAT, the primary mission of the IWG and/or ITF will be to support the Joint Staff.);

•• Provides time-urgent responses to requirements from the NCA, OSD, Chairman of the Joint Chiefs of Staff,

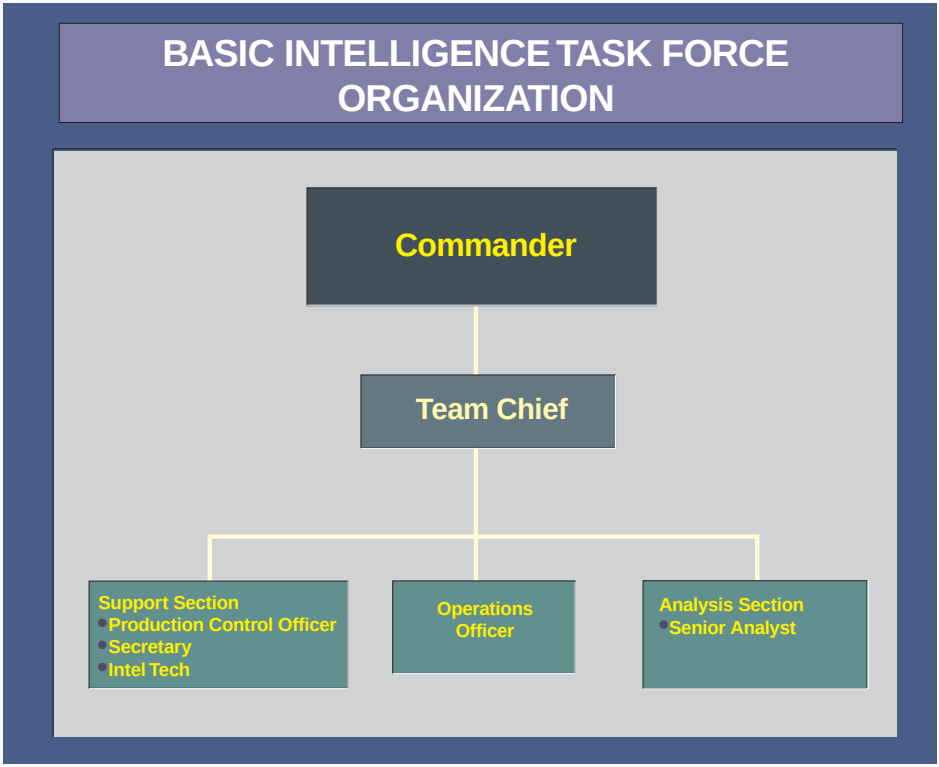


Figure V-2. Basic Intelligence Task Force Organization

A NIST can be requested by a JTF to supply needed information, such as this artist's concept of the Tarhunah underground chemical plant in Libya.

Joint Staff, Military Services, combatant commands, and deployed operational forces;

•• Provides timely warning to the NCA, OSD, Chairman of the Joint Chiefs of Staff, Joint Staff, Military Services, and the combatant commands of hostilities or potential threats to US interests in the ITF's area of concern;

•• Develops and tailors an all-source intelligence collection strategy plan for the DOD response to the crisis;

•• Responds to requirements from other USG agencies responsible for crisis response activities;

•• Responds to requirements of the United Nations and/or foreign governments consistent with DCI guidelines, and in coordination with the DIA Foreign Disclosure Office; and

•• Coordinates tasking of other USG agencies in support of the NCA, Chairman of the Joint Chiefs of Staff, combatant commanders, JTF commander, and other consumers.

c. **Deputy Directorate for Crisis Operations, J-2O. The J-2O serves as the Joint Staff J-2's executive agent for all NISTs.** The NIST is a nationally sourced team composed of intelligence and communications experts from DIA, CIA, and NSA or other IC agencies as required. **The mission of the NIST is to provide a tailored national-level, all-source intelligence team to deployed commanders during crisis or contingency operations.**

- **Key Functions**

  •• The NIST can provide coordination with national intelligence agencies; analytical expertise; I&W; special assessments; targeting support; access to national data bases; and facilitate RFI management.

  •• The Joint Staff J-2 is the NIST program manager.

•• The Chairman of the Joint Chiefs of Staff deploys the NIST.

- **Deployment Policy.** A NIST is designed to support intelligence operations at the JTF headquarters and is traditionally collocated with the JTF J-2. Support from national agencies is requested by the combatant commander. A request message is forwarded to the Director of the Joint Staff and staffed by the Joint Staff J-2.

- **Participants. The National Intelligence Support Division, Joint Staff, manages the program which involves personnel selection, training, deployment, and support while deployed and redeployed**; respective intelligence agencies are responsible for their member's selection and training.

- **Team Composition and Size.** The Joint Staff J-2 selects the NIST team chief from nominations submitted by participating agencies. The program selects volunteers who are trained and prepared for deployment as a crisis emerges. Teams are composed of agency elements (e.g., NSA, DIA, NIMA, and CIA elements), each under the direction of a team leader. Prior to each deployment, team composition is tailored to ensure it meets the needs of the JTF and to eliminate duplication of skills and functions. **Throughout its tenure, the size and composition of the team will be reviewed and modifications may occur.** Any changes will be done in coordination with the supported command.

- **Required Command Support**

  •• A NIST is not a totally self-contained element; rather it requires logistic and other support from the supported command. **Each NIST deployment is unique based on mission, duration, team composition, and capabilities required.** A NIST requires power, billeting, and automated data processing (ADP) technical support; a full NIST requires a private, access-controlled area within a sensitive compartmented information (SCI) facility work environment, dedicated secure communications (minimum is 64 kilobits per second [kbps] for Joint Deployable Intelligence Support System [JDISS] only; a full NIST requires a T-1 line, 1.544 megabits per second [mbs]), and "expendable" administrative supply items.

  •• **Transportation.** The supported command must provide intratheater transportation of personnel and equipment from the CONUS marshalling area to the operating area during initial deployment and redeployment. The NIST is responsible for transportation from the Washington, DC area to the marshalling area.

  •• **Logistics.** Billeting and mess, if commercially available, will be funded by each respective agency. The supported command provides berthing and messing facilities if the team is living in field conditions or is onboard a ship. The supported command will provide mission specific military equipment (non-standard TA-50 gear, i.e., cold weather gear). Vehicle lift from the airhead may be required dependent on the equipment and communications package deployed. If vehicles are deployed, the supported command provides required fuel and maintenance.

- **NIST Deployed Communications Capabilities.** The NIST is designed to provide a full range of intelligence support to a commander, joint task force (CJTF), from a single agency element with limited ultra high frequency (UHF)

voice connectivity to a fully equipped team with JDISS and Joint Worldwide Intelligence Communications System (JWICS) video teleconferencing (VTC) capabilities. Current methods of operation continue to rely on both agency and command-provided communications paths (i.e., bandwidth) to support deployed NIST elements. The systems that each elements are capable of deploying are discussed in greater detail in Appendix C, "NIST Systems."

- **NIST and JTF Command Relationship. The NIST is deployed in direct support of the JTF J-2 and will perform functions as so designated.** All intelligence generated by the NIST is available to the J-2 organization and CJTF, with the usual restriction based on clearance and programs. Each element leader and the NIST team chief may conduct liaison with parent organizations.

  •• NIST members will not serve as a substitute for normal military intelligence staffing nor as substitutes for augmentation. **The NIST team chief is responsible for the general employment of the NIST.** The element leaders are primarily involved in the intelligence liaison and agency representation.

  •• As the supported organizations request information or finished products from their NIST, the requirement is discussed and deconflicted within the team to determine which element(s) should respond to the tasking.

  •• The NIST team chief will ensure that only time-sensitive RFIs are directly transmitted to the NMJIC RFI Desk and that the command's intelligence center (JIC and/or JAC) is kept informed simultaneously through the COLISEUM RFI management system. **This time-sensitive "reachback" capability is not intended as a "skip echelon."**

  •• **Director of Central Intelligence Directive (DCID) 1/7.** This DCID **provides for the dissemination of originator-controlled material**. The DCI representatives at the combatant commands and the NIST can determine the secondary and follow-on dissemination of products.

An external view of the Tactical Satellite System operated by Alpha Company, 44th Signal Battalion located on Taszar Airfield.

d. **The Defense Collection Coordination Center**, an element of the Requirements Management Division, **is collocated with the NMJIC in the Pentagon and provides tasking interface and expert advice to the NMJIC**. Operating 24 hours a day, the DCCC facilitates timely and responsive management, coordination, validation, approval, and submission of all-source time-sensitive collection requirements supporting the combatant commands, Joint Staff, DIA, Military Services, and other DOD organizations. The DCCC provides direct support to the J-2 NMJIC analysts, ITFs, and IWGs. As the DOD focal point for time-sensitive collection, the DCCC serves as the information base for questions regarding time-sensitive collection issues. Specific responsibilities include:

- Managing the submission of time-sensitive collection requirements to satisfy user needs;
- Formulating and validating time-sensitive intelligence collection and reporting requirements in coordination with the user; and
- Assigning appropriate priorities to available collection and reporting resources.

e. **Deputy Directorate for Targeting Support, J-2T.** Within the Joint Staff J-2, **J-2T is the single DIA manager and point of entry for national-level target intelligence support for conventional, special, and technical operations to the Joint Chiefs of Staff (JCS) and combatant commands, including crisis response and deliberate planning requirements. J-2T is responsible for the development, coordination, and maintenance of joint target intelligence policy, standards, and procedures**, to include Target Materials Production Programs and battle damage assessment (BDA). It functions as the Defense Intelligence Issue Coordinator for Targeting Support, assessing and leveraging the collective resources and capabilities of the IC to satisfy target intelligence requirements. Additionally, J-2T operates the NMJIC Targeting and BDA Cell, which is the single national-level source of targeting and BDA support to the JCS and combatant commands. To accomplish its mission, J-2T is organized in two divisions.

- **Target Operations Division, (J-2T-1). J-2T-1 coordinates all national-level target intelligence support for contingency operations and deliberate planning for the Joint Staff and combatant commands.** This Division focuses the national intelligence community efforts for conventional and special targeting. Operational targeting support done by the Division is divided into four categories: contingency operations; coordination of targeting community efforts; providing targeting expertise to the Joint Staff; and national-level BDA.

  •• **Contingency Operations Support.** Targeting support is provided during peacetime and crisis to the national-level, combatant commands, and the supported commands. Daily coordination is ongoing with the supported command to assist in crisis response or deliberate planning efforts. Target book data is provided as requested to the supported command.

  •• **Coordination of National Targeting Community Efforts.** J-2T-1 coordinates DIA, NSA, CIA, and Joint Command and Control Warfare Center (JC2WC) expertise to ensure best target intelligence information is distributed. During the command target development process J-2T-1 coordinates all national-level input to the command.

•• **Battle Damage Assessment.** The Division is the focal point for national-level BDA and leads the NMJIC Targeting and BDA Cell with membership from NSA, DIA, CIA, Joint Warfare Analysis Center (JWAC), and JC2WC at a minimum. In addition, J-2T-1 provides exercise and operational national-level BDA support to the combatant commands; coordinates and provides the community assessment to the Joint Staff J-2, Chairman of the Joint Chiefs of Staff, and NCA; and coordinates munitions effectiveness and weaponeering analysis.

- **Target Plans Division, (J-2T-2).** J-2T-2 develops joint target intelligence policy, standards, procedures, and requirements for all aspects of targeting, to include BDA and information operations (IO). It ensures standardized joint targeting intelligence techniques, automated targeting tools, and commonly accepted methods. As the Targeting Issue Coordinator for DIA and the Joint Staff J-2, the Division hosts national-level fora for developing and validating these target intelligence-related products, standards, and requirements. The Division is organized into four primary areas: automation development; doctrine and policy; future concepts; and IO.

•• **Automation Development.** J-2T-2 is responsible for establishing and managing functional requirements for joint targeting systems. It is responsible for integrating new technologies into the targeting process. The Joint Targeting Automation Steering Group, which provides a forum to establish and prioritize combatant command and Service targeting automation requirements, is chaired by this Branch.

•• **Doctrine and Policy Development.** The Division, in coordination with J-2P, is responsible for developing evolving joint targeting doctrine. Additionally, in conjunction with the Services and combatant commands, J-2T-2 establishes joint targeting policy. To facilitate this process, it chairs the Military Target Intelligence Committee and the Battle Damage Assessment Working Group. It manages the worldwide US and allied Target Material Program and establishes policy, standards, and specifications for Target Materials, to meet the needs of the US and allied forces.

•• **Future Concept Development.** This section is responsible for developing joint targeting vision, which entails long-term estimates of future operations and the impact of these on targeting.

•• **Information Operations Targeting Development.** This section is responsible for integrating changes brought about by the revolution in Military Affairs. It provides mid-term solutions to fully integrating information operations into the joint targeting process.

f. **Deputy Directorate for Administration. J-2A focuses on all personnel, budget, manpower, and infrastructure issues for the Joint Staff J-2.** All J-2 personnel and security issues are centralized in this Directorate to support J-2 and the IC representatives resident in the NMJIC. It is the central clearinghouse for all ADP requirements necessary to support the J-2 and its operations.

g. **Deputy Directorate for Joint Staff Support. J-2J serves as the DIA focal point for supporting the Chairman of the Joint Chiefs of Staff**, maintains close relationships

with all offices of the Joint Staff, and ensures prompt and responsive DIA participation and support in intelligence matters. **J-2J also serves as the Joint Staff J-2 Military Secretariat**, and receives, tasks, monitors, votes, and ensures suspense dates are met on all Joint Staff actions. **Additionally, J-2J manages the Defense Intelligence Support Officers assigned to the combatant commands, US Forces Korea, and Supreme Headquarters Allied Powers Europe and North Atlantic Treaty Organization (NATO) Headquarters**. Each Defense Intelligence Support Office (DISO) includes a Senior DIA Intelligence Officer, who serves as the personal representative of the DIA Director and as DISO Chief; an administrative assistant; and a varying number of DIA functional intelligence specialists based on the needs of the combatant command. **With the Senior DIA Representative serving as the Agency's primary liaison officer**, other DISO members provide intelligence support skills and services normally available in each command. The DISO organization enhances and expedites the exchange of information covering the broad spectrum of intelligence operations between DIA and the supported command.

h. **Deputy Directorate for Intelligence Assessments, Doctrine, Requirements, and Capabilities. J-2P assesses joint warfighting intelligence, surveillance, and reconnaissance (ISR) capabilities for the CJCS Joint Requirements Oversight Council (JROC) to assist JCS prioritization of high-payoff capabilities. J-2P also develops joint intelligence doctrine, architectures, strategies, and policies that directly support combatant commands and subordinate JFCs worldwide.** Specific responsibilities include the following.

- Leading and conducting the ISR Joint Warfighting Capability Assessments (JWCAs) for the JROC; acting as the secretariat for the ISR JWCA; and providing management and guidance and developing consensus among the IC, combatant commands, Services, Defense agencies and organizations, and OSD.

- Integrating existing studies, data, and analyses for assessments of baseline ISR capabilities and programs; developing a future vision of ISR support to joint warfighting; identifying gaps in capabilities and shortfalls in ISR systems and programs; and recommending improvements and new initiatives for consideration by the JROC and OSD in their development of the key CJCS and SecDef planning and programming guidance.

- Developing capabilities to perform comprehensive analyses of ISR requirements, capabilities, and resulting architectures; developing and maintaining an interactive, multimedia and data access system; and providing all-source intelligence information, sensor characteristics, command, control, communications, computers, and intelligence (C4I) data, organizational relationships, equipment quantities and locations, and associated programmatic information to support assessments of ISR architectures.

- Ensuring that joint intelligence doctrine and intelligence support to information operations are structured to support forces operating during war.

- Developing and maintaining joint, multinational, and combined intelligence doctrine, tactics, techniques, and procedures.

- Conducting liaison with the IC, including representing and monitoring the defense intelligence community and combatant commands or Service requirements for intelligence and intelligence-related capabilities and systems.

- Ensuring that joint intelligence requirements are incorporated in both DCI and DOD planning, programming, and prioritization documents.

- Serving as the Intelligence Requirements Certification Office for the Defense IC.

- Coordinating and facilitating military intelligence issues between the military intelligence and command and control (C2) communities.

- Representing the Joint Staff J-2 in the programmatic and budgetary review of proposed and/or operational community and Defense intelligence programs.

- Participating in the development of DCI, SecDef, and CJCS program guidance documents.

Intentionally Blank

CHAPTER VI
DEFENSE INTELLIGENCE AGENCY

"Knowledge of the country is to a general what a musket is to an infantryman and the rules of arithmetic are to a geometrician. If he does not know the country he will do nothing but make gross mistakes. Therefore study the country where you are going to act."

