Chapter 18

Intelligence

"Our job is to facilitate Army Transformation and support warfighting commanders by providing resources, fielding and sustaining the world's premier Military Intelligence Force."

Lieutenant General Keith B. Alexander, Deputy Chief of Staff, G–2, Headquarters, Department of the Army

Section I
Introduction

18–1. Chapter content

a. Army Intelligence is a globally focused, knowledge-based force composed of expert personnel harnessing the collaborative, analytical, communications, and IT to support leaders at the point of decision. It synchronizes sensor and analytical capabilities within a tactical, operational, joint, and combined environment and leverages the capabilities and expertise of the US Intelligence Community (IC), allies, academia, media, and industry to provide commanders focused knowledge.

b. This chapter defines intelligence and provides an overview of how Army Intelligence supports decision makers and outlines the overall intelligence management process within the DOD and the IC. It includes the composition and responsibilities of the various intelligence organizations at national, DOD, non-DOD, and Service (including HQDA) levels. It also describes the relationship of intelligence to Information Operations (IO), operations security (OPSEC), EW, targeting, and providing seamless intelligence support.

c. Intelligence is the product obtained from the systematic planning and directing, collection, processing, analysis and production, and dissemination of information relating to security. This chapter addresses the management of this effort.

18–2. Pending and on-going intelligence-related organizational changes

a. Concurrent with the publication of this text, the National and Defense Intelligence organizations and systems are undergoing substantial changes. These changes are being driven by a multitude of factors: the perceived intelligence deficiencies surfaced by the 9–11 terrorist attack on the World Trade Center; the creation of the Department of HLS and associated intelligence support requirements; the transformation of the Army Intelligence team; and the execution of the War on Terrorism. Some intelligence-related organizational changes include:

(1) The establishment of the Homeland Security Council with the publication of Homeland Security Presidential Directive-1 (HSPD–1) to coordinate all HLS-related activities (including intelligence) among executive departments and develop and implement HLS policies. HSPD -1 also establishes a Homeland Security Policy Coordination Committee (HSC/PCC) for Detection, Surveillance, and Intelligence that serves as the main day-to-day forum for interagency coordination on HLS-related intelligence policy.

(2) The establishment of the Department of Homeland Security with an Information Analysis and Infrastructure Protection Division intended to merge under one organization the capability to identify and assess current and future threats to the homeland, map those threats against our current vulnerabilities, inform the President, issue timely warnings, and immediately take or effect appropriate preventative and protective action.

(3) The creation of the Terrorist Threat Integration Center (TTIC) at the national level to conduct analyses of intelligence gathered by the CIA, FBI, DOD and Department of Homeland Security. The Center is staffed by officials from each of those agencies, compiles a "daily threat matrix," and serves as the intelligence basis for most executive decisions. (The center was transferred to the National Counterterrorism Center by the recently signed Intelligence Reform and Terrorism Prevention Act of 2004.)

(4) The issuance of a Presidential Executive Order (EO) 13356 dated August 27, 2004, strengthening the management of the Intelligence Community and amending EO 12333.

(5) The establishment of the Department of Defense Counterintelligence Field Activity (DoD CIFA) with the mission to develop and manage Counterintelligence programs and functions that support the protection of DoD.

(6) The internal re-organizations of many of the existing sixteen organizations comprising the IC. These include reforms to: increase resources devoted to counterterrorism, develop or improve terrorist threat analytical capability, improve capability to conduct domestic infrastructure vulnerability assessments, fuse foreign and domestic intelligence, create or develop Human Intelligence (HUMINT) sources, broaden the range of customers within compartmentalization limits through media such as CT Link, SIPRNET and Intelink, and form new internal directorates to interface with the newly established Department of Homeland Security.

(7) The establishment of the office of the Under Secretary of Defense for Intelligence to consolidate oversight of the DOD major intelligence agencies under one high-level official. This was followed by the elimination of intelligence responsibilities from the former Assistant Secretary of Defense for Command, Control, Communications and Intelligence ASD(C3I) and the re-designation of the ASD(C3I) as Assistant Secretary of Defense for Networks and

Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO remains responsible for Information Assurance.

(8) Intelligence support for the newly established Assistant Secretary of Defense for Homeland Defense (ASD/HLD) with his principal duty the overall supervision of the homeland defense activities of the DOD and to provide homeland defense related guidance for USNORTHCOM. Both ASD/HLD and NORTHCOM will require intelligence support to adequately protect the CONUS and its contiguous waters from external threats and attacks.

(9) The establishment of the Terrorist Screening Center (TSC), another interagency joint venture, answering to the FBI Director and responsible for providing reliable and updated terrorist watch-list information to the federal, state, local and private sector officials who need it.

(10) Increased information and intelligence sharing between members of the IC including the signing of the Memorandum of Understanding (MOU) on Information Sharing in March 2004 by the Attorney General, Director of Central Intelligence, and Secretary of Homeland Security.

(11) The FBI's establishment of an intelligence program to ensure the collection and dissemination of intelligence receives the same priority as the collection and processing of evidence for criminal investigations. This included the appointment of a new Executive Assistant Director for Intelligence with the authority and responsibility for implementing the FBI intelligence program.

(12) The establishment of the National Counterintelligence Executive (NCIX) and the Office of the National Counterintelligence Intelligence Executive in July 2003 to govern the conduct of Counterintelligence (CI) Activities. The Office was recently transferred from its location in the Office of the Director of Central Intelligence to the Office of the Director of National intelligence.

(13) Intelligence reforms enacted in the aftermath of the National Commission on Terrorist Attacks Upon the United States (referred to as the 9/11 Commission) report. The most sweeping changes were those recently directed by the passage of the *Intelligence Reform and Terrorism Prevention Act of 2004* that included:

- Appointment of a Director of National Intelligence (DNI) with three principal responsibilities: (1) serve as the head of the intelligence community; (2) act as the principal advisor to the President, the NSC, and HSC for intelligence matters; and, (3) oversee and direct the implementation of the National Intelligence Program (formerly known as the National Foreign Intelligence Program).
- Establishment of the National Counterterrorism Center (NCTC) with the primary missions to: (1) serve as the primary organization for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism (excluding intelligence pertaining exclusively to domestic threats); (2) conduct strategic operational planning for counterterrorism activities integrating all instruments of national power; (3) assign roles and responsibilities to lead Departments or agencies for counterterrorism activities consistent with operational planning; (4) ensure all agencies have access to and receive available all-source intelligence required for counterterrorism activities and to perform their assigned missions; and (5) serve as the central and shared knowledge bank for known and suspected terrorists and terrorist groups.
- Establishment of the National Counter Proliferation Center (NCPC) with the mission to prevent and halt the proliferation of weapons of mass destruction, their delivery systems and related materials and technologies.
- Requires the President to designate a Program Manager responsible for information sharing across the Federal Government and improving the Information Sharing Environment (ISE).
- Codified the Information Systems Council, previously established by Presidential Executive Order 13356, and redesignates the Council as the Information Sharing Council that assists the President and the information sharing Program Manager in the improvement of the ISE.
- Formation of the Joint Intelligence Community Council (JICC) designed to assist the DNI in developing a joint, unified national intelligence effort to protect the national security by: (1) advising the DNI on establishing requirements, developing budgets, financial management, and monitoring and evaluating the performance of the intelligence community; and, (2) ensuring timely execution of programs, policies, and directives established or developed by the DNI.
- Subordination of the Director of the CIA under the DNI and the transfer of the DCI's Community Management Staff and National Intelligence Council to the Office of the DNI.
- Transfer of the Terrorist Threat Integration Center (TTIC) to the National Counterterrorism Center.
- Elimination of the CIA positions of Assistant Directors of Central Intelligence for: Collection; Analysis and Production; and Administration, followed by the transfer of those functions to the Office of the DNI.

b. Many of these initiatives have yet to be approved or fully implemented. Consequently, the following sections will reflect the intelligence relationships effective at the time of publication.

18–3. Intelligence drivers

a. Presidential direction. President Reagan signed Executive Order 12333 on 4 December 1981. The EO provides for the effective conduct of U.S. intelligence activities and the protection of the constitutional rights of U.S. citizens. EO 12333 superseded EO 12036, which regulated U.S. intelligence activities during the Carter Administration. The

original EO on the subject was 11905, signed by President Ford. EO 12333 has not been superseded under subsequent administrations. The Army implements EO 12333 through Army Regulations 381–10 and 381–20. Moreover, President Clinton signed a Presidential Decision Directive (PDD) entitled U.S. Counterintelligence Effectiveness - Counterintelligence for the 21st Century on 5 January 2001. The PDD directed the establishment of a National Counterintelligence BOD and established a National Counterintelligence Executive. Most recently, President Bush signed Executive Order 13356 (27 August 2004) further strengthening the management of the Intelligence Community.

b. DOD Transformation. The Nation requires a Joint Force that is full-spectrum dominant to meet the strategic mandates established by the *National Security Strategy* (NSS) and further elaborated with the *Defense Planning Guidance* (DPG); *Quadrennial Defense Review* (QDR); T*ransformation Planning Guidance* (TPG); Joint Operations Concepts (JOpsC) and Joint Operating Concepts (JOCs). As emphasized in the NSS, the military must transform in order to provide the President with a wider range of military options to discourage aggression and any form of coercion against the United States. The new defense strategy rests on a foundation of transformed intelligence capabilities. The TPG emphasizes the criticality of the Intelligence transformation. It states that the ability to defend America in the new security environment requires unprecedented intelligence capabilities to anticipate where, when, and how adversaries intend to attack. The vision of a smaller, more lethal and nimble joint force capable of swiftly defeating an adversary throughout the depth of the global battlespace hinges on intelligence capabilities that:

(1) Warns of emerging crises and continuously monitors and thwarts the enemy's intentions.

(2) Identifies critical targets for, measures and monitors the progress of, and provides indicators of effectiveness for U.S. effects-based campaigns.

(3) Persists across all domains and throughout the depth of the global battlespace, supplying near-continuous access to our most important intelligence targets.

(4) Provides horizontal integration, ensuring that all of the defense systems plug into the global information grid, provides shared awareness systems, and transformed Command, Control, and Communications (C3) systems.

c. Army Transformation. The ATR details Army actions to identify and build required capabilities now, allowing for better execution of joint operations by the Current Force while developing Future Force capabilities essential to provide relevant, ready, responsive, and dominant land power to the Future Joint Force. Military Intelligence (MI) is an essential, important, and integral element of Army Transformation. The Army Intelligence Transformation represents a fundamental change in the way the Army thinks about and performs intelligence collection, analysis, production, and dissemination. The new focus emphasizes the cognitive requirements of knowledge creation. Intelligence Transformation changes the focus from systems and processes to solutions that improve the warfighter's understanding of the battlespace. Fused intelligence and assessment capabilities provide dominant knowledge to the commander— informing decision making and providing predictive cognizance. Intelligence Transformation delivers high-quality and timely intelligence across the range of military operations. Fundamental to achieving this new capability is developing actionable intelligence that is tailored to the needs of the decision maker. Actionable intelligence allows greater individual initiative and self-synchronizing among tactical units. The intelligence challenge is to redefine Army intelligence so that every Soldier is both a contributor to and a consumer of the global intelligence enterprise. While tactical commanders nearest to the fight can leverage modular, tailored packages to develop intelligence, they are also supported by a grid of analytic centers focused on their intelligence needs. To achieve this objective, Army intelligence pursues six fundamental ends:

(1) *Change Army Intelligence Culture:* Create a campaign quality, joint, and expeditionary mindset through doctrine, operational, and personnel policies, regulations, and organizations, to develop intelligence professionals competent from mud to space who know "how to think" and are focused on the commander at the point of decision.

(2) *Fix Training.* Reshape training to provide the volume, variety and velocity of intelligence and non-intelligence reporting.

(3) *Rapid Technology Prototyping:* Develop an agile technology enterprise that enables the intelligence force to respond to a learning enemy with the best technical solutions available in real time.

(4) *Create the Framework:* Create an information and intelligence grid inherently joint, providing common operational picture (COP), universal visibility of assets, horizontal and vertical integration, and situational understanding, linking every "Soldier as sensor and consumer" to analytic centers.

(5) *Enhance Tactical Echelons:* Provide robust, flexible, modular, all-source collection and analytical capabilities, born joint, and part of a tactical force capable of independent action but empowered by linkages to a global grid and analytic and collection overwatch.

(6) *Transform human intelligence (HUMINT) and counterintelligence (CI):* Grow a CI and HUMINT force with a more tactical focus that provides more relevant reporting.

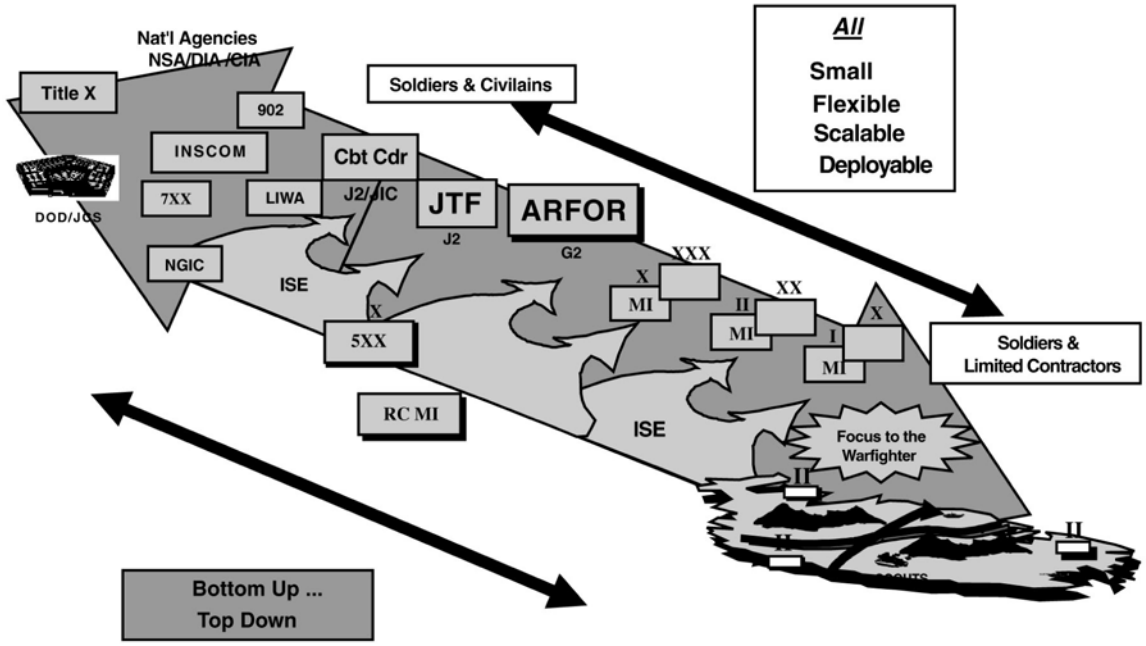

Figure 18–1. Army Intelligence—-Changing Methods and Balance

18–4. Intelligence products

a. Intelligence products may be categorized depending on the intended recipient and scope, level of detail, and the perishability of the product. The distinctions between these types of intelligence products are becoming less pronounced as the nature of offensive, defensive, stability, and support operations overlap within any larger operation. Additionally, technology, including web-enabled technology, facilitates the development, acquisition, and integration of all-source intelligence through a "seamless" architecture from the national to the tactical levels. Examples include the U.S. Army's All Source Analysis System (ASAS), the Joint Worldwide Intelligence Communications System (JWICS), the Secret Internet Protocol Network (SIPRNET), the Joint Deployable Intelligence Support System (JDISS), and other similar types of multidimensional systems and capabilities.