Frederick the Great
Instructions for His Generals, 1747

1. Introduction

The DIA is a combat support agency and a major collector and producer in the defense intelligence community. The DIA is responsible for military and military-related intelligence requirements of the Secretary of Defense and Deputy Secretary of Defense, Chairman of the Joint Chiefs of Staff, other DOD components, and non-DOD agencies of the federal government when appropriate. It also provides the military intelligence contribution to national foreign intelligence and counterintelligence. Its mission is to provide timely, objective, and cogent military intelligence to the warfighters — and to the DOD and USG decision makers and policymakers. This chapter discusses the DIA's responsibilities to provide intelligence capabilities and systems for near-real-time support of crisis, contingencies, and military operations.

2. DIA Responsibilities and Functions

DIA plans and directs, collects, processes and exploits, analyzes and produces, disseminates and integrates, and evaluates military intelligence for the Department of Defense. The DIA's support to policymakers focuses on developing national-level intelligence assessments, presenting and providing perspectives for defense policy, and providing I&W of potential crisis.

a. **Responsibilities.** The Director, DIA advises the Secretary of Defense and Deputy Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, and ASD(C3I) on all matters concerning military and military-related intelligence; is the principal DOD intelligence representative in the national foreign intelligence process; and, with the agreement of the heads of DOD intelligence components, is responsible for coordinating the budgeting and allocation of DOD intelligence component personnel and resources to satisfy DOD intelligence requirements. The DIA's support flows across the range of military operations to include; counterterrorism, counterdrugs, medical intelligence, weapons of mass destruction and proliferation, United Nations peacekeeping and coalition support, missile and space intelligence, noncombatant evacuation efforts, targeting, and BDA. The DIA responsibilities include the following.

- Providing peacetime, crisis, contingency, and combat intelligence support to the operational military forces.
- Providing military intelligence support for the policy and planning activities of DOD components and, as appropriate, for similar activities of non-DOD national authorities.
- Planning, programming, and budgeting activities in support of DOD intelligence

missions to include the following (see Appendix D, "Intelligence Resource Programs," for greater detail on the individual programs).

•• Serving as the Program Manager of the General Defense Intelligence Program (GDIP); developing the GDIP as an input to the NFIP; participating in the NFIP approval process; and overseeing execution of funds appropriate for GDIP and GDIP-related activities.

•• Preparing and submitting the DIA program and budget input to the GDIP, the DOD Foreign Counterintelligence Program, and the JMIP.

•• Serving as the program coordinator of the Defense General Intelligence and Applications Program (DGIAP) of the JMIP.

•• Assembling and developing statements of military intelligence requirements and related plans, programs, and budget proposals, and advising the Chairman of the Joint Chiefs of Staff, ASD(C3I), DCI and other DOD components, as appropriate.

•• Responding to requests by the ASD(C3I) and Chairman of the Joint Chiefs of Staff to review and provide recommendations concerning planning, programming, budgeting, and the use of intelligence resources for collection and production of intelligence in support of planning and operations requirements of the military forces in peacetime, crisis, contingency, and combat situations.

- Providing representation on national and international fora.

- Conducting intelligence activities for which DIA is assigned responsibility, the implementation of which require personnel and resources from one or more of the other DOD intelligence components, and exercising the degree of direction and control over these personnel resources that is required to accomplish the purpose of the activities.

- Fostering jointness in the activities of the DOD intelligence components and enhancing coordination among these components.

- Fostering interoperability of all DOD intelligence systems at all levels.

- Providing support to the Chairman of the Joint Chiefs of Staff for, and participating in, the implementation of sensitive support programs.

- Coordinating and, when appropriate, developing and executing intelligence operation plans.

b. **Organization.** The DIA is organized into six directorates and the Joint Military Intelligence College, in addition to the staff comprising the Command Element (See Figure VI-1). The Directorate for Intelligence, Joint Staff was discussed in Chapter V, "Joint Staff J-2," of this publication. The other Directorates and the College are discussed below.

- **Directorate for Intelligence Production (DI).** The DI produces the broadest range of intelligence for all joint operations of any organization in the Intelligence Community. As the Functional Manager for Production, DI also manages the production of military intelligence throughout the Defense Intelligence Community in response to the needs of DOD and non-DOD customers. In anticipation of crisis and during crisis or deployed US military operations, DI leverages analytic

Figure VI-1. Defense Intelligence Agency Organization

expertise through the Defense Intelligence Community and, where appropriate, from non-Defense agencies to support joint operational needs. DI directs analytical elements in Washington, DC and the production efforts of two field production activities; Armed Forces Medical Intelligence Center (AFMIC) and Missile and Space Intelligence Center (MSIC). The Operational Intelligence Coordination Center (OICC), located in the Defense Intelligence Analysis Center (DIAC), serves as the crisis management office for the DI in direct support to the DIA and/or J-2 and is the single point of contact in DI for requirements involving analytical support during crisis situations and for sustained military operations. Response times are driven by criticality, time sensitivity, and requester priority. The OICC transitions to 24-hour operations as required, and the size and number of OICC watch teams varies depending upon the nature and duration of each crisis. DI's Information Warfare Support Office conducts intelligence preparations of the battlespace, foreign threat assessments, and analysis of foreign deception. Other responsibilities include the following.

•• Participating in and supporting, as appropriate, the activities of the Defense Special Missile and Astronautics Center, IC centers, committees, and working groups established by the DCI and comparable activities established by the Secretary of Defense.

•• Preparing intelligence assessments and estimates concerning transfers of technology, goods, services, and munitions (including associated transfer mechanisms) and participating in interagency, national, and international fora on such transfers.

•• Establishing product standards for, exercising technical and quality control over, overseeing the establishment of requirements for, and managing the non-duplicative scheduled and unscheduled production of integrated scientific and technical and general military intelligence for all DOD intelligence components.

•• Establishing and maintaining a DOD-wide system of DODIPP.

•• Supporting the DOD weapons acquisition process by producing threat assessments within DIA (or validating assessments produced by other DOD intelligence components) for all major DOD acquisition programs. This includes maintaining strong scientific programs within the Department of Defense supporting the acquisition process.

•• Establishing and conducting research and development and testing and evaluating programs and projects, as appropriate, to accomplish the DIA mission.

•• Managing the execution of the Foreign Material Program, except for those acquisition and exploitation activities for which the NSA and ASD(C3I) have primary responsibility.

•• **Armed Forces Medical Intelligence Center.** The AFMIC, located at Ft. Detrick in Frederick, Maryland, is **the only Tri-Service medical intelligence organization within the USG.** The AFMIC products are tailored to the unique requirements of deployed operational forces but are also widely used by national-level policymakers and the acquisition community. Mission responsibilities include the production of finished, all-source, medical intelligence in support of the Department of Defense and its components, national policymakers, and other federal government agencies. Assessments, forecasts, and data bases are prepared on foreign military and civilian health care capabilities and trends, worldwide infectious disease occurrence, global environmental health risks, and military significant life science technologies.

•• **Missile and Space Intelligence Center.** The MSIC, located on Redstone Arsenal near Huntsville, Alabama, **provides current and comprehensive scientific and technical intelligence to US decision makers, weapon system developers, and combatant commanders**. It develops and disseminates intelligence concerning the threat from offensive and defensive guided-missile systems, directed-energy weapons, selected space programs and/or systems and related command, control, and communications to support operationally deployed forces and the material acquisition process. Additionally, it develops and distributes digital threat simulations to force developers and operational forces.

• **Directorate for Intelligence Operations (DO).** The DO **manages**

collection requirements and operations and ensures the effective acquisition and application of all-source intelligence collection resources to satisfy DOD collection requirements. **The DO also directs all non-tactical DOD HUMINT activities through the Defense HUMINT Services (DHS), and measurement and signature intelligence (MASINT) activities through the Central MASINT Office.** In addition to providing HUMINT collection support, DHS deploys forward HUMINT Support Elements to each combatant command to provide a conduit for coordination with DHS, to ensure the J-2 is fully informed of DHS activities, and to assist the command in obtaining HUMINT support. HUMINT operating bases and locations around the world also meet joint information requirements. DHS provides HUMINT resources in response to joint force requirements which may include augmenting a joint force J-2 CI/HUMINT staff element and/or HUMINT Operations Cell and deploying special collection teams. The DHS also manages the worldwide Defense Attaché System. Defense attachés observe and report military and political-military information of interest to the Joint Staff, Services, the Department of Defense, and combatant commands. Other responsibilities include the following.

•• Validating, registering, and recommending priorities for military intelligence requirements; assigning collection responsibilities; and monitoring the application of DOD collection resources, other than signals intelligence (SIGINT) and imagery intelligence (IMINT) resources, to such requirements.

•• Overseeing the development, procurement, and operation of military intelligence collection systems funded in the GDIP, and developing recommendations for future systems.

•• Implementing national intelligence collection tasking authority after such authority is transferred from the DCI to the Secretary of Defense in crisis and/or conflict situations.

•• Serving as the Collection Fund Manager to ensure funding and manpower for valid joint resource requirements.

- **Directorate for Information Systems and Services (DS).** The DS provides information systems and services to the IC in support of warfighters, national policymakers, and defense acquisition authorities. Its functions include ADP and communication engineering development integration and operations for DIA and the IC; information library services, hardcopy and electronic publication and dissemination; video and visual information services; GDIP intelligence infrastructure functional management; and DOD Intelligence Information System (DODIIS) planning, engineering, and life-cycle management efforts. Additional responsibilities include the following.

•• Overseeing the research and development, procurement, and operation of DOD intelligence infrastructure-related programs, systems, and activities funded in the GDIP, to include printing, processing, communications, and information systems.

•• Providing centralized intelligence dissemination services and supervising a DOD-wide intelligence dissemination system.

•• Serving as the Executive Agent for NIMA responsible for imagery

processing, storage, retrieval, and dissemination.

- **Directorate for Policy Support (DP).** The DP, located in the Pentagon, is responsible for ensuring that all requirements for military intelligence support to the Secretary of Defense and senior policymakers in the Department of Defense are satisfied. DP's defense intelligence officers, with regional and function responsibilities, provide the bridge between policy consumers, intelligence collectors and the J-2. They routinely interface with the IC, the Services, the unified commands and substantive analysts in bringing together intelligence-policy perspectives. DP is the central authority for all DOD activities related to non-SIGINT and non-IMINT intelligence agreements and arrangements with foreign governments, allies, and international organizations. It also serves as the single authority for all disclosures of DIA information to foreign governments and international organizations. DP's Defense Intelligence Liaison Offices interface with the Commonwealth nations (Canada, Australia, and the United Kingdom (UK)) in the sharing of intelligence impacting on joint operations. The Policy Support Directorate also manages special access programs in support of the OSD, JCS, the Services, and the commands.

- **Directorate for Administration (DA). DA develops and implements DIA personnel management policies, procedures, and programs.** DA provides support for Agency missions for training and career development of personnel, manages the support services in the areas of engineering, logistics, travel, space management, and facilities maintenance.

  •• DA operates the Joint Military Intelligence Training Center (JMITC). JMITC provides strategic and joint intelligence training in resident and non-resident modes to DIA, the unified commands, the Military Services, other DOD components, and other federal agencies. It also provides DOD-wide oversight of general intelligence training; functional management for GDIP-funded intelligence training; and validation of DOD general intelligence training requirements.

  •• Within DA, the Counterintelligence and Security Activity (DAC) manages security and CI programs to safeguard DIA personnel, information, facilities, systems, and operations. This includes operating as the focal point for all joint counterintelligence issues arising from or in support of the Chairman of the Joint Chiefs of Staff and combatant commanders. It provides CI analysis, production, and staff support to OSD, the Chairman of the Joint Chiefs of Staff, unified commands, Defense agencies, DOD special activities, and the National Intelligence Community for assigned regions. DAC also implements SCI security policy within the Department of Defense, and it develops and publishes security policy manuals, regulations, and handbooks for the Department of Defense. The overseas branch provides tailored technical security support and monitors the threats to the security of US customers.

- **Joint Military Intelligence College (MC).** The College, located at the DIAC, educates military and civilian intelligence professionals who satisfy intelligence requirements as full partners in safeguarding and advancing the nation's interest. A regionally accredited

institution, the College is authorized by Congress to award two degrees, the Master of Science of Strategic Intelligence and the Bachelor of Science in Intelligence. Its educational programs prepare military and civilian personnel for command, staff, and policymaking positions. The College manages an intelligence research program that conducts and disseminates relevant academic research on topics of significance to present and future intelligence missions.

- **Director, Military Intelligence Staff.** The Director, Military Intelligence Staff (DM), which is part of the Command Element, provides the Director, DIA, with plans, policies, and programs to manage resources that support military intelligence. DM serves as the management office for all matters affecting the military intelligence community, coordinating with OSD, Office of Management and Budget, CMS, Services, Defense agencies, and Congress.

Intentionally Blank

CHAPTER VII
NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

"Communications dominate war; broadly considered, they are the most important single element in strategy, political, or military."

Mahan
The Problem of Asia, 1900

1. Introduction

The National Security Agency and its Central Security Service (CSS) ensure cryptologic planning and support for joint operations. This chapter describes the support responsibilities of NSA/CSS, the corresponding coordination responsibilities of the supported commands, and the mechanisms and communications systems that NSA/CSS has developed for interfacing with military forces.

2. NSA/CSS Responsibilities

The NSA/CSS, working with the tactical cryptologic units of a command, provides SIGINT and information security (INFOSEC), encompassing communications security (COMSEC) and computer security as well as telecommunications support and operations security (OPSEC). The people and equipment providing SIGINT, INFOSEC, and OPSEC constitute the United States Cryptologic System (USCS). The NSA/CSS, through the USCS, fulfills cryptologic command and/or management, readiness, and operational responsibilities in support of military operations according to the SecDef tasking, priorities, and standards of timeliness.

a. To meet command and management responsibilities, NSA/CSS and the USCS will perform the following functions.

- Operationally control the SIGINT activities of the USCS and execute the responsibilities of the Secretary of Defense as Executive Agent for US INFOSEC and interagency operations security training.

- Function as the SIGINT and INFOSEC advisor to the Secretary of Defense and the Chairman of the Joint Chiefs of Staff. Provide cryptologic advice and assistance to the unified combatant commands and other military commands through NSA/CSS representatives at those locations.

- Determine, in conjunction with the combatant commanders and subordinate JFCs, when the Director, National Security Agency (DIRNSA) and Chief, CSS should delegate SIGINT operational tasking authority to an appropriate commander.

- Implement programs and initiatives that promote interaction among national and tactical cryptologic assets.

b. To meet readiness responsibilities, NSA/CSS and the USCS will perform as follows.

- Respond comprehensively, directly, and quickly to the validated and prioritized readiness information requirements of military commanders.

- Ensure the designated wartime and contingency cryptologic resources productively support appropriate readiness requirements.

- Promote programs and provide technical support to the Chairman of the Joint

Chiefs of Staff, the Chiefs of the Services, and the combatant commander on SIGINT, INFOSEC, and OPSEC to enhance mission effectiveness.

- Provide security assessments to assist the military in determining the vulnerability of their information systems.

- Assist the Services in developing information systems security; evaluating and developing information system architectures and standards; managing associated encryption systems; designing secure internetting architectures, standards and protocols; and implementing standards.

- Assist the Services in defining information systems transmission security standards, and evaluating jam-resistant and low-probability-of-interception and/or detection systems.

- Develop, test, and implement new concepts, plans, capabilities, and procedures to improve cryptologic support to US and allied military commands.

- Provide systems development, engineering, and programmatic support to Joint, Service, and/or Multinational tactical cryptologic initiatives.

- Develop cryptologic support plans in support of the Chairman of the Joint Chiefs of Staff and command operation plans, as required.

- Ensure that personnel of NSA, the Service cryptologic elements (SCEs), and tactical commands, in conjunction with the Services, are adequately trained to fulfill cryptologic tasks across the range of military operations.

- Conduct, participate in, and support both US and allied exercises to facilitate the use of SIGINT, INFOSEC, and OPSEC in military operations.

c. To meet operational responsibilities, NSA/CSS, and the USCS will perform as follows.

- Respond immediately to the changing and time-sensitive needs of military commands in war or MOOTW based on SIGINT requirements forwarded directly, or via other means, to NSA.

- Provide information systems encryption materials to military users during peacetime, in crisis, contingency, and war.

- Provide cryptologic support to information operations.

- Provide cryptologic support to US allied military commands in coordination with US and allied cryptologic activities.

- Support, in coordination with other national intelligence activities, US contingency operations consistent with procedures defined in CJCS Joint Operations manuals for support to conventional and special operations missions.

- Support military special technical operations.

- Provide SIGINT support through appropriate channels to the commanders responsible for C2 of mobile military SIGINT platforms.

- Provide direct and dedicated interoperable cryptologic communications support to facilitate the delivery of perishable SIGINT to military commands and provide for continued cryptologic support to emergency or rapid recovery and reconstitution teams.

d. **NSA/CSS Command Relationship**

- **The combatant commands and Services must coordinate all cryptologic plans with the NSA/CSS.** Cryptologic planning encompasses but is not limited to: cryptologic and/or SIGINT subarchitectures to the Command Intelligence Architecture Planning Program; cryptologic support plans to operation plans and operation plans in concept format; new or revised policies, concepts, plans, or procedures enhancing cryptologic support to combatant commands and multinational forces; and planning involving second- and third-party nations.

- The USCS is organized and managed to support peacetime through wartime needs of military commanders at various echelons. Critical to providing such support is a thorough understanding of the commander's plans, operational concepts, and intelligence needs under the various conditions which will be encountered. **To ensure that proper SIGINT support is provided, a close working relationship must exist among the commander, staff, and supporting cryptologic elements.** The support must be tailored, timely and responsive to the commander's expressed interests. SIGINT support is provided by a combination of national and tactical programs.

e. **NSA Cryptologic Support Mechanisms**

- **National Security Operations Center (NSOC).** The NSOC functions as the current operations and crisis management center of the NSA/CSS to ensure that time-sensitive cryptologic needs of commanders are met. The NSOC operates cohesively with the NMCC and DOD I&W watch centers.

- **Special Support Activity (SSA).** The SSA provides real time threat warning in its role as the contingency and crisis management center of the NSOC. It serves as the NSA/CSS lead on all NISTs, and its personnel are deployable for up to 90 days. It may function as a temporary cryptologic support group (CSG) in responding to RFIs by commanders, and also monitors exercises.

- **The Joint COMSEC Monitor Activity (JCMA).** JCMA is a JCS-sponsored organization operating under the auspices of the NSA. The mission of the JCMA is to conduct COMSEC monitoring (collection, analysis, and reporting) of DOD telecommunications signals (encrypted and unencrypted) and automated information systems and monitoring of related noncommunications signals. The purpose is to identify vulnerabilities exploitable by potential adversaries and to recommend countermeasures and corrective actions.

- **Director of Military Support (DMS).** Through the DMS, DIRNSA and Chief, CSS, is responsible for planning and executing cryptologic support strategy for operations planned or executed in coordination with Chairman of the Joint Chiefs of Staff and supported commands. The Assistant Deputy Director for Operations/Military Support (ADDO[MS]), will function as the DMS and be the Agency focal point for all matters relating to military support. The NSA element to a NIST action office falls under the supervision of the ADDO(MS).

- **National Cryptologic Representative (NCR) Defense (NCRDEF).** The NCRDEF is the DIRNSA's senior NSA

representative at the Pentagon, providing day-to-day advice and support to the Department of Defense, Chairman of the Joint Chiefs of Staff, Joint Staff, and Military Services.

- **National Cryptologic Representative and Cryptologic Support Groups**

  •• NCRs and CSGs are established in coordination with unified and selected component commands. **They are advisors to the supported combatant commander and J-2 for cryptologic matters,** to include SIGINT and INFOSEC.

  •• CSGs are considered to be extensions of the NSOC and are one mechanism for the commanders to gain access to and support from the USCS. The function of the CSG will normally include supporting operational commanders by: providing timely SIGINT interpretation, advice, and assistance; assisting in stating cryptologic requirements; and facilitating the flow of SIGINT from the USCS to the operational users. For example, a CSG provides 24-hour support to the Joint Staff J-2 NMJIC.

- **Regional SIGINT Operations Centers (RSOCs).** RSOCs are NSA field activities with the mission to enhance combat SIGINT support to commanders at all echelons. **The RSOCs are regionally focused and receive inputs from multiple sources.** These centers are multi-Service military and/or civilian facilities and provide an opportunity to build on the synergy of national and tactical assets.

3. Contingency Communications Systems

a. NSA's telecommunications and intelligence support capabilities are vast. While many of their systems could have useful applications in contingency operations, the three most commonly employed systems are the Tributary System, the Scaleable Transportable Intelligence Communications System (STICS) and Critical Source (CS). Though not exclusive to NIST deployments, these systems are often deployed with NISTs and are discussed in greater detail in Appendix C, "NIST Systems."

- **Tributary.** The Tributary System is a standing voice and (limited) data

INTELLIGENCE PREPARATION OF THE BATTLESPACE DESERT SHIELD AND DESERT STORM

During Operation DESERT SHIELD and throughout air operations of DESERT STORM, US Navy and Army special operations personnel and force reconnaissance Marines established a series of observation sites along the Kuwaiti-Saudi Arabian border. Tasked to conduct surveillance of the border and intelligence collection in support of follow-on operations, these sites were manned by Navy SEALs, Army Special Forces and Marine Corps force reconnaissance teams, augmented with Marine Corps and Army SIGINT personnel. Through nightly patrols and continuous visual and electromagnetic monitoring of Iraqi forces, the surveillance teams were able to conduct all-source collection of Iraqi army activity across the border. Their efforts laid the groundwork for a thorough intelligence preparation of the battlespace that was instrumental in planning for the forthcoming ground offensive to liberate Kuwait.

SOURCE: Navy Doctrine Publication 2

network that can provide direct threat warning to operational forces. The Tributary System uses portable UHF satellite communications equipment to provide military commanders with direct subscriber linkage to NSA's SSA. SSA teams can be activated and deployed as needed to assist a JTF in response to crisis or contingencies. JTF commanders need not establish special communications pathways to access Tributary, since it is a standing, NSA-maintained network. In some contingencies, a separate dedicated network has been created. Although the main purpose of Tributary is to provide time-sensitive threat warning and reporting, the voice and data capabilities can also be used to support CSG functions. Tributary equipment includes an LST-5 B/C UHF radio, a portable computer, and an antenna appropriate for the mission. Encryption devices are provided by NSA, but the supported command must arrange for the proper keymat. Most Tributary sets are forward-deployed with the operational units that are most likely to require threat warning support. Sufficient equipment packages are available for most contingencies.

- **STICS IIC.** STICS is an intelligence support communication system used as a dedicated intelligence link to coordinate both intratheater and nation-level support. Scaled to meet the user's requirements, a typical STICS configuration contains an LST-5 based UHF satellite communications (SATCOM) transceiver, an encryption device, a universal power supply, and an appropriate antenna. The STICS IIC is contained in a single suitcase for ease of transport. It also comes in an airborne version for deployment with paratroopers and a voice-only shipboard version. Shipment of STICS equipment can be effected with 24 hours of approval (See Appendix C, "NIST Systems").

- **CS.** CS is a scaleable, deployable equipment suite that provides operational forces with access to theater and national SIGINT support and other national intelligence resources. This secure, multimedia, tactical voice and data processing system extends the powerful NSA/CSS communications infrastructure to a forward-deployed CSG or the NSA element of a NIST. CS can provide entry into the National Time Sensitive System (NTSS), the National Secure Telephone System (NSTS) or "Gray phone", the NSA-NET gateway, and other national systems such as JWICS. Communications pathway and satellite access remain the responsibility of the supported command; however, communications can be effected via any suitable front end, such as Trojan Spirit or the NSA-maintained Critical Source Satellite Terminal (CSAT). (See Appendix C, "NIST Systems.")

b. Support to military operations depends on JWICS and on the SECRET Internet Protocol Router Network (SIPRNET), the DODIIS-standard SECRET-level-high-speed communications and/or dissemination network. The Near-Real-Time Dissemination (NRTD) system, one of NSA's key combat support mechanisms, depends upon JWICS and SIPRNET for Internet Protocol (IP) network broadcast of vital time-sensitive data. NRTD uses satellite broadcast media for delivery of intelligence to combat units not connected to the IP networks (JWICS or SIPRNET). In the future, NRTD will play a role in the evolving Integrated Broadcast System (IBS), currently being developed by the IC. The IBS will eventually become a major component of the community combat support infrastructure.

Intentionally Blank

CHAPTER VIII
NATIONAL IMAGERY AND MAPPING AGENCY

"Nothing should be neglected in acquiring a knowledge of the geography and military statistics of their states, so as to know their material and moral capacity for attack and defense as well as the strategic advantages of the two parties."

Jomini
Precis de l' Art de la Guerre, 1838

1. Establishment

On 1 October 1996, the NIMA was established by DOD Directive. The NIMA mission is to provide timely, relevant, and accurate intelligence and geospatial information in support of national security objectives of the United States. NIMA was established, as a combat support agency, under the authority, direction, and control of the Secretary of Defense.

2. Responsibilities and Functions

The Director of NIMA advises the Secretary of Defense, DCI, Chairman of the Joint Chiefs of Staff, and the combatant commanders on imagery, imagery intelligence, and geospatial information. In exercising these responsibilities the Director, NIMA shall perform the following duties.

a. Provide responsive imagery, imagery intelligence, and geospatial products, support, services, and information to include:

- the coordination of imagery collection;
- national tasking;
- processing;
- exploitation; and
- primary and secondary dissemination.

NIMA ensures that required imagery, such as this photo of MIG aircraft at Taszar Airfield, Hungary, is provided quickly and efficiently.

b. Perform imagery analysis and geospatial production.

c. Manage and task national collection operations in accordance with applicable US codes, Presidential Executive Orders (EOs), and consistent with the DCI's collection authorities, as follows.

- Establish and consolidate national imagery collection requirements.
- Support the imagery collection elements to meet national intelligence requirements.
- Advise DOD imagery collection elements on the collection of imagery to meet non-national intelligence requirements.
- Establish and consolidate DOD geospatial information data collection requirements.

d. Provide advisory tasking for theater and tactical assets.

e. Disseminate and ensure the dissemination of imagery, imagery analysis, and geospatial information.

f. Serve as the Program Manager for the National Imagery and Mapping Program for activities within the NIMA.

g. Serve as the functional manager for the Consolidated Imagery and Mapping Program within the NFIP and as the functional manager for the Joint Imagery and Mapping Program within the JMIP.

h. Establish end-to-end imagery-related architectures and systems integrated into the Defense information structure as follows.

- Perform and direct the research and design, development, deployment, operation, and maintenance of systems related to the processing, dissemination, and archiving of imagery (including tasking, collection, processing, exploitation, and dissemination), imagery intelligence, and geospatial information.
- Transfer or otherwise provide such systems to the DOD components as appropriate.
- Develop and field systems of common concern related to IMINT and geospatial information.

i. Prescribe and mandate the use of standards and technical architectures related to IMINT and geospatial information.

- Standards for end-to-end imagery-related and geospatial information architectures.
- Standards for geospatial products produced within the Department of Defense.
- Technical guidance and direction to all of the DOD components regarding standardization and interoperability of systems requiring geospatial information or imagery support.
- Technical guidance and direction to all DOD components on exploitation and dissemination of imagery-related products and geospatial information.

j. Evaluate the performance of imagery, IMINT, and geospatial information components of the Department of Defense in meeting national and military intelligence requirements. Report evaluations annually to the Secretary of Defense, Chairman of the Joint Chiefs of Staff, and DCI. Define and recommend cooperative production and dissemination arrangements for the performance of imagery, IMINT and geospatial information components of the

Department of Defense and the IC to support wartime and contingency operations.

k. Review and respond to the imagery, IMINT, and geospatial information requirements and priorities for military operations, in support of the combatant commanders.

l. Develop and submit to the Secretary of Defense a consolidated statement of geospatial information production requirements and priorities in accordance with the National Military Strategy and National Security objectives of the United States.

m. Manage archives of national and theater imagery, imagery products, and geospatial information.

n. Exercise imagery and geospatial information systems for responsiveness and support to military forces in wartime and contingency operations.

o. In accordance with the DOD plan for Peacetime Use of Reserve Component Intelligence Elements, identify imagery and IMINT tasks, products, support services, and information requirements that can appropriately be satisfied from within the Military Services Reserve Forces. In coordination with DIA, establish the capability to conduct mission tasking and mission management of Reserve Forces engaged in or capable of being engaged in those activities.

p. Develop policies and provide DOD participation in national and international imagery and geospatial information activities. Represent the Department of Defense in national and international geospatial information standardization activities.

q. Provide intelligence sources and methods in accordance with the National Security Act of 1947 and EO 12333, "United States Intelligence Activities."

r. Advise the Secretary of Defense and DCI on future needs for imagery and geospatial information-related matters to the DOD components.

s. Serve as the sole DOD action agency for all purchases of commercial- and foreign government-owned remote sensing data by the Department of Defense.

t. Advise the DOD Acquisition Board, the Defense Science Board and other DOD boards on geospatial information and imagery-related issues.

u. Establish and maintain a NIMA Joint Manpower Program that will be reviewed annually by the Chairman of the Joint Chiefs of Staff.

v. Serve as the DOD Modeling and Simulation Management Executive Agent for Terrain, managing and overseeing all aspects of DOD modeling and simulation related to the authoritative representation of terrain, including both data and the dynamic process models describing related natural and manmade effects.

w. Promulgate procedures and instructions for imagery, IMINT, and geospatial information and related matters to the Department of Defense, including publication of handbooks for the collection, analysis, dissemination and release of imagery, imagery-derived products, and geospatial information.

x. Provide planning support to the combatant commands and Services for imagery and geospatial services. This support begins with a thorough understanding of the commander's plans, operational concepts, and intelligence and geospatial needs.

3. The NIMA Organization

a. NIMA is structured with three directorates. The chief of each Directorate serves as a Deputy Director to the Director, NIMA. This structure is reflected in Figure VIII-1.

b. The Operations Directorate, Customer Support Office, is the focal point for interface with external customers, including the JCS, combatant commands, Services, and National and Defense agencies. Members of the Defense Intelligence and Joint Staff Team are located in the following key areas to support their customers; the Pentagon in the J-2 and NMJIC, the NMCC, and OSD spaces, as well as at the DIAC and Clarendon. The NIMA Operations Center at the Pentagon provides around-the-clock, near-real-time imagery analysis support in response to the intelligence requirements of the J-2, combatant commands, Services, and other joint staff elements.

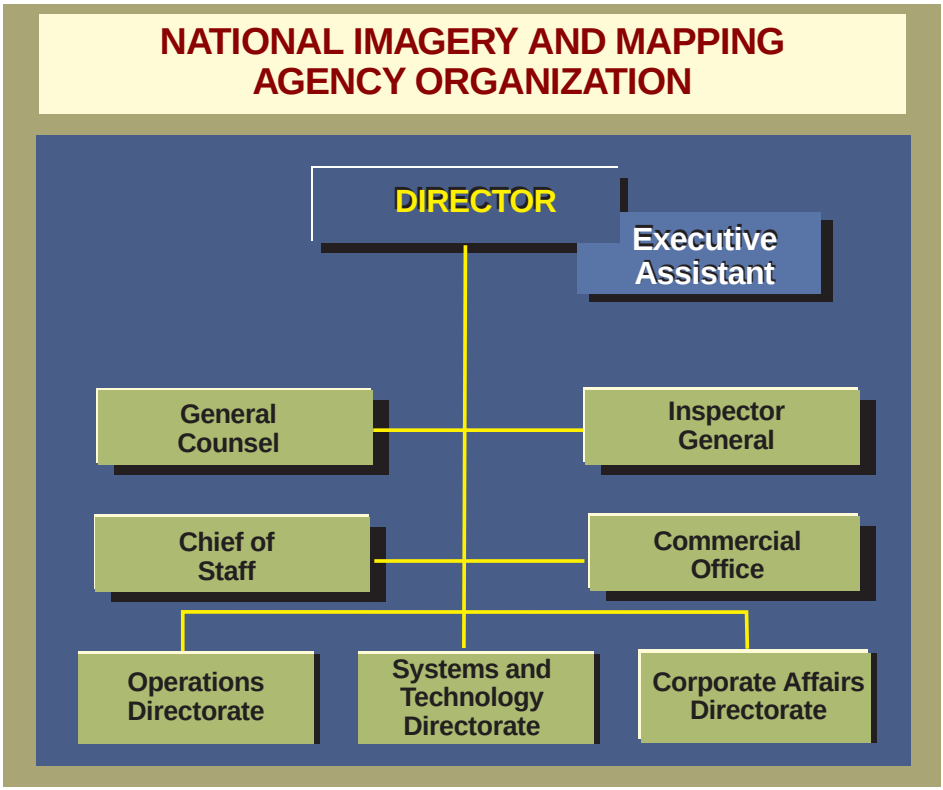


Figure VIII-1. National Imagery and Mapping Agency Organization

CHAPTER IX
NATIONAL RECONNAISSANCE OFFICE AND DEFENSE AIRBORNE RECONNAISSANCE OFFICE

"Time spent on reconnaissance is seldom wasted."