(1) National intelligence is integrated departmental intelligence usually produced by the National Intelligence Council (NIC) (see para 18–5e(2)), coordinated with the National Foreign Intelligence Board (NFIB) and approved by the Director of National Intelligence (DNI). Various finished all-source intelligence products of the IC which are approved by the DNI are also included under the definition of national intelligence. National Intelligence covers the broad aspects of national policy and national security, is of concern to more than one department or agency, and transcends the exclusive competence of a single department or agency.

(2) Departmental intelligence is all-source finished intelligence that is produced by the intelligence components of any department of the federal government without interagency coordination and in direct support of the parent department. This may include intelligence produced by any or all of the following: Department of Homeland Security (Secret Service, Border and Transportation Directorate, U.S. Coast Guard); DOS's Bureau of Intelligence and Research (INR); components of the Department of the Treasury and DOJ; and the DIA and other major intelligence organizations of the DOD.

b. Levels of intelligence use.

(1) The executive and legislative branches of government, departments and selected agencies use intelligence at the strategic level to develop national strategy and policy, monitor the international situation, prepare strategic plans, determine major procurement programs and organizational and force structure requirements, and conduct strategic operations.

(2) Combatant commanders and subordinate JFCs and component commanders are the primary users of intelligence at the operational level. At the operational echelons, intelligence:

- Focuses on the military capabilities and intentions of enemies and threats.
- Provides analysis of events within the AOR and helps commanders determine when, where, and in what strength the adversary might stage and conduct campaigns and major operations.

- Supports all phases of military operations, from mobilization all the way through deployment, employment, sustainment and redeployment of US forces.
- Supports all aspects of the joint campaign.
- Identifies adversary centers of gravity and High Value Targets (HVT).
- Provides critical support to friendly Information Operations (IO).

(3) Tactical commanders use intelligence for planning and conducting battles and engagements. Relevant, accurate, predictive and timely intelligence allows tactical units to achieve an advantage over their adversaries. Precise and predictive intelligence on threats and targets is essential for mission success. Predictive intelligence also enables the staff to better identify or develop Enemy Courses of Action (ECOA). Tactical commanders use intelligence to:

- Identify and assess the enemy's capabilities, vulnerabilities, intentions and expectations.
- Describe the battlespace and its operational impacts.
- Seek to identify the enemy's most likely and most dangerous COAs: when, where, in what strength and for what purpose the enemy will conduct tactical operations.
- Provides critical support to friendly Information Operations (IO).
- Develops and disseminates targeting information and intelligence.

c. Categories of intelligence. The intelligence operations and products of national, joint, and service organizations that make up the intelligence community are classified into one of six categories:

(1) Indications and warnings (I&W) are those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the US or allied/coalition military, political, or economic interests or to US citizens abroad.

(2) Current intelligence involves the integration of time-sensitive, all-source intelligence and information into concise, accurate, and objective reporting on the battlespace and current situation such as the enemy situation portion of the Common Operational Picture (COP).

(3) General military intelligence (GMI) concerns military capabilities of foreign countries or organizations or topics affecting potential US or multinational military operations relating to armed forces capabilities, including Order of Battle (OB), organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness, and area and terrain intelligence. The intelligence planners develop their initial Intelligence Preparation of the Battlefield (IPB) from the GMI database/products.

(4) Target Intelligence is the analysis of enemy units, dispositions, facilities, and systems to identify and nominate specific assets or vulnerabilities for attack, re-attack, or exploitation (for intelligence). It consists of two mutually supporting tasks: target development and combat assessment.

(5) Scientific and Technical Intelligence (S&TI) is the product resulting from the collection, evaluation, analysis, and interpretation of foreign S&T information which covers foreign developments in basic and applied research and in applied engineering techniques and S&T characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems and materiel, the research and development (R&D) related thereto, and the production methods employed for their manufacture.

(6) Counterintelligence (CI) is that intelligence which deals with the information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, subversion, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or terrorist activities. CI is integrated with operations security (OPSEC) and force protection through the CI assessment of the vulnerability of specific U.S. Forces, areas, or activities to foreign intelligence collection, terrorist activities and other hostile operations by intelligence and security services.

d. Intelligence disciplines. Intelligence is also categorized by a series of interdependent disciplines. No single discipline can normally satisfy the commander's requirements. The actual mix of disciplines tasked to satisfy a requirement is situation dependent. The Army lists seven disciplines while JP 2–0 defines eight, the same seven plus Open-Source Intelligence (OSINT). The Army currently defines OSINT as a category of information and not a separate discipline.

(1) *All-source intelligence.* All-source intelligence is defined as the intelligence products, organizations, and activities that incorporate all sources of information and intelligence, including open-source information, in the production of intelligence. All-source intelligence is a separate intelligence discipline, as well as the name of the task used to produce intelligence from multiple intelligence or information source.

(2) *Human Intelligence.* HUMINT is the collection of foreign information by a trained HUMINT Collector from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources as a tool, and a variety of collection methods, both passively and actively, to collect information.

(3) *Imagery Intelligence.* IMINT is intelligence derived from the exploitation of imagery collected by visual photography, infrared, lasers, multi-spectral sensors, and radar. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media.

(4) *Signals Intelligence.* SIGINT is the category of intelligence comprising individually or in combination all

communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), however transmitted. SIGINT is derived from communications, electronics, and foreign instrumentation signals.

(5) *Measurement and Signatures Intelligence.* MASINT is technically derived intelligence that detects, locates, tracks, identifies and/or describes the specific characteristics of fixed and dynamic target objects and sources. It also includes the additional advanced processing and exploitation of data derived from IMINT and SIGINT collection. MASINT collection systems include but are not limited to radar, spectroradiometric, electro-optical (E–O), acoustic, radio frequency (RF), nuclear detection, and seismic sensors, as well as techniques for gathering chemical, biological, radiological, and nuclear (CBRN), and other material samples.

(6) *Technical Intelligence.* TECHINT is intelligence derived from the collection and analysis of threat and foreign military equipment and associated materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical (S&T) capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages.

(7) *Counterintelligence.* CI counters or neutralizes intelligence collection efforts through collection, counter-intelligence investigations, operations, analysis, and production, and functional and technical services. CI includes all actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies; and is the key intelligence community contributor to protect US interests and equities. CI assists in identifying EEFI, identifying vulnerabilities to threat collection, and actions taken to counter collection and operations against US forces

Section II
The National Foreign Intelligence System, system management and oversight, and management of collection and production

18–5. U. S. intelligence community goals and organization

The goal of the U.S. intelligence effort is to provide the President, the NSC, the Homeland Security Council, U.S. policymakers, and military leaders information on which to base decisions concerning the development and conduct of foreign, defense, and domestic policy, and the protection of U.S. interests from foreign threats. The Intelligence community (IC) itself is composed of 16 intelligence agencies, including those in the Departments of Defense, Homeland Security, Justice, Treasury, National Geospatial-Intelligence Agency, Energy, State, the CIA and Office of the Director of National Intelligence. To reach its goals, the U.S. IC is directed and organized as shown in Figure 18–2.

a. The National Security Council (NSC). The NSC supported by the NSC Staff reviews, guides, and directs the conduct of all national foreign intelligence, CI, special activities, and attendant policies and programs. Within the NSC system, the Policy Coordination Committee (PCC) for Intelligence and Counterintelligence formulates policy, monitors decisions, and evaluates the adequacy and effectiveness of collection efforts. It is chaired by the Assistant to the President for National Security Affairs.

b. The Homeland Security Council (HSC). The HSC coordinates all HLS-related activities among executive departments and agencies and promotes the effective development and implementation of all HLS policies. Within the HSC system, the Detection, Surveillance and Intelligence PCC coordinates the development and implementation of intelligence policies by multiple departments and agencies. It is chaired by the Senior Director, Intelligence and Detection within Department of Homeland Security.

c. The President's Foreign Intelligence Advisory Board (PFIAB).