British Army Field Service Regulation, 1912

1. Introduction

This chapter describes the responsibilities of the two offices that provide airborne and space-based reconnaissance assets in support of joint operations. **The NRO provides the nation's space-based reconnaissance capabilities, while the Defense Airborne Reconnaissance Office (DARO) oversees the management of DOD airborne reconnaissance assets.** Used together, airborne and space-based reconnaissance assets can be synergistically employed to assist in providing the JFC an optimized intelligence picture.

2. National Reconnaissance Office

a. The mission of the NRO is to enhance USG and military information superiority, across the range of military operations. The NRO is responsible for the unique and innovative technology, large scale systems engineering, development and acquisition, and operations of space reconnaissance systems and related intelligence activities needed to support global information superiority.

b. The NRO's organizational structure is shown in Figure IX-1. The position of Deputy Director for Military Support (DDMS) was created in 1990 when the role and value of NRO systems to support military operations was recognized. The DDMS is responsible for consolidating NRO military support and oversees all actions impacting the Department of Defense. NRO Directorates and Offices provide NRO training, education, and exercise support to national, military, and civil customers. For the military, these efforts implement Congressional direction to increase warfighters' knowledge of NRO systems capabilities and limitations in order to maximize warfighting capabilities. The NRO's support to military programs includes tailored training, professional military education, and exercise support conducted by the Operational Support Office and the IMINT and SIGINT Directorates. The Plans and Analysis Office develops engineering assessments of future military requirements to ensure that they can be met by systems being launched today.

3. NRO Support to Military Operations

a. **Responsibilities.** NRO responsibilities include support to I&W; monitoring arms control agreements; and crisis support to the planning and conduct of military operations. The NRO accomplishes its mission by building and operating IMINT and SIGINT reconnaissance satellites and associated communications systems. The NRO Liaison Officers and Theater Support representatives located with each of the combatant commands serve as direct links to NRO for the combatant commanders and their staffs. Together, these personnel support each command's unique operating environment and requirements.

b. **Application of Data.** NRO support must be continuously incorporated into the planning process. As a key element in achieving information superiority, it should be viewed as part of all aspects of full spectrum dominance, not simply those areas that fall within the purview of the joint force J-2. Many of the greatest gains can be realized in nontraditional

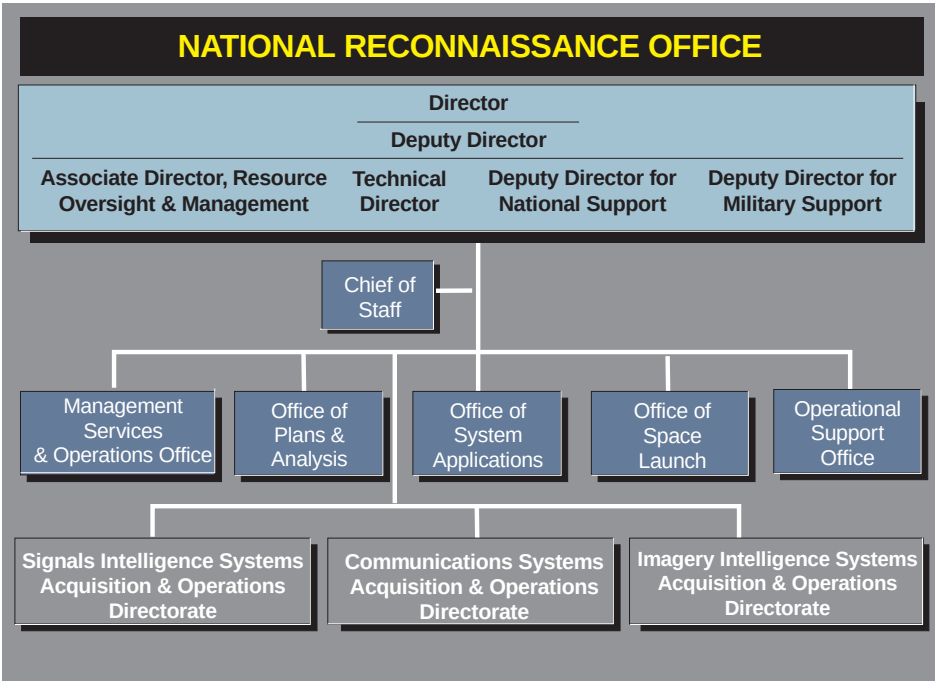


Figure IX-1. National Reconnaissance Office

areas such as supporting logistics with terrain data from NRO systems or providing warning for force protection. The NRO accommodates the functional needs of battlespace information dominance with near-continuous coverage architectures in partnerships with the OSD, JCS, IC, and US Space Command. Advances in technology enable the NRO to provide greater amounts of useful information to ever lower tactical echelons, with the primary impact of NRO data being realized at the operational level. With regard to security, the goal is to downgrade classification and disseminate products essential to operations.

c. **Obtaining Support.** The DIA is the overall coordinator of NRO support for the Department of Defense, which it manages with on-line systems. IMINT requirements are tasked through the NIMA and SIGINT requirements through the NSA. NRO liaison officers and the NRO's Operational Support Office facilitate end-to-end support from education and tasking to dissemination of the product and service. The basic reference for obtaining support is the Joint-Service Tactical Exploitation of National Systems Manual.

4. Defense Airborne Reconnaissance Office

a. DARO, an activity of the OSD, oversees the programs of the Defense Airborne Reconnaissance Program. The DARO organizational structure is shown in Figure IX-2. The DARO was formed and is manned by the Under Secretary of Defense for Acquisition and Technology and the ASD (C3I) to provide effective and coordinated oversight of joint-, Service-, and Defense-wide airborne reconnaissance programs in response to warfighting needs.

b. **The primary focus of DARO is to satisfy warfighter operational surveillance and intelligence requirements by using streamlined, cost-effective, innovative development and acquisition techniques and maintaining the Military Departments' integrated airborne**

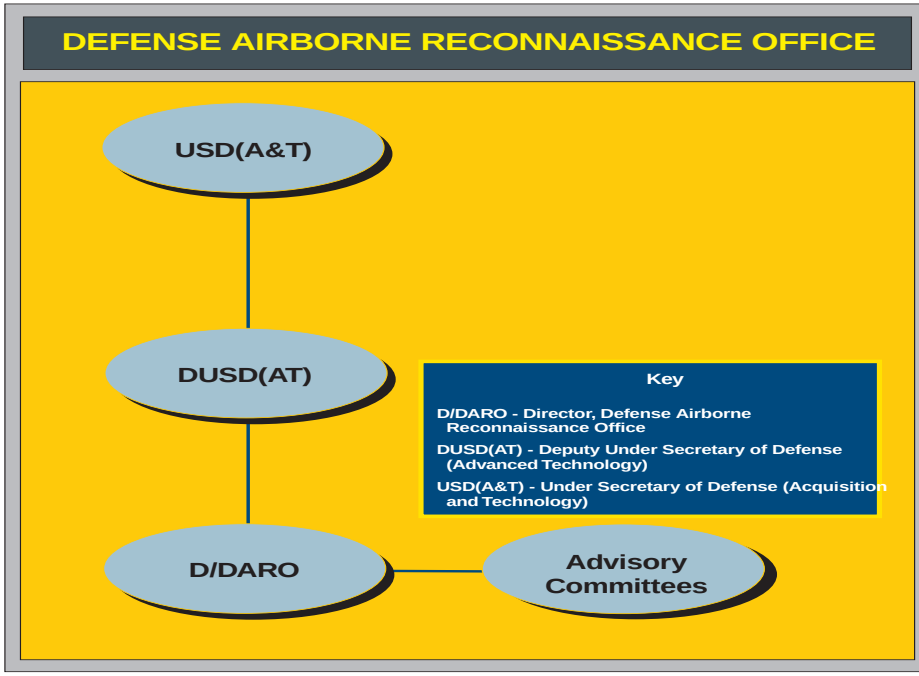


Figure IX-2. Defense Airborne Reconnaissance Office

reconnaissance architecture. A User Advisory Committee at the working level provides the expertise required to clearly understand and interpret warfighter needs and ensure the needs are addressed in the development and acquisition process. The User Advisory Committee includes members from the Joint Staff, combatant commands, Services, Defense agencies, and Community Management Staff.

Intentionally Blank

CHAPTER X
SERVICE INTELLIGENCE ORGANIZATIONS

"The great military victory we achieved in DESERT STORM and the minimal losses sustained by US and Coalition forces can be directly attributed to the excellent intelligence picture we had on the Iraqis."

General H. Norman Schwarzkopf, USA
Commander in Chief, Central Command, 1991

1. Introduction

The Chiefs of the Military Services provide intelligence support for Departmental missions related to military systems, equipment, training, and national intelligence activities. The Services act to support DOD entities, including combatant commands and the Service components of those commands. This chapter addresses the responsibilities and structures of the Services organizations and agencies that support the overall DOD intelligence effort.

2. US Army

a. **Deputy Chief of Staff for Intelligence (DCSINT).** The DCSINT is responsible to the Chief of Staff, Army for **long-range planning and policy guidance on all matters relating to Army intelligence, security, and CI activities.** The DCSINT manages the Army portion of the NFIP, Army departmental-level general military intelligence and scientific and technical intelligence production missions, intelligence readiness training, the Army language program, and the Army Foreign Material Program. The DCSINT exercises staff supervision over the US Army Intelligence and Security Command (INSCOM) and has operational control over its departmental production resources.

b. **INSCOM.** INSCOM, headquartered at Fort Belvoir, Virginia, **is responsible for Army echelons above corps (EAC) intelligence and electronic warfare (IEW) operations.** With subordinate commands located worldwide, INSCOM is a major participant in national intelligence activities and support to theater IEW operations. Its subordinate commands consist of three broad categories of organizations that provide cryptologic, general military, and theater intelligence support to strategic and operational level commanders in the areas of tactical intelligence and related activities (TIARA) HUMINT (HUMINT resources not transferred to the DHS), IMINT, MASINT, SIGINT, CI, IO, and intelligence analysis and/or production. Through its force projection military intelligence (MI) brigades and other specialized units, INSCOM:

- Conducts overt TIARA HUMINT collection worldwide, in response to Army commanders' requirements;
- Performs ground MASINT collection for the Defense IC, under the direction of the Central MASINT office, in support of theater, Army, and national requirements;
- Functions as the Army's SCE for the US SIGINT System;
- Conducts, in coordination with CIA and FBI, CONUS and OCONUS CI operations and all CI and counterespionage (CE) investigations of Army military personnel worldwide; and
- Performs CI analysis and production for the Army.

c. **Theater MI Brigades and/or Groups.** INSCOM Theater MI brigades and/or groups conduct multidiscipline EAC intelligence operations in support of the respective theater's Army component commander and, if one is designated by the JFC, the joint force land component commander (JFLCC). The four EAC units are:

- 66th MI Group, US Army Europe, US European Command;
- 500th MI Brigade, US Army Pacific, US Pacific Command;
- 501st MI Brigade, 8th US Army, US Forces Korea; and
- 513th MI Brigade. The 513th is tasked to provide support, as required, to Army forces (ARFOR) commanders in US European, US Central Command, and US Southern Command.

d. **902d MI Group**

- The 902d MI Group, located at Fort Meade, Maryland is subordinate to INSCOM and is the largest CI organization within the Department of Defense. The Group has a worldwide mission to detect and neutralize the collection against the US Army's forces, secrets, and technologies posed by foreign intelligence services. This encompasses both offensive and defensive CI operations and CE investigations, to include investigations of Army information network denial and/or disruptions, computer systems penetrations, and attempted penetrations. In this regard, the Group supports the Army's land information warfare activity (LIWA) command and control protection (C2P) mission through its investigations, analysis, and CI operations. The Group has supported numerous JTFs with tailored CI support packages, to include operations in Somalia, Haiti, Bosnia, Europe, and Central America. It conducts RED Teams evaluations to provide a realistic picture of a command's organizational vulnerabilities. The Group also provides CI support to the Army technology base and acquisition community.
- The 902d MI Group is one of three DOD CONUS-based units chartered to identify and report Foreign Intelligence Service (FIS) collection operations (i.e., threat information, modus operandi, interests, habits, trends, activities). Analysts at the Group's Army CI Center (ACIC) support US Army CE investigations, CI operations, C2P and special access programs through analysis of FIS targets, trends, and modus operandi; provide analysis of raw information and open-source material to meet worldwide Army requirements; and produce multidiscipline CI threat assessments, counterterrorism, and other threat products. It is the ACIC that conducts the Army CI production mission to complement the National Ground Intelligence Center (NGIC).
- The 902d MI Group is the Army's sole element responsible for providing SCI oversight, inspections, advice, and assistance and site-based accreditation for the Army component of the DODIIS computer security programs. Through its battalions, the Group identifies and neutralizes technical penetrations directed against US forces, secrets, and technology through its technical surveillance countermeasures (TSCM) and TEMPEST teams; conducts polygraph examinations in support of Army technology and operations; and provides signals profiling primarily for sensitive facilities and US Army special operations forces. The 902d MI Group provides basic TSCM training for all

DOD personnel and is the only TSCM certification-granting institution in the Army.

- The 902d MI Group conducts CI operations to determine foreign collection patterns and areas of interest; predicts foreign technology collection requirements; and develops cost effective countermeasures which will prevent those targeted critical technologies from being defeated on the battlefield, countered, or duplicated to the detriment of US forces. The 902d MI Group addresses the foreign collection threat posed by foreign liaison officers, foreign scientist and engineer exchange programs, foreign visitor programs, and the data exchange programs as well as the emerging CI threat to the Army from other nontraditional sources.

- The 902d MI Group provides direct CI support to the Army Special Operations Command, the Defense Special Weapons Agency, the On-Site Inspection Agency, NIMA, and the combatant commands and subordinate forces. The group conducts national-level liaison for INSCOM.

e. **National Ground Intelligence Center.** The NGIC, located in Charlottesville, Virginia, is assigned to INSCOM and is under the operational control (OPCON) of the Army DCSINT. NGIC is the Service National production center for ground forces intelligence and has DODIPP primary production responsibility for most ground force intelligence functional codes under the worldwide area of responsibility. The NGIC provides the following.

- All-source scientific, technical, and general military intelligence on foreign ground forces in support of Army Title 10 requirements.

- IMINT and secondary imagery dissemination to support training, exercises, and contingency planning.

- Executes the Army's foreign materiel acquisition requirements and exploitation program.

- Current and future oriented ground capabilities threat assessments to support operational forces, the combat and materiel development community, contingency planners, force planners, wargame personnel, and doctrine development organizations.

- Detailed analysis and production of systems capabilities and parametric data for all foreign ground and ground-related systems (to include helicopters, air defense guns, infantry, armor and anti-armor, fire support engineer mines, electronic warfare [EW], reconnaissance, chemical warfare, directed-energy weapons, and command, control, and communications systems). Produces assessments of ground systems trends.

- A shared production and data base maintenance responsibility for selected countries.

- Reinforcing support to other Intelligence Centers as required.

f. **Land Information Warfare Activity.** LIWA is assigned to INSCOM and is under the OPCON of the Office of the Deputy Chief of Staff for Operations and Plans, Headquarters (HQ), DA. The LIWA provides operations support for the planning and execution of the command and control warfare (C2W) from the Military Department level through tactical-levels on operational issues related to IO. Support across the spectrum of IO is also

provided to the JFLCC, if one is designated by the JFC. Primary LIWA functions include the following.

- Provide IO staff support to ARFOR and JFLCC staff as required.
- Coordinate and synchronize IO intelligence and CI support to operational and tactical ground commanders, including the JFLCC, as required.
- Coordinate and deploy field support teams to assist ARFOR commanders and JFLCCs in the area of C2-protect, C2-attack and C2-support planning.
- Establish computer emergency response teams to provide information systems security and automated systems security incident support across the range of military operations.

3. US Navy

a. **Director of Naval Intelligence (DNI).** The DNI is the intelligence executive to the Chief of Naval Operations, exercising overall authority throughout the Department of the Navy on matters pertaining to intelligence, cryptology, CI, and special security. The DNI manages the Navy portion of the national foreign intelligence, sets naval intelligence policy, and directs naval intelligence planning and programs.

b. **Office of Naval Intelligence (ONI).** The DNI is also the Commander of the ONI, headquartered in Suitland, Maryland. The ONI supports the requirements of the Department of the Navy by providing the intelligence necessary to plan, build, train, equip, and maintain US maritime forces.

c. **National Maritime Intelligence Center (NMIC). The NMIC is the national production center for maritime intelligence.** Located at Suitland, Maryland, NMIC consists of ONI, a detachment of the Marine Corps Intelligence Activity (MCIA), and the US Coast Guard Intelligence Coordination Center. The NMIC supports Navy, Marine Corps, Coast Guard, joint, and national-level requirements through a variety of intelligence production capabilities, including:

- Naval weapons systems analysis;
- Integrated tactical analysis of foreign navies and maritime threats;
- Acoustic collection and analysis;
- Naval foreign material acquisition and exploitation;
- Civil maritime analysis such as merchant shipping, sanctions violations, commercial treaty violations, counterdrug, and maritime smuggling;
- Intelligence support to naval information warfare (IW) and/or C2W;
- Naval-related collection and information systems development; and
- Community management support on naval budget, security, and reserve issues.

d. **Naval Criminal Investigative Service (NCIS). NCIS fulfills the criminal investigative and CI responsibilities of the Navy.** The Director, NCIS, is directly subordinate to the Secretary of the Navy, and also serves as Assistant Director of Naval Intelligence for CI. Intelligence on potential terrorist and unconventional warfare threats to the Navy and Marine Corps is provided by the Navy Antiterrorist Alert Center (NAVATAC), a 24-hour terrorism I&W center. A branch of NCIS, the NAVATAC provides a full range of counterterrorism, CI, and technology transfer analysis for the Department of the Navy.

4. US Air Force

a. **Air Force Director of Intelligence, Surveillance, and Reconnaissance (AF/XOI).** AF/XOI is responsible to the Air Force Chief and Deputy Chief of Staff for Air and Space Operations for policy, planning, programming, resource allocation, and program evaluation activities aimed at ensuring information superiority in peace, crisis, and war.

b. **Air Intelligence Agency (AIA).** AIA, headquartered at Kelly Air Force Base (AFB), Texas, **oversees processing and production elements worldwide.** It provides customers at all echelons with multi-source intelligence products, applications, and services and provides intelligence expertise in the areas of IW and C2W (to include information protection), acquisition, foreign weapons systems and technology, and treaty monitoring. Additionally, AIA serves as the Air Force Validation Office for Production and Application Requirements under the DODIPP. When Air Force component intelligence requirements exceed the theater's capabilities, AIA may reinforce the combatant command with analytical expertise and products.

c. **National Air Intelligence Center (NAIC). The NAIC, subordinate to AIA, is the principal agency for assessing the foreign air and space threat.** The NAIC can provide deployed forces with unique capabilities for aerospace intelligence for DOD operational commands, research and development centers, weapon acquisition agencies, and national planners and policymakers. HQ NAIC is located at Wright-Patterson AFB, Ohio; subordinate NAIC elements operate in Washington, DC, Langley AFB, Virginia, and Offutt AFB, Nebraska.

d. **Air Force Information Warfare Center (AFIWC). AFIWC explores, applies, and migrates offensive and defensive IW capabilities** for operations, acquisition, and testing. The AFIWC provides advanced IW training for the Air Force, develops and maintains C2W data bases and applications, performs vulnerability analyses of friendly electronic systems, and protects friendly C2 against adversary attacks. The AFIWC's data bases and application are a major dissemination mechanism to provide IW related intelligence to the warfighter. Support is provided both directly from the AFIWC and via JC2WC which are collocated in San Antonio, Texas. (See Appendix A, "Joint Warfare Analysis Centers").

e. **Air Force Office of Special Investigations (AFOSI). AFOSI provides a full range of CI services** encompassing four primary mission areas: collection, analysis and production, operations, and investigations. These missions are accomplished through proactive and reactive programs in support of Service, combatant command, and national-level agencies. AFOSI's primary responsibility during all levels of conflict is to provide Air Force commanders CI support to identify and neutralize the sabotage, clandestine intelligence, subversive, terrorist, and criminal threat to resources. In war or MOOTW, a realignment of AFOSI forces may be accomplished to meet the commander's requirements.

5. US Marine Corps

a. **The Assistant Chief of Staff (AC/S), C4I.** AC/S, C4I, is designated the Director of Intelligence (DIRINT), US Marine Corps. The DIRINT is the Marine Corps' Senior Intelligence Officer and **principal intelligence advisor to the Commandant of the Marine Corps.** The Intelligence Division is the staff support element of the AC/S, C4I.

b. **US Marine Corps Intelligence Activity.** The MCIA is an element of C4I, HQ, Marine Corps. MCIA has two locations: the Support

Division and Concepts Based Requirements Divisions at the Marine Corps Combat Development Command in Quantico, Virginia, and the Expeditionary Warfare Support Division collocated with the NMIC in Suitland, Maryland. The mission of MCIA is to provide tailored intelligence support to:

- The Commandant of the Marine Corps;
- The development of Service-specific doctrine, force structure, force modernization, training and education, and acquisition policy and programming; and
- Fleet Marine Force contingency planning and other requirements of intelligence products not satisfied by either theater, other Service, or national research and analysis capabilities.

c. **MCIA Functions**

- Acts as production manager and validation authority for Marine Corps production requirements.
- Acts as the Service collection requirements manager.
- Serves as the Service geospatial information and services (GI&S) focal point.
- Acts as the Service representative to the Joint Foreign Material Program and has the responsibility to satisfy Marine Corps foreign material acquisition and exploitation requirements.
- Functions as a DODIPP production center and responds to DOD-wide requirements for intelligence support to expeditionary warfare operations.
- Develops threat assessments and documentation based on all-source scientific and technical (S&T) analysis in support of Marine Corps combat development, acquisition, and operational testing.
- Coordinates community requirements for the DOD Country Handbook Production Program.
- Provides predeployment and Service-unique crisis support intelligence products.
- Prepares intelligence training and exercise support for Marine training and education activities.

INTELLIGENCE SUPPORT TO MILITARY OPERATIONS OTHER THAN WAR

Since the standup of Joint Task Force Four in 1989, naval cryptologic operations have played a major role in the detection and monitoring of illicit drug trafficking in the Caribbean Sea and Pacific Ocean.

During Operation RESTORE HOPE in 1993, Marine Corps tactical HUMINT operations proved to be indispensable. By "taking the pulse" of the local populace, HUMINT personnel were able to determine which indigenous forces were friendly, neutral, or potentially hostile, where weapons caches were located and where threat situations might develop. Additionally, they provided the joint task force commander an appreciation of Somali perception of, and reaction to, United Nations' support and relief operations.

During the Mississippi River flooding in the summer of 1993, naval tactical aircraft flew photographic reconnaissance missions over the Mississippi River Valley, mapping the extent of flood damage and providing that information to the Federal Emergency Management Agency and other civil authorities charged with flood relief efforts.

SOURCE: Navy Doctrine Publication 2

Intentionally Blank

APPENDIX A
JOINT WARFARE CENTERS

1. Joint Command and Control Warfare Center

a. The CJCS Instruction 5118.01, "Charter for the Joint Command and Control Warfare Center," is the charter for the JC2WC. Through USACOM with Joint Staff oversight and guidance, the JC2WC serves as the principal field agency within the Department of Defense for non-Service specific C2W and IO support.

b. The mission of the JC2WC (formerly the Joint Electronic Warfare Center) is to provide direct C2W and IO support to operational commanders. The JC2WC will support the integration of the constituent elements of C2W — OPSEC, psychological operations, military deception, EW, and physical destruction as well as the noncombat military application of IO — throughout the planning and execution phases of operations. This direct support will be provided in the following priority order: JFCs (combatant commanders, subordinate unified commanders, and JTF commanders); Service component commanders; and functional component commanders. Support will also be provided to the OSD, the Joint Staff, the Services, USG agencies, NATO, and allied nations.

c. The JC2WC executes its mission through its directorates of Operations, Protect and Defense, and Technology Integration.

2. Joint Warfare Analysis Center

a. The JWAC is located at the Naval Surface Warfare Center in Dahlgren, Virginia. Like the JC2WC, JWAC is not strictly an intelligence organization; however, a significant portion of its work supports intelligence applications. To request JWAC support, contact them directly at DSN 249-8781.

b. The JWAC assists the Chairman of the Joint Chiefs of Staff and the combatant commanders in preparation and analysis of joint operational plans and assists the Service Chiefs in the analysis of weapon effectiveness. JWAC serves as the Joint Staff agent for the integration and analysis of data concerning infrastructure networks. JWAC supports the combatant commands and the Joint Staff as prioritized by United States Atlantic Command (USACOM) J-3. Secondarily, they provide support to the Military Services, OSD, and other government agencies as tasked by USACOM J-3.

c. The JWAC executes its mission through the following directorates: Intelligence; Operations; Information Systems; and Strategic and Technical Initiatives. Within these directorates, JWAC maintains a regional focus aligned with the geographic combatant commands.

Intentionally Blank

APPENDIX B
OTHER GOVERNMENTAL ORGANIZATIONS

1. US Coast Guard, Department of Transportation

The US Coast Guard (USCG) is not a formal member of the IC. However, its unique missions and responsibilities as both an armed force and a law enforcement agency make it a significant player in several national security issues. The USCG intelligence program supports counterdrug operations, mass seaborne migration operations, alien migration interdiction operations, living marine resource enforcement, maritime intercept operations, port status and/or safety, counterterrorism, coastal and harbor defense operations, and marine safety and/or environmental protection. The USCG Intelligence Coordination Center (ICC) is the Coast Guard's primary interface with the IC. The ICC is a tenant command within the US Navy's NMIC in Suitland, Maryland, and maintains a 24-hour intelligence watch, providing I&W input to the NMIC. The ICC acts as the strategic center with ties to both national intelligence agencies and the headquarters-level intelligence activities of law enforcement organizations. The ICC supports strategic analysis, manages Coast Guard collection, and provides national imagery exploitation support, including tactical support to operational commanders. Intelligence components of the area commanders' staff provide regional and operational intelligence for USCG operations. Coast Guard intelligence entities access Navy and IC data bases and C4I systems, including JWICS, the Anti-Drug Network, US Atlantic Command intelligence data handling system, and the Joint Maritime Information Element.

2. Office of National Drug Control Policy

The Director of the ONDCP is responsible for establishing policies, objectives, and priorities for the National Drug Control Program and for annually promulgating a National Drug Control Strategy to be submitted by the President to the Congress. The Director advises the President regarding necessary changes in the organization, management, budgeting, and personnel allocation of Federal agencies involved in drug enforcement activities.

3. Law Enforcement Agencies

a. **The Drug Enforcement Administration (DEA), Department of Justice.** The DEA enforces laws and regulations governing narcotics and controlled substances, chemical diversion, and trafficking. It is also the lead agency overseas for counterdrug law enforcement activities and investigations.

b. **Customs Service, Department of Treasury.** The US Customs Service is the principal border enforcement agency. Its missions include interdicting and seizing contraband, including narcotics and illegal drugs.

4. Other Government Agencies

a. **USG Agencies (Information Support).** There are a number of "non-intelligence" USG agencies and organizations responsible for gathering and maintaining information and statistics related to foreign governments and

international affairs. Such organizations as the Library of Congress, the Departments of Agriculture and Commerce, the National Technical Information Center, US Information Agency, US Information Service, and the US Patent Office are potential sources of detailed, specialized information on political, economic, and military-related topics. The national-level IC may draw on these organizations to support and enhance research and analysis and for relevant, peripheral data and background information for planners and decision makers.

b. **USG Agencies (Operational Support).** Many other USG agencies may become directly involved in supporting the Department of Defense, especially during MOOTW. These organizations include: the Department of Transportation; the Disaster Assistance Response Team, within the Office of Foreign Disaster and the US Agency for International Development; the Immigration and Naturalization Service; the US Border Patrol; and the Federal Emergency Management Agency.

APPENDIX C
NIST SYSTEMS

1. DIA

a. **The Joint Deployable Intelligence Support System.** The JWICS provides the NIST with an interactive computer link back to the National Intelligence Community. JDISS enables the NIST to access national-level data bases, as well as to communicate directly with analysts throughout the various intelligence working groups in Washington, DC. The NIST normally will deploy with two JDISS computer terminals: the SunSPARC desktop suite and/or the RDI Powerlite Notebook.

Equipment	Weight Pounds	Size, Cubic Feet	Transit Cases
SunSPARC 20	195	15.4	3
RDI Powerlite	23	3	N/A
Peripherals and/or Support Equipment (CD-Rom, Laser Printer, Kodak Printer, CJ10 Printer, Tape Drive, Scanner, UPS Power Supply)	860	62.7	9

b. **International Maritime Satellite (INMARSAT).** The NIST uses INMARSAT terminals to transmit and receive either voice or data communications. The INMARSAT provides the NIST expedient temporary access to JWICS (the main communications network for transmitting top secret (TS) and/or SCI material) during the initial stages of a deployment, when no other communications pipeline is available. The INMARSAT transmits and receives information at a maximum of 64 kbps, and can be set up and operational in less than 45 minutes.

Equipment	Weight Pounds	Size, Cubic Feet	Transit Cases
INMARSAT-A	80	6.3	3
INMARSAT-B	60	3	1

c. **Containerized Joint Worldwide Intelligence Communications.** Containerized JWICS provides a portable JWICS communications suite to a deployed NIST and JTF. The Containerized JWICS is a deployable system that provides secure multimedia communications between the JTF and the IC. The Containerized JWICS gives the user access to the JWICS Data Network, JWICS VTC System, and the NSTS. The system consists of the standard VTC studio capability and a gateway for data communications, both of which are deployed in hard transit cases. The Containerized JWICS requires commercial power and a communications circuit.

Equipment	Weight Pounds	Size, Cubic Feet	Transit Cases
(2) Television Monitors, VCE, IDNX Multiplexer, Router, Crypto, Cables	600	22	4

d. **JWICS Mobile Integrated Communications System (JMICS).** The JMICS provides a JTF with a mobile JWICS communications system. The JMICS is a deployable system that provides secure TS and/or SCI high speed multimedia communications connectivity between the JTF and the IC. JMICS gives the user access to the JWICS Data Network, JWICS VTC System, the NSTS, secure telephone unit-III (STU-III), and selected other communications feeds. JMICS consists of a heavy high mobility multipurpose wheeled vehicle (HMMWV), communications shelter, and a generator trailer. The system is transportable on C-130, C-141, and C-5 aircraft. It is typically deployed with the Trojan SPIRIT II communications transmission system, although it can operate with commercial transmission systems (such as CSAT). The JMICS will be deployed at the direction of the Joint Staff in support of combatant commander and/or JTF requirements.

Equipment	Weight Pounds	Size, Cubic Feet	Transit Cases
JMICS HMMWV and Shelter	10,000	435.4	N/A
Generator Trailer	4,200	779	N/A

(DIA does not maintain ownership of JMICS; maintenance and support is provided by the US Army's "power projection brigades.")

2. NSA

a. **INMARSAT-B.** See information above.

b. **Scaleable Transportable Intelligence Communications System and Tributary System.** The STICS IIC provides portable, secure voice and/or data terminals using either military UHF, SATCOM media, or other line of sight (LOS) transmissions. It is designed for worldwide SATCOM or LOS communications versatility. Each unit is deployed as a self-contained case that provides all interconnect wiring, data device (usually a computer) port, and a voice and/or data interface module on a hinged equipment shelf for easy equipment installation and repair. The NSA SSA uses STICS IIC terminals for worldwide threat warning broadcasts over the Tributary Network. The equipment configured for a Tributary System is virtually identical to that of a STICS. STICS IIC is also deployed with the CS as a backup emergency communications system.

Equipment	Weight Pounds	Size, Cubic Feet	Transit Cases
STICS IIC	75	5	2

c. **Fly Away Terminal Satellite / NIST LITE (FTSAT/NISTLITE).** FTSAT/NISTLITE is a military satellite communications (MILSATCOM) interoperable lightweight tactical SATCOM terminal designed to support low data rate communications requirements. The terminal is fully operable over X, C, and Ku-band satellites (International Telecommunications Satellite Organization, domestic satellites, and military Defense Satellite Communications System, NATO, and UK SKYNET) and will support an aggregate data rate of 128 kbps to 256 kbps (depending on gateway termination and operating band). The FTSAT/NISTLITE terminal is used to provide SATCOM communications connectivity during the initial stages of a NIST deployment. The aggregate communications link will support a low-density JDISS local area network, two-channel secure voice link, plus unique agency communications between the deployed NIST location and national intelligence until relieved by more capable NIST communications systems (CSAT or Trojan SPIRIT II).