(1) The PFIAB reports directly to the President and provides advice concerning the objectives, conduct, management and coordination of the various activities of the agencies of the IC. In addition to the President, the DNI, the CIA, or other government agencies engaged in intelligence activities can request PFIAB recommendations concerning ways to achieve increased effectiveness in meeting national intelligence needs.

(2) Executive Order 12863, signed by President Clinton on 13 September 1993, established the Intelligence Oversight Board (IOB) as a standing committee of the PFIAB. The IOB is required to report through the PFIAB to inform the President of intelligence activities that any member of the Board believes are in violation of the Constitution or laws of the United States, Executive orders, or Presidential directives; to forward to the Attorney General reports received concerning intelligence activities that the Board believes may be unlawful; to review the internal guidelines of each agency within the IC concerning the lawfulness of intelligence activities; to review the practices and procedures of the inspectors general and general counsels of the IC for discovering and reporting intelligence activities that may be unlawful or contrary to an Executive Order or Presidential Directive; and to conduct such investigations as the Board deems necessary to carry out its functions under this order.

d. Information Sharing Council (ISC). Established by Executive Order 13356 and codified in the Intelligence Reform and Terrorism Prevention Act of 2004, the ISC is chaired by a designee of the Director of Office of Management and Budget and is composed of designees from the Department of State, Treasury, DOD, Commerce, Energy, HLS, the Attorney General, CIA, FBI, NCTC, and others as the Director of OMB may designate. It plans for and oversees the establishment of an interoperable terrorism information sharing environment (ISE) to facilitate the

automated sharing of terrorism information among appropriate agencies and ensures the implementation of related policies. It advises the President and the Presidential designated information sharing Program Manager in developing policies, procedures, guidelines, roles, and standards necessary *to establish, implement, and maintain the ISE.*

e. The Director of National Intelligence (DNI). The DNI is directly responsible to the President, the Homeland Security Council and the NSC. The DNI is the primary adviser to the President and other members of the NSC/HSC on national intelligence and is the intelligence system's principal spokesman to Congress. The DNI develops objectives and prepares guidance for the IC to enhance its capabilities for responding to expected future needs for national intelligence, formulates policies concerning intelligence arrangements with foreign governments, and coordinates intelligence arrangements between agencies of the IC. The DNI also oversees the National Counterterrorism Center and ensures maximum availability of and access to intelligence information within the intelligence community. A complete list of DNI responsibilities is contained in the Intelligence Reform and Terrorism Prevention Act of 2004, S. 2845. Other highlights include:

(1) The DNI establishes objectives and priorities for the intelligence community and manages and directs tasking of collection, analysis, production, and dissemination of National intelligence. The DNI approves requirements for collection and analysis, including requirements responding to the needs of consumers.

(2) The DNI can establish boards, councils, committees, or groups as required for the purpose of obtaining advice from within the IC. Pursuant to S. 2845, the DNI can also establish one or more national intelligence centers to address intelligence priorities, including regional issues. The advisory boards the DNI chairs are the newly established Joint Intelligence Community Council (JICC) and, the DNI will likely assume chairmanship for the National Foreign Intelligence Board, the Intelligence Community Principals Committee and the Expanded DRB (co-chair with DepSecDef).

(3) The DNI assumed substantial authority over the intelligence budget process. The Act directed that the DNI "develop and determine" the annual budget for the National Intelligence Program based upon the proposals provided by the heads of the agencies and organizations of the IC. It is also specified that the DNI be responsible for managing the NIP appropriations by "directing the allotment or allocation" of such appropriations through the heads of the departments containing the agencies or organizations of the IC. This gives the DNI significant leverage in the acquisition and program management efforts of the IC including the intelligence agencies in the DOD.

f. DNI Subordinate Agencies and Activities.

(1) *The National Counterterrorism Center (NCTC).* The NCTC is established in the Office of the DNI. The Director of the NCTC is Senate-confirmed and reports to the DNI on budget and intelligence matters, but to the President on the planning and progress of joint counterterrorism operations (other than intelligence operations). The NCTC conducts "strategic operational planning," which is defined to include the mission, the objectives to be achieved, the tasks to be performed, interagency coordination of operational activities, and the assignment of roles and responsibilities. The NCTC Director monitors the implementation of strategic operational plans and obtains relevant information from departments and agencies on the progress of such entities in implementing the plans. The Terrorist Threat Integration Center (TTIC) was also transferred to the NCTC under the provisions of the Intelligence Reform and Terrorism Prevention Act of 2004. Whether it will be subsumed into NCTC's internal organizational structure or remain a separate entity is yet to be determined.

(2) *The National Counterproliferation Center (NCPC).* The NCPC takes into account all appropriate government tools to prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies. (Note: the Intelligence Reform and Terrorism Prevention Act of 2004 allowed the President to waive the requirement to establish the NCPC. As of the time of this publication, the President had not yet exercised the option of forming the NCPC or waiving this requirement.)

(3) *The National Intelligence Council (NIC).* The NIC was formerly chaired by the Assistant Director of Central Intelligence for Analysis and Production (ADCI/Analysis & Production). The functions performed by the ADCI/ Analysis & Production and the entire NIC were transferred to the Office of the DNI. The council is currently responsible for intelligence analysis and production to include: evaluating community-wide production of intelligence; assessing the analytical capabilities of the IC community; developing DNI guidance on intelligence priorities; providing staff support to the NFIB; and preparing testimony and testifying before Congress. The NIC is comprised of National intelligence officers—senior experts drawn from all elements of the community and from outside the Government. The NIC serves as a senior advisory group to the DNI in his capacity as leader of the IC. National intelligence officers concentrate on the substantive problems of particular geographic regions of the world and of particular functional areas such as economics and weapons proliferation. Through routine close contact with policymakers, collection, research, and community analysis, the NIC provides the DNI with the information needed to assist policymakers as they pursue shifting interests and foreign policy priorities. National intelligence officers lead the IC's effort to produce National Intelligence Estimates (NIEs) and other NIC products. NIEs are the DNI's most authoritative written judgments concerning national security issues and contain the coordinated judgments of the IC regarding the likely course of future events. Finally, the NIC assists the IC by evaluating the adequacy of intelligence support and works with the community's functional managers to refine strategies to meet the most crucial needs of senior consumers.

(4) *The Joint Intelligence Community Council.* The Joint Intelligence Community Council (JICC), chaired by the DNI, is composed of the Secretaries of State, Treasury, Defense, Energy, and Homeland Security, as well as the

Attorney General and such other officers as the President may designate. The JICC shall assist the DNI by advising on budget and other matters and by ensuring the timely execution of the programs, policies, and directives of the DNI.