Equipment	Weight Pounds	Size, Cubic Feet	Transit Cases
FTSAT/NIST LITE	800	57	8

d. **CSAT.** The CSAT is a MILSATCOM interoperable HMMWV-mounted tactical Tri-band SATCOM terminal designed to support medium data rate communications. The terminal is fully operable over C, X, and Ku-band satellites at a data rate between 512 kbps to 2.048 mbs. The CSAT system has full redundancy for automatic switching should active components fail, keeping an operational ability of 99.9 percent. The system is interoperable with a variety of user interface subsystems, but is primarily used with the CS. The CSAT will be the key JWICS path provider for unique JTF NIST echelons below JTF, small deployments requiring support greater than the FTSAT/Tri-band, or other unique requirements. The CSAT is deployable via C-130, C-141, C-5, rotary-wing sling, ship, or rail.

Equipment	Weight Pounds	Size, Cubic Feet	Transit Cases
CSAT	10,000	1,082.2	N/A

e. **Critical Source.** The CS provides tailorable, secure voice and/or data switching and processing to extend the JWICS and NSA communications infrastructure and services to CSG, the combatant commands, and Services to the deployed NIST. The CS is equipped with an electronic equipment shelter, and is mounted on a heavy HMMWV. The CS can interface with FTSAT/Tri-band, CSAT, Trojan SPIRIT II, INMARSAT, and fiber optic or copper wire transmission systems. It transmits and receives data or voice communications at a rate of up to 1.544 mbs. The CS communications system equipment includes all equipment necessary for the user to access the JWICS Data Network, the NTSS, the NSTS, and selected NSA data bases via an ethernet-based connection. CS provides secure facsimile and telephone service via STU-III and commercial or military Defense Switched Network service. With planned upgrades, the CS will provide full NIST JWICS and/or JDISS support, to include VTC capability with add-on VTC systems.

Equipment	Weight Pounds	Size, Cubic Feet	Transit Cases
Critical Source	10,000	1,082.2	N/A
Support Van	10,000	1,082.2	N/A
Generator Trailer	1,650	518.5	N/A
Crew Vehicle	8,600	681.2	N/A

3. CIA

The CIA element of the NIST deploys with its own secure satellite communications package. These communications provide direct connectivity between the JTF and CIA Headquarters and worldwide stations and bases. The fully redundant communications package is capable of secure voice and data transmissions as a stand-alone communications system, and can also interface with the JWICS and JMICS.

Equipment	Weight Pounds	Size, Cubic Feet	Transit Cases
(2) DI Data Base Systems, (4) Tempest computers, (4) Printers, (2) LST 5-C UHF Transceivers, Crypto, Cables	2,000	100	26

N/A = Not Applicable

APPENDIX D
INTELLIGENCE RESOURCE PROGRAMS

1. Introduction

A large number of organizational elements have evolved in the intelligence arena to manage intelligence and intelligence-related activities. The numerous activities and assets that comprise the total US national intelligence effort fall within a broad spectrum ranging from strategic to tactical. There are three major intelligence groups that manage all intelligence activities and directly contribute to effective and coherent support to military intelligence consumers: National Foreign Intelligence Program (NFIP), Joint Military Intelligence Program (JMIP), and Tactical Intelligence and Related Activities (TIARA). The NFIP serves national-level decision makers across multiple government agencies and departments with primarily strategic intelligence. The JMIP provides intelligence to joint mission-oriented customers defense-wide. TIARA is focused on individual Military Services or agencies whose principal consumers are operational and tactical military commanders. Each of the three intelligence categories are addressed in this appendix.

2. Resource Programs

a. Intelligence activities and assets are grouped and funded according to their function and/or purpose. Strategic intelligence typically is considered to be national-level activities and assets funded under a number of resource programs referred to collectively as the NFIP. Strategic or national intelligence primarily supports the NCA and national-level political and military leadership. It is primarily strategic in nature, concerns plans and intentions of foreign entities and serves as the basis for the national military strategy. The NFIP is jointly managed by the Deputy Secretary of Defense and the DCI. The NFIP resources provide the funding for intelligence activities and assets necessary for intelligence operations to support the US military for EAC. It is conducted by a wide range of intelligence organizations (See top arrow Figure D-1).

b. The JMIP was established to improve the effectiveness of DOD intelligence activities when those activities involve resources from more than one DOD component; when the users of the intelligence data are from more than one DOD component; and/or when centralized planning, management, coordination, or oversight will contribute to the effectiveness of the effort. The JMIP focuses on joint, defense-wide initiatives, activities, and programs that provide more effective and coherent intelligence programmatic decision making (See middle arrow Figure D-1). Military intelligence consumers supported include the warfighter, policymaker, and force modernization planners. JMIP-funded activities are managed by the Deputy Secretary of Defense. JMIP and TIARA constitute the basis for Defense intelligence outside the NFIP.

c. TIARA resources provide the funding of tactical intelligence, related activities, and assets necessary for military operations at the corps, wing, naval battle group, and Marine expeditionary force level and below (See bottom arrow Figure D-1). TIARA-funded activities are managed under the direction of the Secretary of Defense. The programs are designed, built, and operated by the Military Services and Defense agencies and compete for funding with combat and combat-support programs. TIARA funds represent those portions of the DOD budget devoted to non-NFIP intelligence and other related activities that respond to combatant commander's requirements to gather and interpret time-

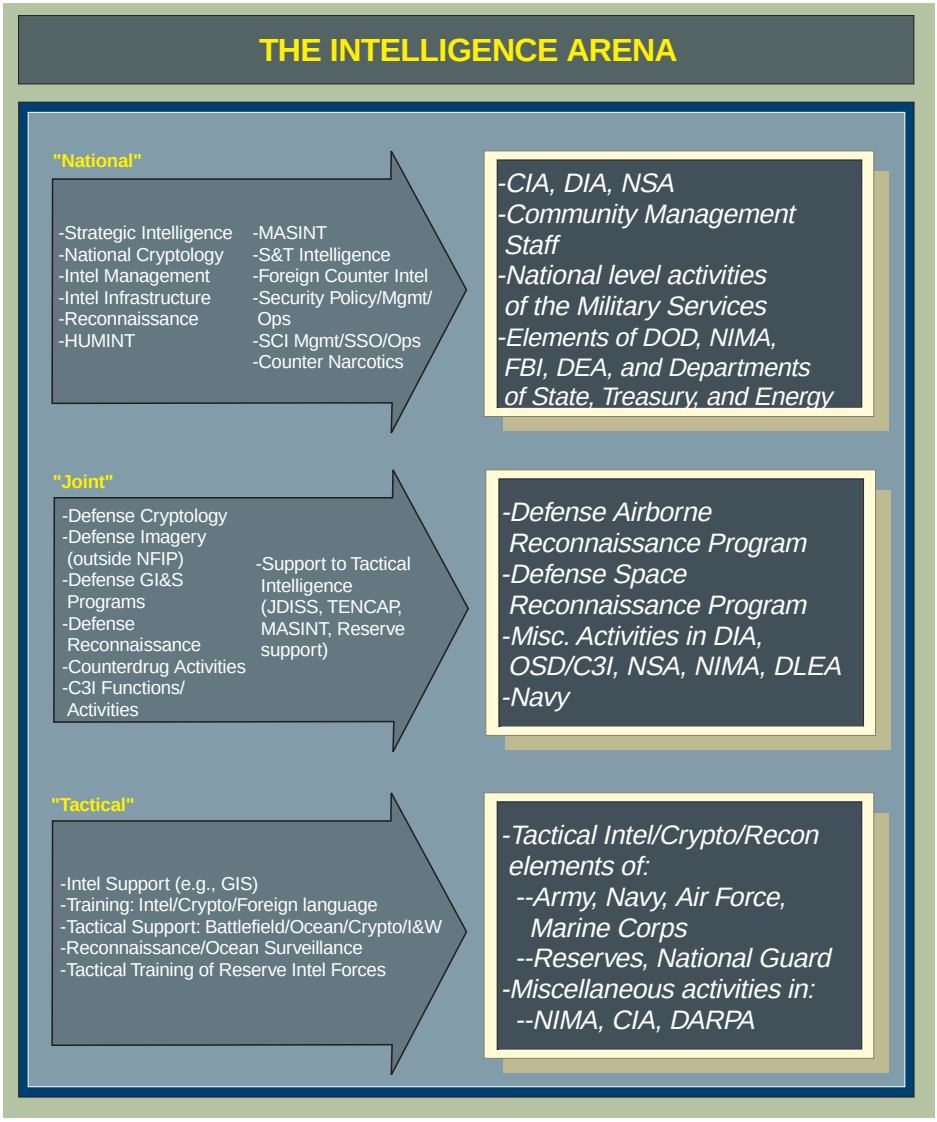


Figure D-1. The Intelligence Arena

sensitive intelligence on foreign entities. TIARA includes programs that fund intelligence training, reserve forces, and research and development. A universal "rule of thumb" is anything that is not NFIP-funded must be considered either a tactical-level intelligence asset (i.e., TIARA) or something other than an intelligence asset (i.e., operational). The definitional model in Figure D-2 reflects the difference and overlap of the NFIP, JMIP, and TIARA funding arenas.

3. National Foreign Intelligence Program

a. The NFIP encompasses the bulk of the activities of the four major national civilian and military intelligence agencies; CIA, DIA, NIMA, and NSA, the staff of the DCI, national-level DOD intelligence, foreign counterintelligence, reconnaissance activities, and other intelligence programs within the USG designated for inclusion in the NFIP by the heads

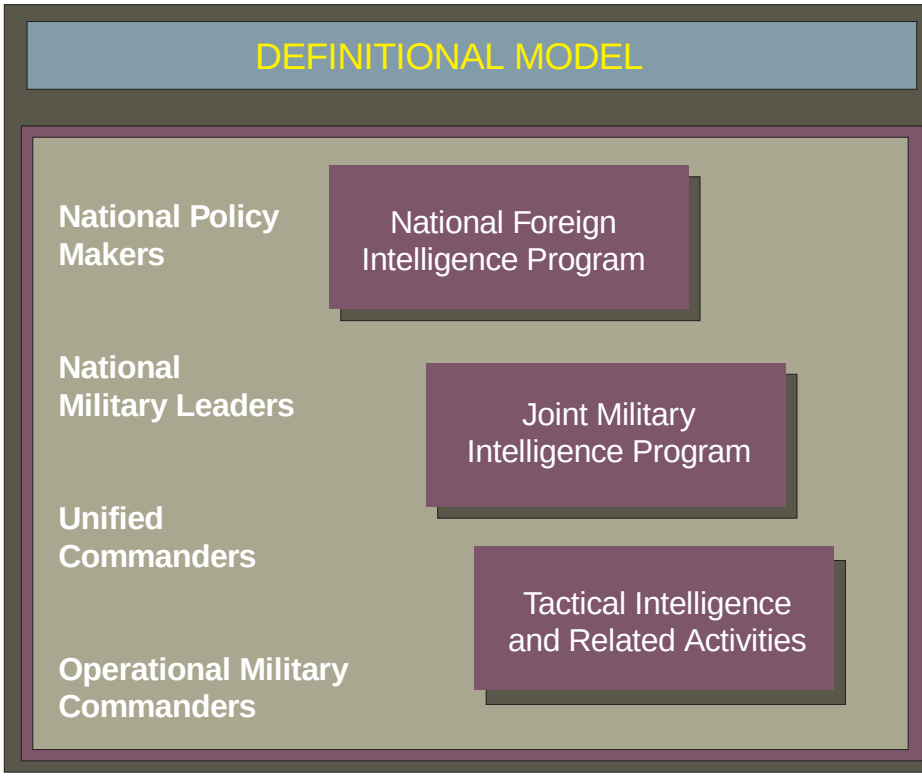


Figure D-2. Definitional Model

of the executive department involved and the DCI or the President.

b. Each NFIP program is headed by a program manager who prepares the program's annual budget and oversees the expenditure of the funds allocated to the program. While some NFIP programs are managed by the heads of organizations most closely associated with them (e.g., the Consolidated Cryptologic Program [CCP] by the Director of NSA), others are not (e.g., the Central Intelligence Agency Program [CIAP] is not managed by the DCI, but by the Deputy Director of CIA). The program managers receive policy and fiscal guidance from the DCI and prepare and submit their programs' budget for DCI approval and consolidation into the single NFIP budget which is submitted to the President.

c. The NFIP budget is not openly published for national security reasons. NFIP funding is actually embedded within elements of the Defense budget. These funds are administered by the Military Services, but under the close scrutiny of NFIP program managers.

4. General Defense Intelligence Program

a. The broadest-based NFIP program within the Department of Defense and Military Services is the GDIP. This program funds military intelligence units and activities that involve something other than cryptology, CI, and certain types of specialized reconnaissance. It includes DIA, intelligence units from each of the Military Departments, and unified command units that have theater-

wide responsibilities and significant national or departmental intelligence missions.

b. The GDIP encompasses the following activities.

- All defense intelligence production not funded elsewhere in the NFIP.
- All national-level DOD human source intelligence.
- A wide range of activities that provide defense intelligence infrastructure.
- Significant collection (other than cryptologic and CI) against geographic targets, foreign forces, and foreign weapon systems.

c. GDIP-funded units and activities collect information, process and analyze data, and produce MI for the following spectrum of missions.

- Support to warfighting
  - •• Input to national military strategy.
  - •• Indications and warning.
  - •• Countermeasures and military contingency operations.
  - •• Theater-level battle planning and direction of combat operations.
  - •• Planning and conducting small scale contingency operations (e.g., Noncombatant Evacuation Operations).
- Equipping and training of forces
  - •• Weapons and countermeasures acquisition.
  - •• Force structure development.
  - •• Doctrine and tactics training.
  - •• Military education and training.
- Direct support for national-level priorities
  - •• Foreign policy development.
  - •• Arms control negotiations and treaty monitoring.

d. Units and activities funded by the GDIP must be tasked in peacetime to perform their principal intelligence mission and must support missions of the Department of Defense, a Military Department, a unified command, or more than one component command.

- The GDIP supports OSD and JCS decision making; Military Service training and equipping; and production, collection, ADP, or intelligence communications capabilities within combatant commands, JICs, and essential EACs intelligence capabilities at component headquarters.
- GDIP is affected by resource decisions and actions of other programs within the NFIP and TIARA. For example, GDIP often funds the training of operators of new systems acquired through other programs. It also provides equipment and communications for other systems to ensure interoperability and compatibility with other systems funded outside the GDIP.

e. GDIP funds are expended mainly in the four following areas of intelligence

- Production
  - •• GDIP-funded production includes all Defense intelligence production in the NFIP (except SIGINT, MASINT, and CI)

and supports the timely production of fused all-source finished intelligence for warfighters and the national, Service, and departmental leadership. Its products include data bases of foreign military forces and programs, targeting materials, S&T analyses, and threat assessment.

•• The Director, DIA is the Program Manager of the GDIP and the agency is one of the major producers. DIA produces a full range of basic, current, warning, and estimative intelligence that supports geographic combatant commanders and operational forces, the Military Departments, and national policymakers.

•• Military Service producers focus mainly on national-level intelligence needed to equip and train forces to support the combatant commanders and maintain S&T centers and operational intelligence centers funded through the GDIP.

•• A significant portion of GDIP intelligence production is accomplished in theater intelligence production centers, imagery centers, and component analytical centers.

- **Collection.** The GDIP funds intelligence collection primarily in three areas.

  •• HUMINT conducted through Defense attachés and other overt collection, and through controlled activities.

  •• MASINT.

  •• Collection (other than SIGINT and certain other types of collection conducted through other NFIP programs) against geographic targets and foreign forces and weapon systems. The collection is achieved mainly through technical sensors on airborne reconnaissance platforms and aboard a variety of other collection systems.

- **Infrastructure.** This third aspect of the GDIP includes the following.

  •• **Automation.** All intelligence ADP support and networking of automated intelligence systems under the Department of Defense Intelligence Information System and non-cryptologic communications for sensitive compartmented information dissemination.

  •• Reproduction, presentation, and dissemination of a wide range of intelligence materials and data.

  •• Physical, personnel, industrial, computer, telecommunications, and operations security. This includes non-cryptologic sensitive compartmented information policy and operations as well as adjudication of special background investigations.

  •• Intelligence training and education, such as the courses conducted at the MC.

- **Management.** GDIP funds three types of intelligence management: program intelligence management, functional management, and fiscal management. Program management was discussed earlier in this appendix. Functional managers and their staffs are oriented along the three broad functional areas of production, collection, and infrastructure which encompass the full range of activities funded under the GDIP. Fiscal management involves the GDIP programming and budget process, a structured sequence within the NFIP that runs parallel to that of all other NFIP programs against which GDIP requests eventually compete for a share of the

NFIP budget. The process begins when the GDIP Program Manager receives guidance from the DCI and uses it to develop his own "top-down" policy and fiscal guidance to the Service intelligence elements, DIA, and the unified commands or the Program Manager's Guidance Memorandum (PMGM). Based on the Program Manager's guidance, the functional managers provide funding priorities and specific guidance relative to their respective area of responsibility which is included in the PMGM.

5. Other NFIP Programs

a. **Central Intelligence Agency Program.** The activities of CIA are funded under the CIAP. This NFIP program provides funds for analytical and controlled activities, administration, field operations, and research and development. The Deputy Director of the CIA is designated as the Program Manager of the CIAP.

b. **Consolidated Cryptologic Program.** CCP is operated and managed by NSA, with the DIRNSA serving as the Program Manager. In addition to its own worldwide SIGINT and OPSEC operations, NSA also oversees national-level operations of the three Service cryptologic elements. These elements include Navy's Security Group, the cryptologic components of the Army's Intelligence and Security Command, and the Air Force's Intelligence Agency.

c. **DOD Foreign Counterintelligence Program.** This component of the NFIP conducts counterintelligence activities in support of DOD components outside the US in coordination with the CIA, and within the US in coordination with the FBI, pursuant to procedures agreed upon by the Attorney General and the Secretary of Defense.

d. **Special Reconnaissance Intelligence Programs in DOD.** Two sensitive programs collect specialized intelligence through reconnaissance. These programs are responsible for:

- Carrying out consolidated reconnaissance programs for specialized intelligence:
- Responding to taskings in accordance with procedures established by the DCI; and
- Delegating authority to the various agencies and departments for research, development, procurement, and operation of designated means of collection.

e. **Treasury Department Intelligence Program.** This NFIP program is that element of the Treasury responsible for:

- Overt collection of foreign financial and monetary information;
- Participation with the DOS in the overt collection of general foreign economic information;
- Production and dissemination of foreign intelligence relating to US economic policy as required for the execution of the responsibilities of the Secretary of the Treasury; and
- Conduction, through the Secret Service, of activities to determine the existence and capability of surveillance equipment being used against the President, the Executive Office of the President, and other US officials, as authorized by the Secretary of the Treasury or the President.

f. **State Department Bureau of Intelligence and Research.** This NFIP organization is that element of the State Department that:

- Overtly collects information relevant to US foreign policy concerns;
- Produces and disseminates foreign intelligence relating to US foreign policy as required for the execution of the SECSTATE's responsibilities;
- Disseminates, as appropriate, reports received from US diplomatic and consular posts;
- Transmits reporting requirements of the IC to the Chiefs of US Missions abroad; and
- Supports Chiefs of Missions in discharging their statutory responsibilities for direction and coordination of mission activities.

g. **FBI Foreign Counterintelligence and International Terrorism Program.** This NFIP element is responsible for:

- Conducting CI activities within the United States;
- Conducting CI activities outside the United States in coordination with the CIA, as required by agreement of the DCI and the Attorney General;
- Collecting, producing, and disseminating foreign intelligence and CI; and
- Carrying out research, development, and procurement of technical systems and devices related to their authorized functions.

h. **Department of Energy Intelligence and Satellite Instrumentation Program.** This program is responsible for:

- Participating with the DOS in overtly collecting information with respect to foreign energy matters;
- Participating in formulating intelligence collection and analysis requirements where the special expert capability of the DOS can contribute; and
- Providing expert technical, analytical, and research capability to other agencies within the IC.

i. **Special NFIP Accounts.** In addition to the programs described above, there are two additional accounts managed as part of the NFIP. These two accounts are the CIA Retirement and Disability System and the Security Evaluation Program.

6. Joint Military Intelligence Program

a. The JMIP is designed specifically to improve the oversight of selected Defense-wide intelligence programs and resources. Defense-wide resources are those initiatives, activities, and programs that predominantly provide intelligence information and support to multiple Defense consumers. The JMIP institutes a management system to oversee programs intended for multiple users, and/or cross-Service support, to ensure genuine responsiveness to the requirements of those who are to be supported and to revitalize the concepts of commonality and interoperability.

b. As the Program Executive, the Deputy Secretary of Defense provides policy and substantive programmatic and fiscal guidance for the JMIP and exercises review and approval authority over JMIP and any subsequent program modifications that significantly alter cost, schedule, or capability. Reprogramming of JMIP funds requires the approval of the Program Executive.

c. The JMIP is composed of four major programs.

- **Defense Cryptologic Program.** The Program Manager is the DIRNSA.

- **Defense Imagery and Mapping Program.** The Program Manager is the Director, NIMA.

- **GI&S Program.** The Program Director is the Director, NIMA.

- **Defense General Intelligence and Applications Program.** The Program Coordinator is the Director, DIA.

d. The DGIAP is comprised of five component programs. Each program focuses on a certain key area of joint support. The Program Coordinator works with each component to best integrate and utilize available resources and assists the five DGIAP component managers in developing their program submissions, resolving programmatic issues across the DGIAP and, in conjunction with those Program Managers, resolves issues across the JMIP. As such, the DGIAP Program Coordinator is the principal interface with the other JMIP programs, NFIP, and TIARA.

- The component programs include:

  •• Defense Airborne Reconnaissance Program.

  •• Defense Intelligence Tactical Program.

  •• Defense Intelligence Counterdrug Program.

  •• Defense Intelligence Special Technologies Program.

  •• Defense Space Reconnaissance Program.

- Each of the above programs consists of former TIARA or selected NFIP programs whose primary customer base was judged to be multiple Service and defense-wide.

e. The JMIP uses the DOD Planning, Programming, and Budgeting System. The JMIP management process avoids the establishment of dedicated panels or working groups to raise and resolve issues by employing existing force such as the Intelligence Systems Board, the MIB, and the Military Communications and Electronic Board.

APPENDIX E
REFERENCES

The development of Joint Pub 2-02 is based upon the following primary references:

1. National Security Act of 1947, as amended.

2. Title 10, United States Code Armed Forces, as amended.

3. Goldwater-Nichols Department of Defense Reorganization Act of 1986.

4. Executive Order 12333, "United States Intelligence Activities."

5. Executive Order 12958, "Classified National Security Information."

6. Joint Pub 1, "Joint Warfare of the Armed Forces of the United States."

7. Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)."

8. Joint Pub 1-0, "Doctrine for Personnel Support to Joint Operations."

9. Joint Pub 1-01, Change 2, "Joint Publication System, Joint Doctrine and Joint Tactics, Techniques, and Procedures Development Program."

10. Joint Pub 1-02, "DOD Dictionary of Military and Associated Terms."

11. Joint Pub 2-0, "Doctrine for Intelligence Support to Joint Operations."

12. Joint Pub 2-01, "Joint Intelligence Support to Military Operations."

13. Joint Pub 2-01.1, "Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting."

14. Joint Pub 2-01.2, "Joint Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Operations."

15. Joint Pub 2-03, "JTTP for Geospatial Information and Services Support to Joint Operations."

16. Joint Pub 3-0, "Doctrine for Joint Operations."

17. Joint Pub 3-07, "Joint Doctrine for Military Operations Other Than War."

18. Joint Pub 5-0, "Doctrine for Planning Joint Operations."

19. Joint Pub 5-00.2, "Joint Task Force Planning Guidance and Procedures."

20. Joint Pub 6-0, "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations."

21. Joint Pub 6-02, "Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems."

22. NDP-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," (Short Title: "National Disclosure Policy.")

23. DOD 5200.2-R, "DOD Personnel Security Program."

24. DOD Directive S-5210.36, "Provision of DOD Sensitive Support to DOD Components and Other Departments and Agencies of the US Government."

25. DOD Directive 5230-11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations."

26. DOD Directive 5240.1, "DOD Intelligence Activities."

27. DOD-0000-151-YR, "DOD Intelligence Production Program."

28. DCS-2600-5345-92, "DIA Guide to Foreign Disclosure."

29. MJCS-51-88, "Doctrine for Intelligence Support to Joint Operations."

30. MCM-15-94, "Memorandum of Agreement Concerning CIA Support to US Military Forces."

31. CJCSI 5118.01, "Charter for the Joint Command and Control Warfare Center."

32. CJCSI 5221.01, "Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations."

33. "Joint-Service Tactical Exploitation of National Systems (J-TENS) Manual."

34. IPSG/INCA-133, "Communications Handbook for Intelligence Planners."

APPENDIX F
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to the Joint Warfighting Center, Attn: Doctrine Division, Fenwick Road, Bldg 96, Fort Monroe, VA 23651-5000. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent and the Joint Staff doctrine sponsor for this publication is the Director for Intelligence (J-2).

3. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J2-J2P/J7-JDD//

Routine changes should be submitted to the Director for Operational Plans and Interoperability (J-7), JDD, 7000 Joint Staff Pentagon, Washington, DC 20318-7000.

b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

4. Distribution

a. Additional copies of this publication can be obtained through Service publication centers.

b. Only approved pubs and test pubs are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PSS, Room 1A674, Pentagon, Washington, DC 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 1 November 1988, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands."

By Military Services:

Army:	US Army AG Publication Center SL 1655 Woodson Road Attn: Joint Publications St. Louis, MO 63114-6181
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Marine Corps Logistics Base Albany, GA 31704-5000
Coast Guard:	Coast Guard Headquarters, COMDT (G-OPD) 2100 2nd Street, SW Washington, DC 20593-0001

d. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R.

GLOSSARY

PART I — ABBREVIATIONS AND ACRONYMS

ACIC	Army CI Center
AC/S, C4I	Assistant Chief of Staff, Command, Control, Communications, Computers and Intelligence (USMC)
ADDO(MS)	Assistant Deputy Director for Operations/Military Support
ADP	automated data processing
AFB	Air Force Base
AFIWC	Air Force Information Warfare Center
AFMIC	Armed Forces Medical Intelligence Center
AFOSI	Air Force Office of Special Investigations
AF/XOI	Air Force Director of Intelligence, Surveillance, and Reconnaissance
AIA	Air Intelligence Agency
ARFOR	Army forces
ASD (C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
BDA	battle damage assessment
C2	command and control
C2P	command and control protection
C2W	command and control warfare
C3I	command, control, communications, and intelligence
C4I	command, control, communications, computers, and intelligence
CAT	crisis action team
CCP	Consolidated Cryptologic Program
CD-ROM	compact disc-read only memory
CE	counterespionage
CI	counterintelligence
CIA	Central Intelligence Agency
CIAP	Central Intelligence Architecture Plan
CJCS	Chairman of the Joint Chiefs of Staff
CJTF	commander, joint task force
CMO	collection management officer
CMS	Community Management Staff
COMSEC	communications security
CONUS	continental United States
CS	Critical Source
CSAT	Critical Source Satellite Terminal
CSG	cryptologic support group (NSA)
CSS	Central Security Service
DA	Directorate for Administration (DIA)
DAC	Directorate for Administrative Counterintelligence and Security Activity

DARO	Defense Airborne Reconnaissance Office
DCCC	Defense Collection Coordination Center
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DCSINT	Deputy Chief of Staff for Intelligence (Army)
DDCI	Deputy Director of Central Intelligence
DDMS	Deputy Director for Military Support
DEA	Drug Enforcement Administration
DGIAP	Defense General Intelligence and Applications Program
DHS	Defense HUMINT Service
DI	Directorate for Intelligence Production (DIA)
DIA	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center
DIEB	Defense Intelligence Executive Board
DIRINT	Director of Intelligence (USMC)
DIRNSA	Director, National Security Agency
DISO	Defense Intelligence Support Office
DM	Director, Military Intelligence Staff
DMS	Director of Military Support
DNI	Director of Naval Intelligence
DO	Directorate for Intelligence Operations (DIA)
DOD	Department of Defense
DODIIS	Department of Defense Intelligence Information System
DODIPP	Department of Defense Intelligence Production Program
DOJ	Department of Justice
DOS	Department of State
DP	Directorate for Policy Support (DIA)
DS	Directorate for Information Systems and Services (DIA)
EAC	echelons above corps
EO	Executive Order
EW	electronic warfare
EXDIR/ICA	Executive Director for Intelligence Community Affairs
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FIS	Foreign Intelligence Service
FTSAT/NISTLITE	Fly Away Terminal Satellite / NIST LITE
GDIP	General Defense Intelligence Program
GI&S	geospatial information and services
HMMWV	high mobility multipurpose wheeled vehicle
HQ	headquarters
HUMINT	human intelligence
I&W	indications and warning
IBS	Integrated Broadcast System

IC	Intelligence Community
ICC	Intelligence Coordination Center (USCG)
IC/EXCOM	Intelligence Community Executive Committee
IEW	intelligence and electronic warfare
IMINT	imagery intelligence
INFOSEC	information security
INMARSAT	international maritime satellite
INR	Bureau of Intelligence and Research (State Department)
INSCOM	United States Army Intelligence and Security Command
IO	information operations
IP	Internet Protocol
ISR	intelligence, surveillance, and reconnaissance
ITF	intelligence task force
IW	information warfare
IWG	intelligence working group
J-2	Intelligence Directorate of a joint staff
J-2A	Deputy Directorate for Administration, Joint Staff
J-2J	Deputy Directorate for Joint Staff Support, Joint Staff
J-2M	Deputy Directorate for Crisis Management, Joint Staff
J-2O	Deputy Directorate for Crisis Operations, Joint Staff
J-2P	Deputy Directorate for Assessment, Doctrine, Requirements, and Capabilities, Joint Staff
J-2T	Deputy Directorate for Targeting Support, Joint Staff
J-2T-1	Target Operations Division, Joint Staff
J-2T-2	Target Plans Division, Joint Staff
J-3	Operations Directorate of a joint staff
JAC	Joint Analysis Center
JC2WC	Joint Command and Control Warfare Center
JCMA	Joint COMSEC Monitor Activity
JCS	Joint Chiefs of Staff
JDISS	Joint Deployable Intelligence Support System
JFC	joint force commander
JFLCC	joint force land component commander
JIC	joint intelligence center
JMICS	JWICS Mobile Integrated Communications System
JMIP	Joint Military Intelligence Program
JMITC	Joint Military Intelligence Training Center
JROC	Joint Requirements Oversight Council
JTF	joint task force
JWAC	Joint Warfare Analysis Center
JWCA	Joint Warfighting Capability Assessment
JWICS	Joint Worldwide Intelligence Communications System
kbps	kilobits per second
LIWA	land information warfare activity
LOS	line of sight

MASINT	measurement and signature intelligence
mbs	megabits per second
MC	Joint Military Intelligence College
MCIA	Marine Corps Intelligence Activity
MI	military intelligence
MIB	Military Intelligence Board
MILSATCOM	military satellite communications
MOOTW	military operations other than war
MSIC	Missile and Space Intelligence Center
NAIC	National Air Intelligence Center
NATO	North Atlantic Treaty Organization
NAVATAC	Navy Antiterrorist Alert Center
NCA	National Command Authorities
NCIS	Naval Criminal Investigative Service
NCR	National Cryptologic Representative
NCRDEF	National Cryptologic Representative Defense
NFIP	National Foreign Intelligence Program
NGIC	National Ground Intelligence Center
NIC	National Intelligence Council
NIMA	National Imagery and Mapping Agency
NIST	national intelligence support team
NMCC	National Military Command Center
NMIC	National Maritime Intelligence Center
NMJIC	National Military Joint Intelligence Center
NRO	National Reconnaissance Office
NRTD	Near Real Time Dissemination
NSA	National Security Agency
NSC	National Security Council
NSOC	National Security Operations Center
NSTS	National Secure Telephone System
NTSS	National Time-Sensitive System
OCONUS	outside the continental United States
OICC	Operational Intelligence Coordination Center
OMA	Office of Military Affairs (CIA)
ONDCP	Office of National Drug Control Policy
ONI	Office of Naval Intelligence
OPCON	operational control
OPSEC	operations security
OSD	Office of the Secretary of Defense
PFIAB	President's Foreign Intelligence Advisory Board
PMGM	Program Manager's Guidance Memorandum
RFI	request for information
RSOC	Regional SIGINT Operations Center