(5) *The Community Management Staff (CMS).* The CMS was an independent element formerly headed by the Deputy Director of Central Intelligence/Community Management (DDCI/CM). This staff was transferred in its entirety to the Office of the Director of National Intelligence. The duties performed by this staff essentially executed the duties and missions for the DCI that are now among the responsibilities of the DNI. These duties include the overall management of the NIP and IC personnel and resources; ensuring the effective collection of national intelligence; oversight of intelligence analysis and production by IC component agencies; developing, coordinating, and executing the DNI's community responsibilities for resource management; program assessment and evaluation of policies; and collection requirements management. These roles and missions will be subsumed in the organizational structure and functions of the Office of the DNI.

(6) *The Collection Staff.* The functions associated with the Assistant Director of Central Intelligence for Collection was also transferred to the DNI. The Office of the DNI will now perform the efficient and effective collection of national intelligence.

g. IC Committees and Boards.

(1) *Intelligence Community Principals and Deputies Committee (IC/PC & IC/DC).* This committee serves as the senior advisory board to the senior intelligence official (now the DNI) on intelligence planning, needs management and evaluation, and decisions affecting NIP programs. The IC/PC is the principal forum through which major policy issues impacting the IC are addressed. Permanent IC/PC members now include the DNI and his deputy (Principal Deputy Director of National Intelligence (PDDNI)) as well as the following members: Director of the CIA; VCJCS; Director, NSA; Director, DIA; Assistant Secretary of State for INR; Director, NRO; Director, NGA; Chairman, NIC; USD (I); and the DNI deputy for CM. Similarly, the IC Deputies Committee (IC/DC) provides another venue for senior-level coordination and addresses major policy issues affecting the IC. The committee will be chaired by the PDDNI and consists of the deputies of the IC component agencies. This body attempts to address and resolve issues not requiring the IC/PC level involvement.

(2) *National Foreign Intelligence Board (NFIB).* The DNI will also likely assume the chair of the NFIB with the PDDNI serving as the Vice Chairman. The NFIB is responsible for approving all National Intelligence Estimates (NIEs), for coordinating interagency intelligence exchanges and the numerous bilateral relationships with foreign nations that share intelligence with the United States, and for developing policy for the protection of intelligence sources and methods.

(3) *Expanded Defense Resources Board (EDRB).* The EDRB meets during the decision making stage of the Capabilities Programming and Budgeting System (CPBS) and the PPBE Process to deliberate on major issues involving all DOD NIP programs, the Joint Military Intelligence Program (JMIP), and the Tactical Intelligence and Related Activities (TIARA) program. During each budget cycle the DRB is temporarily expanded to include the DNI and several IC officials to make recommendations on major defense intelligence program/budget issues.

(4) *Intelligence Program Review Group (IPRG).* The IPRG integrates the program and budget reviews across the three major intelligence programs (NIP, JMIP, TIARA) by reviewing issues, analyzing priorities, and examining funding alternatives. The IPRG will fall under the Office of the DNI and will likely continue to be supported by the CM staff that will serve as the permanent secretariat and administrative support for its members.

(5) *National Intelligence Collection Board (NICB).* The NICB acts as the IC's coordinating body for seamless, cross-discipline, collaborative intelligence. The NICB is composed of representatives from all agencies involved in collection to include all sources and discipline specific. It is chaired by the ADCI/Collection (whose functions were transferred to the Office of the DNI) and addresses strategic collection issues to include developing recommendations for collection strategies.

(6) *National Intelligence Production Board (NIPB).* The NIPB is chaired by the ADCI/Analysis & Production (whose functions were transferred to the Office of the DNI). The Board addresses analysis and production issues by serving as the major conduit for customer-driven intelligence priorities; encouraging cross community initiatives; and leading assessments and evaluations of IC analytical capabilities.

h. Central Intelligence Agency (CIA). The CIA reports to the Director of National Intelligence regarding the activities of the CIA. The internal organization and structure of the CIA will likely be modified after the Office of the DNI is completely established and the roles and responsibilities of both organizations are further refined. Currently the Director of the CIA is responsible for:

(1) Collecting intelligence through human sources and by other appropriate means including a variety of clandestine and overt means. The Agency also engages in research, development, and deployment of high-leverage technology for intelligence purposes. The CIA is organized along functional lines to carry out these activities and to provide the flexible, responsive support necessary for its worldwide mission.

(2) Correlating and evaluating intelligence related to the national security and providing appropriate dissemination of such intelligence. The agency emphasizes adaptability to meet the needs of intelligence consumers. To assure that all of the Agency's capabilities are brought to bear on those needs, the CIA has tailored its support for key policymakers and has established on-site presence in the major military commands.

(3) Providing overall direction for and coordination of the collection of national intelligence outside the United States through human sources by elements of the intelligence community.

(4) Performing other functions and duties related to intelligence affecting the national security as the President or the DNI may direct.

(5) Supporting military plans and operations through the Office of Military Affairs (OMA) in the CIA. The OMA falls under the Associate Director of Central Intelligence for Military Support, a flag rank military officer, and provides a central point of contact to the military departments to facilitate coordination with the CIA.

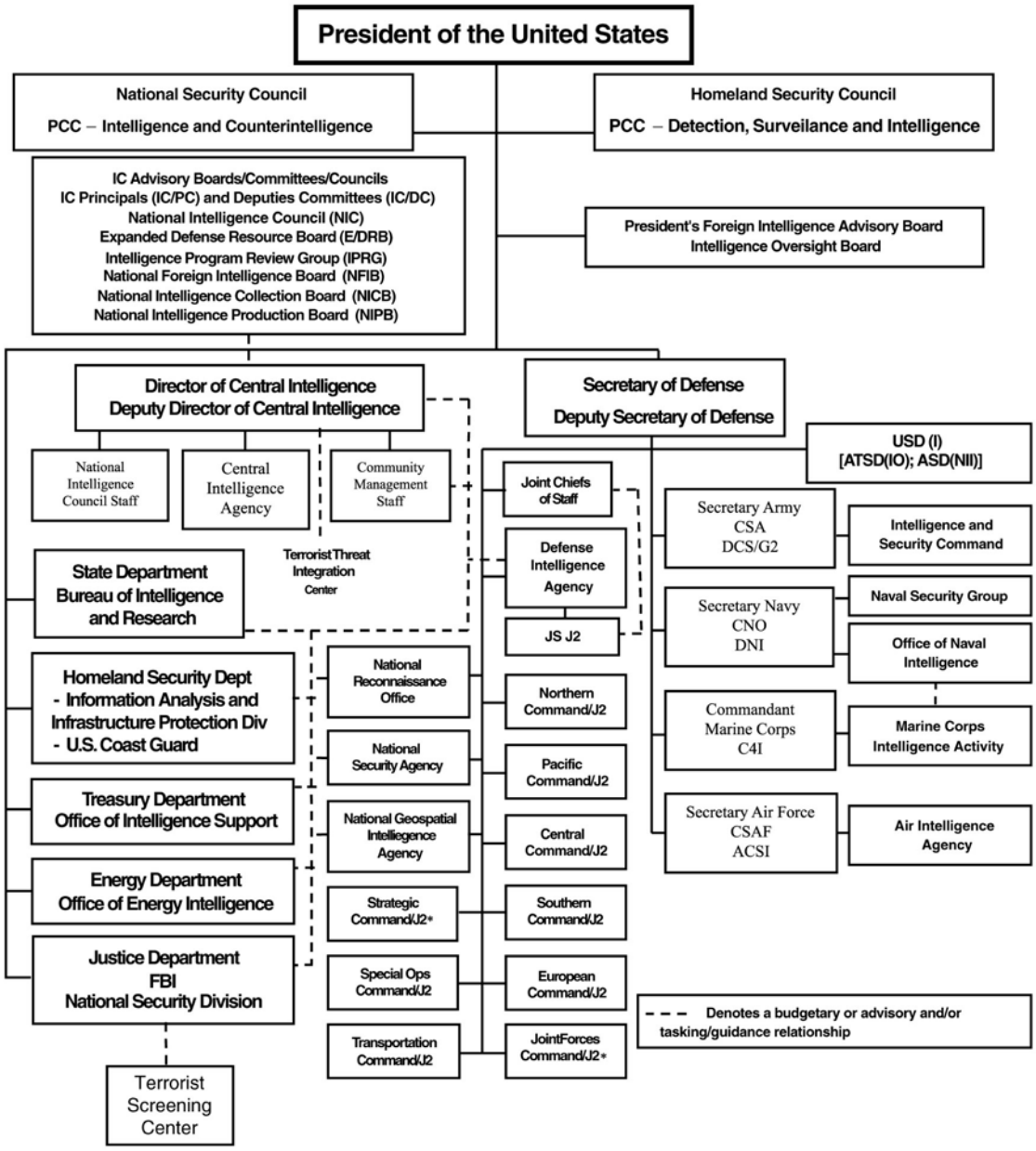

Figure 18–2. Organization of the National Intelligence System

18–6. Executive and Congressional intelligence resource management

The NSC and Homeland Security Council provide overall executive branch guidance, direction, and review for all national foreign intelligence and IC activities. Within the legislative branch, the House Permanent Select Committee on Intelligence (HPSC(I)) and the Senate Select Committee on Intelligence (SSC(I)) along with the Foreign Relations, Foreign Affairs, and the Armed Services Committees are responsible for authorizing intelligence resources and overseeing intelligence activities. The appropriations committees are authorized by the Constitution to appropriate funds for all government activities, including intelligence activities. The NSC and HSC systems have special committees within its framework, which deal with its intelligence responsibilities. In addition to the management of the individual agencies or elements thereof, which constitute the intelligence system, management of intelligence focuses mainly on intelligence resources, requirements, collection tasking, collection, analysis, production and dissemination. While not a member of the IC, the OMB provides program and budget guidance to the DNI for development of the NIP as part of the Federal budget. Within the DOD, the Under Secretary of Defense (Intelligence) (USD(I)) is the DOD focal point for intelligence management.

a. National Intelligence Program (NIP), formerly known as the National Foreign Intelligence Program (NFIP). The NIP provides funds for the bulk of all national-level intelligence, CI, and reconnaissance activities of the DNI, CIA, DOD, and all civilian Federal agencies and departments, as well as the IC management structure. The program is comprised of two major components - national-level intelligence programs within the DOD and those in Federal departments and agencies outside DOD. The defense programs include the General Defense Intelligence Program (GDIP), the Consolidated Cryptologic Program (CCP), the DOD Foreign Counterintelligence Program (FCIP), the National Geospatial-Intelligence Agency Program (NGAP), the National Reconnaissance Program (NRP), and specialized DOD reconnaissance activities. The PM for the GDIP is the Director, DIA; PM for the CCP is the Director, NSA; PM for the FCIP is the Director of Counterintelligence. PM for the NGAP is the Director, NGA; and PM for the NRP is the Director, NRO.

b. Joint Military Intelligence Program (JMIP). The JMIP focuses on joint, defense-wide initiatives, activities and programs that predominantly provide intelligence information and support to multiple defense consumers; bridge existing programmatic divisions across Service, departmental and national intelligence lines to provide more effective and coherent intelligence programmatic decision-making; and ultimately support MI consumers. These include warfighters, policymakers, and force modernization planners. The JMIP is composed of four programs: the Defense Cryptologic Program, Defense Imagery and Mapping Program, the Defense Joint Counterintelligence Program and the Defense General Intelligence and Applications Program. The Defense General Intelligence and Applications Program, coordinated by the Director, DIA is further divided into five components. The components of this program include the Defense Airborne Reconnaissance Program, the Defense Intelligence Tactical Program, the Defense Intelligence Counterdrug Program, the Defense Intelligence Special Technologies Program, and the Defense Space Reconnaissance Program.

c. Combatant Command and Service participation. COCOM commanders formally participate in the Capabilities Programming and Budgeting System and influence the DOD PPBE process for intelligence resources through their COCOM Commander's IPL. Through the Command Intelligence Architecture Program, COCOM commanders identify their intelligence collection, processing, and dissemination resource requirements. The Command Intelligence Architecture Program has become the driving force for acquiring the requisite MI capabilities into the 21st century.

(1) Within HQDA, the Deputy Chief of Staff, G–2 participates in the PPBE Process through the PEGs and membership on the PPBE Process COC; Planning, Programming, and Budget Committee; and Senior Resource Group.

(2) The Army participates directly in three of the programs of the NIP: the Consolidated Cryptologic Program, the FCIP and the GDIP. Program and budget information is prepared by the Army and sister Services and forwarded through PMs to the DNI.

(3) In addition to the NIP budget, many Army intelligence resources are included in the DOD Joint Military Intelligence Program and TIARA funding. These programs include most intelligence resources directly supporting operational commanders at the Joint and Service levels.

d. TIARA accounts. TIARA accounts provide funding for timely intelligence support primarily to tactical operations of military forces. TIARA activities and systems are planned, programmed, and executed by the military Services and USASOC and compete for funding with the combat and combat-support programs they support. As defined by the Congress, TIARA funds represent those portions of the DOD budget devoted to Service-level MI activities outside the NIP. TIARA is an aggregation of portions of the DOD budget that provide tactical intelligence and related support to military operations. In contrast to the NIP, countless military officials on a decentralized basis manage TIARA assets.

e. Intelligence oversight. The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence play key roles in the conduct of intelligence oversight. These roles, specified by law, require that the committees be kept fully informed of all intelligence activities that are the responsibility of, are engaged in by, or are carried out for or on behalf of any department; that they be furnished any information or material concerning

intelligence activities requested in order to carry out authorized responsibilities; and that the committees be informed in a timely fashion of any illegal intelligence activity or significant intelligence failure and any corrective action.

(1) Within the DOD the officer responsible for the oversight of intelligence activities is the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD–IO). DOD Directive 5148.11, dated May 21, 2004, establishes the responsibilities, functions, relationships and authorities of the ATSD–IO. The ATSD–IO had been designated as the sole conduit between the DOD and the President's Intelligence Oversight Board. Upon the establishment of the JMIP, the Secretary of Defense (SecDef) also created the Defense Intelligence Executive Board as a management mechanism to provide oversight of Defense intelligence programs, and to make key decisions for the allocation of available resources to meet defense needs.

(2) The Army General Counsel and the Army Inspector General share responsibility for the oversight of intelligence activities within the Army.