S&T	scientific and technical
SATCOM	satellite communications
SCE	Service cryptologic element
SCI	sensitive compartmented information
SecDef	Secretary of Defense
SECSTATE	Secretary of State
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SSA	Special Support Activity (NSA)
STICS	Scaleable Transportable Intelligence Communications System
STU-III	secure telephone unit-III
TIARA	tactical intelligence and related activities
TS	top secret
TSCM	technical surveillance countermeasures
UHF	ultra high frequency
UK	United Kingdom
USACOM	United States Atlantic Command
USCG	United States Coast Guard
USCS	United States Cryptologic System
USG	United States Government
VTC	video teleconferencing

all-source intelligence. 1. Intelligence products and/or organizations and activities that incorporate all sources of information, including, most frequently, human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the production of finished intelligence. 2. In intelligence collection, a phrase which indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation and reporting systems and resources are identified for possible use and those most capable are tasked. (Joint Pub 1-02)

architecture. A framework or structure that portrays relationships among all the elements of the subject force, system, or activity. (Joint Pub 1-02)

area of intelligence responsibility. An area allocated to a commander in which the commander is responsible for the provision of intelligence within the means at the commander's disposal. (Joint Pub 1-02)

battle damage assessment. The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called BDA. (Joint Pub 1-02)

centers of gravity. Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight. Also called COGs. (This term and its definition modifies the existing term and its definition and will be approved for inclusion in the next edition of Joint Pub 1-02)

coalition force. A force composed of military elements of nations that have formed a temporary alliance for some specific purpose. (Joint Pub 1-02)

collection management. The process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results and retasking, as required. (Joint Pub 1-02)

combat intelligence. That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. (Joint Pub 1-02)

combatant command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (Joint Pub 1-02)

communications intelligence. Technical and intelligence information derived from foreign communications by other than the intended recipients. Also called COMINT. (Joint Pub 1-02)

concept of intelligence operations. A verbal or graphic statement, in broad outline, of a J-2's assumptions or intent in regard to intelligence support of an operation or series of operations. The concept of intelligence operations, which complements the commander's concept of operations, is contained in the intelligence annex of operation plans. The concept of intelligence operations is designed to give an overall picture of intelligence support for joint operations. It is included primarily for additional clarity of purpose. (Joint Pub 1-02)

contingency. An emergency involving military forces caused by natural disasters, terrorists, subversives, or by required military operations. Due to the uncertainty of the situation, contingencies require plans, rapid response, and special procedures to ensure the safety and readiness of personnel, installations, and equipment. (Joint Pub 1-02)

contingency plan. A plan for major contingencies which can reasonably be anticipated in the principal geographic subareas of the command. (Joint Pub 1-02)

coordinating authority. A commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more Military Departments or two or more forces of the same Service. The commander or individual has the authority to require consultation between the agencies involved, but does not have the authority to compel agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. Coordinating authority is more applicable to planning and similar activities than to operations. (Joint Pub 1-02)

counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (Joint Pub 1-02)

data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. (Joint Pub 1-02)

data base. Information that is normally structured and indexed for user access and review. Data bases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files. (Joint Pub 1-02)

deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Joint Pub 1-02)

defense intelligence production. The integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence for known or anticipated military and related national security consumer requirements. (Joint Pub 1-02)

doctrine. Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. (Joint Pub 1-02)

essential elements of information. The critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. Also called EEI. (Joint Pub 1-02)

estimate. 1. An analysis of a foreign situation, development, or trend that identifies its major elements, interprets the significance, and appraises the future possibilities and the prospective results of the various actions that may be taken. 2. An appraisal of the capabilities, vulnerabilities, and potential courses of action of a foreign nation or combination of nations in consequence of a specific national plan, policy, decision, or contemplated course of action. 3. An analysis of an actual or contemplated clandestine operation in relation to the situation in which it is or would be conducted in order to identify and appraise such factors as available and needed assets and potential obstacles, accomplishments, and consequences. See also intelligence estimate. (Joint Pub 1-02)

foreign intelligence. Information relating to capabilities, intentions, and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities. (Joint Pub 1-02)

geospatial information and services. The concept for collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the earth's surface. These data are used for military planning, training, and operations including navigation, mission planning, mission rehearsal, modeling, simulation, and precise targeting. Geospatial information provides the basic framework for battlespace visualization. It is information produced by multiple sources to common interoperable data standards. It may be presented in the form of printed maps, charts, and publications; in digital simulation and modeling data bases; in photographic form; or in the form of digitized maps and charts or attributed centerline data. Geospatial services include tools that enable users to access and manipulate data, and also includes instruction, training, laboratory support, and guidance for the use of geospatial data. Also called GI&S. (This term and its definition are provided for information and are proposed for inclusion in the next edition of Joint Pub 1-02 by Joint Pub 2-03.) Note: GI&S includes what formerly had been referred to as "mapping, charting, and geodesy" or "MC&G."

human intelligence. A category of intelligence derived from information collected and provided by human sources. Also called HUMINT. (Joint Pub 1-02)

human resources intelligence. The intelligence information derived from the intelligence collection discipline that uses human beings as both sources and collectors, and where the human being is the primary collection instrument. Also called HUMINT. (Joint Pub 1-02)

imagery intelligence. Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors, such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. Also called IMINT. (Joint Pub 1-02)

information. 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (Joint Pub 1-02)

intelligence. 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (Joint Pub 1-02)

intelligence doctrine. Fundamental principles that guide the preparation and subsequent provision of intelligence to a commander and staff to aid in planning and conducting military operations. (Joint Pub 1-02)

intelligence estimate. The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. (Joint Pub 1-02)

intelligence operations. The variety of intelligence tasks that are carried out by various intelligence organizations and activities. Predominantly, it refers to either intelligence collection or intelligence production activities. When used in the context of intelligence collection activities, intelligence operations refer to collection, processing, exploitation, and reporting of information. When used in the context of intelligence production activities, it refers to collation, integration, interpretation, and analysis, leading to the dissemination of a finished product. (Joint Pub 1-02)

intelligence preparation of the battlespace. An analytical methodology employed to reduce uncertainties concerning the enemy, environment and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also known as IPB. (Joint Pub 1-02)

intelligence requirement. 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the battlespace or threat forces. (This term and its definition are provided for information and are proposed for inclusion in the next edition of Joint Pub 1-02 by Joint Pub 2-0.)

interoperability. 1. The ability of systems, units or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. 2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (Joint Pub 1-02)

joint doctrine. Fundamental principles that guide the employment of forces of two or more Services in coordinated action toward a common objective. It will be promulgated by the Chairman of the Joint Chiefs of Staff, in coordination with the combatant commands, Services, and Joint Staff. (Joint Pub 1-02)

joint force. A general term applied to a force which is composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (Joint Pub 1-02)

joint force commander. A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command or operational control over a joint force. Also called JFC. (Joint Pub 1-02)

joint intelligence architecture. A dynamic, flexible structure that consists of the National Military Joint Intelligence Center, the theater joint intelligence centers, and subordinate joint force joint intelligence support elements. This architecture encompasses automated data processing equipment capabilities, communications and information flow requirements, and responsibilities to provide national, theater, and tactical commanders with the full range of intelligence required for planning and conducting operations. (Joint Pub 1-02)

joint intelligence center. The intelligence center of the combatant command headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the combatant commander and staff, components, subordinate joint forces and elements, and the national intelligence community. Also called JIC. (This term and its definition are provided for information and are proposed for inclusion in the next edition of Joint Pub 1-02 by Joint Pub 2-0.)

joint intelligence doctrine. Fundamental principles that guide the preparation of intelligence and the subsequent provision of intelligence to support military forces of two or more Services employed in coordinated action. (Joint Pub 1-02)

joint intelligence support element. A subordinate joint force forms a joint intelligence support element as the focus for intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. Also called JISE. (Joint Pub 1-02)

joint task force. A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. Also called JTF. (Joint Pub 1-02)

Joint Worldwide Intelligence Communications System. The sensitive compartmented information portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (Joint Pub 1-02)

measurement and signature intelligence. Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target. The detected feature may be either reflected or emitted. Also called MASINT. (Joint Pub 1-02)

medical intelligence. That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information which is of

interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors. Also called MEDINT. (This term and its definition modifies the existing term and its definition and will be approved for inclusion in the next edition of Joint Pub 1-02)

Military Intelligence Board. A decision making forum which formulates Defense intelligence policy and programming priorities. The Military Intelligence Board, chaired by the Director, Defense Intelligence Agency (DIA), who is dual-hatted as Director of Military Intelligence, consists of senior military and civilian intelligence officials of each Service, US Coast Guard, each Combat Support Agency, the Joint Staff/J-2/J-6, Deputy Assistant Secretary of Defense (Intelligence), Intelligence Program Support Group, DIA's Directorates for Intelligence Production, Intelligence Operations, and Information and Services, and the combatant command J-2s. Also called MIB. (This term and its definition modifies the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

national intelligence support team. A nationally sourced team composed of intelligence and communications experts from either Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, National Imagery and Mapping Agency, or any combination of these agencies. Also called NIST. (Upon approval of this publication, this term and its definition will modify the existing term and its definition and will be included in Joint Pub 1-02.)

National Reconnaissance Office. A Department of Defense agency tasked to ensure that the United States has the technology and spaceborne and airborne assets needed to acquire intelligence worldwide, including support to such functions as monitoring of arms control agreements, indications and warning, and the planning and conducting of military operations. This mission is accomplished through research and development, acquisition, and operation of spaceborne and airborne intelligence data collection systems. Also called NRO. (Joint Pub 1-02)

nuclear intelligence. Intelligence derived from the collection and analysis of radiation and other effects resulting from radioactive sources. Also called NUCINT. (Joint Pub 1-02)

open-source intelligence. Information of potential intelligence value that is available to the general public. Also called OSINT. (Joint Pub 1-02)

operational intelligence. Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or areas of operations. See also intelligence. (Joint Pub 1-02)

operation plan. Any plan, except for the Single Integrated Operation Plan, for the conduct of military operations. Plans are prepared by combatant commanders in response to requirements established by the Chairman of the Joint Chiefs of Staff and by commanders of subordinate commands in response to requirements tasked by the establishing unified commander. Operation plans are prepared in either a complete format (OPLAN) or as a concept plan (CONPLAN). The CONPLAN can be published with or without a time-phased force and deployment data (TPFDD) file. a. OPLAN—An operation plan for the conduct of joint operations that can be used

as a basis for development of an operation order (OPORD). An OPLAN identifies the forces and supplies required to execute the CINC's Strategic Concept and a movement schedule of these resources to the theater of operations. The forces and supplies are identified in TPFDD files. OPLANs will include all phases of the tasked operation. The plan is prepared with the appropriate annexes, appendixes, and TPFDD files as described in the Joint Operation Planning and Execution System manuals containing planning policies, procedures, and formats. Also called OPLAN. b. CONPLAN—An operation plan in an abbreviated format that would require considerable expansion or alteration to convert it into an OPLAN or OPORD. A CONPLAN contains the CINC's Strategic Concept and those annexes and appendixes deemed necessary by the combatant commander to complete planning. Generally, detailed support requirements are not calculated and TPFDD files are not prepared. Also called CONPLAN. c. CONPLAN with TPFDD—A CONPLAN with TPFDD is the same as a CONPLAN except that it requires more detailed planning for phased deployment of forces. (Joint Pub 1-02)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (Joint Pub 1-02)

priority intelligence requirements. Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. Also called PIR. (Joint Pub 1-02)

radar intelligence. Intelligence derived from data collected by radar. Also called RADINT. (Joint Pub 1-02)

reconnaissance. A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (Joint Pub 1-02)

scientific and technical intelligence. The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information which covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel, the research and development related thereto, and the production methods employed for their manufacture. Also called S&TI. (This term and its definition modifies the existing term and its definition and will be approved for inclusion in the next edition of Joint Pub 1-02)

signals intelligence. 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT. (Joint Pub 1-02)

situation assessment. Assessment produced by combining military geography, weather, and threat data to provide a comprehensive projection of the situation for the decisionmaker. (Joint Pub 1-02)

strategic intelligence. Intelligence that is required for the formulation of strategy, policy, and military plans and operations at national and theater levels. (Joint Pub 1-02)

surveillance. The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. (Joint Pub 1-02)

synchronization. 1. The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2. In the intelligence context, application of intelligence sources and methods in concert with the operational plan. (Joint Pub 1-02)

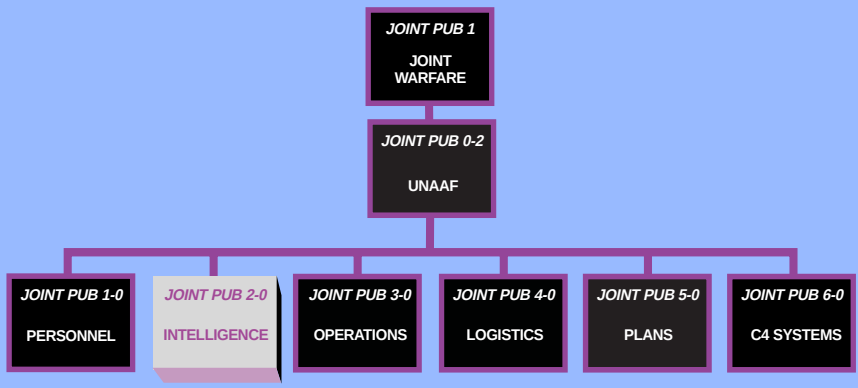
tactical intelligence. Intelligence that is required for planning and conducting tactical operations. Also called TACINTEL. (This term and its definition modifies the existing term and its definition and will be approved for inclusion in the next edition of Joint Pub 1-02)

targeting. 1. The process of selecting targets and matching the appropriate response to them taking account of operational requirements and capabilities. 2. The analysis of enemy situations relative to the commander's mission, objectives, and capabilities at the commander's disposal, to identify and nominate specific vulnerabilities that, if exploited, will accomplish the commander's purpose through delaying, disrupting, disabling, or destroying enemy forces or resources critical to the enemy. (Joint Pub 1-02)

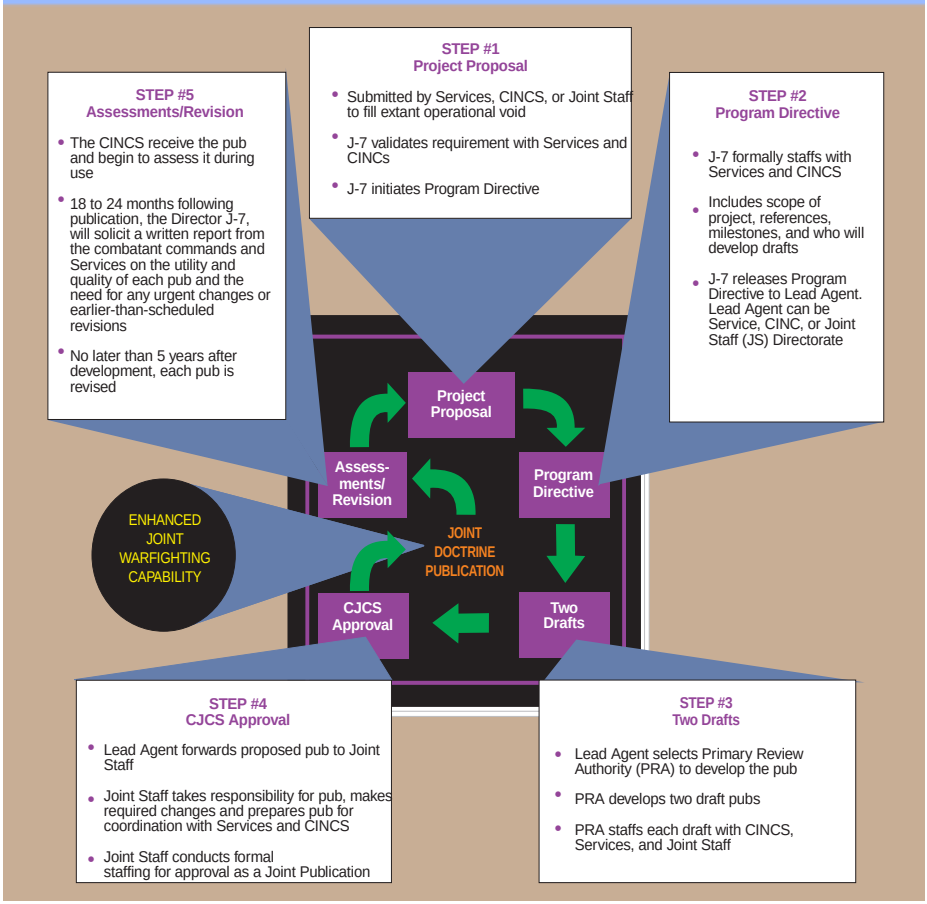
validation. 1. A process normally associated with the collection of intelligence that provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not been previously satisfied. 2. In computer modeling and simulation, the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model or simulation. (Joint Pub 1-02)

Intentionally Blank

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy as shown in the chart above. **Joint Pub 2-02** is in the **Intelligence** series of joint doctrine publications. The diagram below illustrates an overview of the development process:




JOINT
CHIEFS OF STAFF