18–7. Intelligence process

Generally, the intelligence process consists of planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; and evaluation and feedback. Intelligence requirements and production management guide the bulk of the process and the expenditures of resources. Within the Army, the design and structure of the intelligence operations support the commander's operations process by providing him with intelligence regarding the enemy, the battlefield environment, and the situation. Intelligence operations consist of the functions that constitute the intelligence process: plan, prepare, collect, process, produce, and the three common tasks of analyze, disseminate, and assess. Just as the activities of the operations process overlap and recur as circumstances demand, so do the functions of the intelligence process. Additionally, the analyze, disseminate, and assess functions of the intelligence process occur continuously throughout the intelligence process. The operations and intelligence processes are mutually dependent.

a. Requirements management. The intelligence process begins and ends with the consumer. A consumer's requirements are passed to the producer for fulfillment. If the producer cannot satisfy the consumer's requirements, the producer levies the requirement on the collector. The user must be able to state clearly the intelligence interests or needs (requirements) in addition to those that are already satisfied by existing finished intelligence. Requirements compete for limited collection resources at the national, departmental, strategic, operational, and tactical levels. Requirements are prioritized in accordance with the intelligence requirements contained in a classified 2 March 1995 Presidential Decision Directive 35, which established as its highest priority, intelligence support to military operations. The military commander must however make a case for the priority of his or her requirement if resources not assigned or organic to his or her command are needed to fulfill the requirement. Army tactical intelligence requirements are satisfied primarily through Intelligence, Surveillance, and Reconnaissance (ISR) operations focused on the Commander's Critical Information Requirements (CCIRs) and managed by an intelligence synchronization plan. The intelligence officer, with staff participation, synchronizes the entire collection effort to include all the assets the commander controls, knowledge of the collection efforts of lateral and higher echelon units and organizations, and intelligence reach to answer the commander's priority intelligence requirements (PIRs) and Information Requirements (IRs). Requirements are managed at higher levels in a conceptually similar manner:

(1) The DIA, in its support role to the JCS, prepares a listing of intelligence priorities for strategic planning for JCS publication and validates the intelligence requirements of the Services. A prioritized list of both long-term and short-term national interests is established by the NSC and passed to the DNI. There a determination is made as to whether sufficient intelligence exists to fulfill the requirement or whether additional intelligence is needed. If it is, detailed prioritized requirements are passed to the Office of the DNI (CM Staff) for collection tasking.

(2) All collection operations are conducted in response to validated requirements for the production of finished intelligence. The ADCI/Collection (whose functions are now resident in the Office of the DNI) is responsible for the efficient and effective collection of national intelligence by IC component agencies. The Office of the DNI (CM Staff) tasks its members for collection to fulfill prioritized requirements. The selection of the specific collection resource rests with the department or the PM. The management aspects of collection involve ensuring that the assets selected are the most cost-effective that can fulfill the requirement on a timely basis.

(3) Collection operations tasked by the DIA in response to DOD-generated requirements are normally conducted on an all-source, common-service basis. Conversely, the conduct of intelligence operations at the tactical level to directly support the commander's immediate needs is usually accomplished by assigned or supporting intelligence organizations. Tactical commanders obtain much of their information on their areas of operation from assigned or supporting assets including MI units, artillery, cavalry, aviation, and maneuver units in contact. However, tactical commanders leverage national/theater collection capabilities by placing small numbers of tactical force intelligence soldiers at key nodes in the intelligence system to provide direct response to the supported commanders' requirements. Additional information and intelligence on the area of interest is provided from higher echelons.

b. Analysis and production management. National intelligence production is the responsibility of the DNI and is exercised through the ADCI/Analysis and Production (whose functions are now resident in the Office of the DNI) which establishes schedules and priorities for national intelligence production conducted by the IC. The Office of the DNI is responsible for the production and dissemination of all-source intelligence.

(1) No single intelligence product format usually meets the needs of all consumers. It is necessary to have a continuing dialogue between the consumer and the producer of intelligence assuring the consumer does not influence the conclusions of the product.

(2) The most prestigious intelligence product is the President's Daily Brief (PDB), which is currently prepared by the CIA and forwarded to the President. The Intelligence Reform and Terrorism Prevention Act of 2004 did not address the preparation of the PDB. However, since this is the principal daily intelligence report to the President, it is likely that the DNI will assume this responsibility. Other national reports include the Senior Executive Intelligence Brief (SEIB). The SEIB is also currently produced by the CIA in coordination with other intelligence agencies and contains key current intelligence items. It is produced six days a week and regularly forwarded to major U.S. military commands and overseas diplomatic posts. The CIA also produces many other products including: the Economic Executives' Intelligence Brief, serial publications and situations reports (regional reviews, terrorism reviews, narcotics monitor, proliferation digest, and international arms trade reports) and research studies (special intelligence reports, intelligence memoranda, and intelligence reports). Some of these will also likely transfer to the Office of the DNI.

(3) Individual departments and agencies establish their own production schedules and priorities for the production of departmental intelligence. The DIA establishes production schedules in the DOD and distributes responsibilities among the COCOMs and services.

(4) The DIA Directorate for Intelligence Production produces and manages the production of all-source MI knowledge base to support the policy, planning, and operational requirements of the OSD; JCS; the Services; and the COCOMs. As the DOD Production Functional Manager, the Directorate for Intelligence Production ensures that DOD intelligence production requirements are articulated; resources are programmed and executed in compliance with national and DOD guidance; and programs are re-evaluated as missions, technical capabilities, and threat environments change. It also operates the Operational Intelligence Crises Center which manages crisis-related all-source MI.

Section III
Defense and Army Intelligence and uses of intelligence

18–8. Department of Defense (DOD)

The DOD is the nation's largest user of intelligence information and the largest investor in intelligence programs. The DOD has an overriding responsibility to support commanders at all levels.

a. Secretary of Defense (SecDef). The SecDef exercises full direction, authority, and control over the day-to-day intelligence activities of the DOD. Success of DOD missions depends on the collection, analysis, production, and dissemination of timely, relevant, accurate, fused, and predictive intelligence on the capabilities and intents of foreign powers.

(1) Defense intelligence, as part of the IC, is faced with a growing number of challenges to the successful accomplishment of its defense intelligence mission. The international environment has grown more complex with the emergence of transnational threats. Changing political alignments and instability, concern for WMD proliferation, growing economic interdependence, nationalistic tendencies and ethnic rivalries, increased international terrorism, international crime, health and ecological security issues have all resulted in more diverse intelligence requirements. The nature of many of these complexities limits collection efforts and other targets are protected by relatively sophisticated command, control and communications systems, which are readily available to even the poorest countries.

(2) To strengthen the DOD performance of its intelligence functions, on 8 May 2003, the SecDef approved a plan for restructuring defense intelligence. Essentially, the memo established the USD(I) as the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary on all intelligence, counterintelligence and security, and other intelligence-related matters and outlined the USD(I) roles and responsibilities.

b. Office of the Under Secretary of Defense for Intelligence (OUSD(I)). The USD(I) has as a primary duty the overall supervision of all intelligence affairs of the DOD. The USD(I) is the DOD principal staff assistant for the development, oversight, and integration of all DOD policies and programs relating to intelligence and counterintelligence and security. The USD(I) is responsible for providing capabilities that enable the U.S. military forces to generate, use, and share the information necessary to survive and succeed in our national security missions. The USD(I) exercises authority, direction, and control over the DIA, NGA, NRO, NSA, DSS, and the DoD Counterintelligence Field Activity (CIFA).

c. Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)). The ATSD(IO) serves as the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for the independent oversight of all intelligence, counterintelligence, and intelligence-related activities in DoD. The ATSD(IO) ensures that all intelligence activities performed by DoD are conducted in compliance with Federal law, Executive orders, Presidential directives, and DoD Directives System issuances.

d. Defense Intelligence Agency (DIA). The Director, DIA is responsible for satisfying the foreign military requirements (less cryptologic) of the SecDef, OSD, CJCS, Office of the JCS (OJCS), JS, COCOM Commanders, major DOD components, and other U.S. Government agencies, allied governments, and coalition partners (when required), and has been designated by the CJCS as a DOD combat support agency. DIA provides defense intelligence contributions to

national intelligence estimates and production capabilities. The Director, DIA is a member of the National Foreign Intelligence Board and is the DOD intelligence collection manager. DIA produces, or through tasking and coordination, ensures the production of foreign military and military-related intelligence. To provide daily support to the COCOMs and U.S. Forces Korea, NATO, and Supreme Headquarters Allied Powers Europe (SHAPE), the DIA initiated on-site liaison elements managed by an experienced senior civilian intelligence officer. These liaison elements, called Defense Intelligence Support Offices, expedite actions between DIA and the commands. The DIA supervises the DOD Indication and Warning System and provides support to the NMCC through the National Military Joint Intelligence Center (NMJIC). The DIA has the responsibility to satisfy the DOD intelligence collection requirements and to coordinate and review activities of the DOD collection resources not assigned to the DIA

(1) To provide tailored support to a joint force commander, DIA can deploy national intelligence support teams (NIST) composed of DIA, NSA, and CIA personnel as well as personnel from other organizations, as required. The NIST deploys with its organic support capability and provides critical on-site intelligence connectivity between the supported command and Washington to ensure receipt of national-level intelligence. DIA also shares or provides intelligence support to the President, NSC Staff, Homeland Security Council, National Warning Staff, Departments of Energy/State/ Treasury/ and Commerce, and the NGA. The DIA provides central management for the Central MASINT Organization and operates the Defense HUMINT Service, with its subordinate Defense Attaché System and HUMINT Operating Bases. DIA also operates the Joint Military Intelligence College.

(2) The Military Intelligence Board (MIB), chaired by the Director of the DIA and composed of the senior intelligence officers of the U.S. Army, U.S. Air Force, U.S. Navy, and U.S. Marine Corps, advises the SecDef and Defense agencies on matters pertaining to MI. The concerns of the COCOMs are represented by DIA's Directorate for Intelligence which functions as the Joint Staff J2. The MIB serves as the senior "Board of Governors" for the intelligence organization in DOD and advises the SecDef, CJCS, Military Service Chiefs, COCOM Commanders, and defense agencies on matters pertaining to MI. The Director DIA seeks consensus across the IC through the MIB process.

e. National Security Agency (NSA) and Central Security Service. The Director of the NSA is the Chief of the Central Security Service (CSS) and manages the Consolidated Cryptologic Program, the largest single program in the NIP. The Director is responsible for the operations of an effective unified organization for SIGINT activity. No other department or agency may engage in such activity without a delegation of authority by SecDef. The NSA's SIGINT collection, processing, and dissemination activities are extremely sensitive and involve both positive and CI information and are in DS of military commanders and operations and responsive to national foreign intelligence requirements. The NSA/CSS is also a JCS Combat Support Agency.

(1) The Director of the NSA is responsible for the R&D required to meet the needs for SIGINT and communications security (COMSEC). The Director is the executive agent for executing the responsibilities of the SecDef for the COMSEC of the Government. The Director also has oversight of the Defense Cryptologic Program that lies outside the NIP, and is responsible for providing cryptologic training and training support to the Services.

(2) NSA also has the mission of information security (INFOSEC). As the world becomes more and more technology-oriented, the INFOSEC mission becomes increasingly challenging. This mission involves protecting all classified and sensitive information that is stored or sent through U.S. Government equipment. INFOSEC professionals go to great lengths to make certain that Government systems remain impenetrable. This support spans from the highest levels of U.S. Government to the individual warfighter in the field.

f. The National Geospatial-Intelligence Agency (NGA). The NGA (formerly National Imagery and Mapping Agency (NIMA)) was established on 1 October 1996 to address the expanding requirements in the areas of imagery, IMINT, and geospatial information.

(1) The NGA consolidated all functions of the Defense Mapping Agency. These include defense mapping, charting, and geodetic operations; production, source data storage and retrieval, and management of distribution facilities; and supervision of the Hydrographics/Topographic Center and the Defense Mapping School. NGA also incorporated all functions of the Central Imagery Office, National Photographic Interpretation Center, and some imagery exploitation, dissemination, and processing elements of the DIA, NRO and the Defense Airborne Reconnaissance Office. NGA develops and makes recommendations on national imagery policy and is chartered to ensure responsive imagery support to the DOD, the CIA, and other Federal Government departments. The NGA tasks and evaluates imagery elements of the DOD to meet national intelligence requirements and ensures imagery systems are exercised to support military forces.

(2) Within the DOD, the NGA establishes the architectures for imagery tasking, collection, processing, exploitation, and dissemination. NGA has responsibility for establishing standards for imagery systems for which the DOD has responsibility, and ensures compatibility and interoperability of these systems. Standards for training of personnel performing imagery tasking, collection, processing, exploitation, and dissemination functions are established by NGA. NGA also supports and conducts R&D activities related to this imagery function.

g. National Reconnaissance Office (NRO). The NRO is the single, national program to meet U.S. Government needs through space borne reconnaissance. The NRO is an agency of the DOD. The DepSecDef, as recommended by the Director of Central Intelligence, declassified its existence on 18 September 1992. The mission of the NRO is to ensure that the U.S. has the technology and space borne assets needed to enable U.S. global information superiority. This

mission is accomplished through research, development, acquisition, and operation of the nation's intelligence satellites. The NRO's assets collect intelligence to support functions of indications and warning, arms control agreements, military operations and exercises, and natural disasters and other environmental issues.

h. Defense Security Service (DSS). The Defense Security Service (DSS) is a separate agency of the Department of Defense under the direction, authority and control of the USD(I). DSS is assigned the administration of four programs: The Personnel Security Investigations Program; The Defense Portion of the National Industrial Security Program; The Arms, Ammunition and Explosives Program and the key asset Protection Program. Additionally, DSS has a counterintelligence office to ensure that agency mission areas support the national counterintelligence strategy through the integration of counterintelligence into all DSS security countermeasures activities. The DSS is a law enforcement, personnel security investigative and industrial security agency. Note: the DSS employees and investigative functions were scheduled to be transferred outside of DoD and into the Office of Personnel Management (OPM) in FY '04. However, the transfer was delayed pending the attainment by DSS of OPM-specific investigative performance standards and final acceptance by the OPM Director of the transfer of the DSS.

i. Department of Defense Counterintelligence Field Activity (DoD CIFA). The DoD CIFA has the mission to develop and manage Counterintelligence programs and functions that support the protection of the Department, including CI support to protect DoD personnel, resources, critical information, research and development programs, technology, critical infrastructure, economic security, and U.S. interests, against foreign influence and manipulation, as well as to detect and neutralize espionage against the DoD. It is a Field Activity within the DoD under the authority of the USD(I). However, for certain functions specified in DoD Directive 5105.67, the DoD CIFA is treated as a Combat Support Agency. It consists of the Joint Counterintelligence Evaluation Group, the Defense CI Information System (DCIIIS) Program Office, the Joint CI Training Academy (JCITA), and the Defense CI Force Protection Response Group (FPRG).

18–9. Army intelligence system

The SECARMY has delegated to the Under Secretary of the Army responsibility for the general supervision of the intelligence, CI, investigative, and intelligence oversight activities of the Army. The intelligence and CI elements of the military Services are responsible for the planning, direction, collection, processing, and dissemination of military and military-related intelligence, including information on indications and warnings, foreign capabilities, plans and weapons systems, and scientific and technical developments. See Figure 18–3 for a simplified organization of the Army intelligence system. The conduct of CI activities and the production and dissemination of CI studies and reports is a Service responsibility as are the development, procurement, and management of tactical intelligence systems and equipment; the conduct of related research, development, and test and evaluation activities; the development of intelligence doctrine; and the training of intelligence personnel.

a. Deputy Chief of Staff, G–2. The G–2 is the intelligence officer for the U.S. Army and is responsible to the Chief of Staff for the policy formulation, planning, programming and budgeting (shared with the Deputy Chief of Staff for Programs (DCSPRO) for JMIP and TIARA), management, propriety and overall coordination of the intelligence and CI activities of the Army. The G–2 has general staff responsibility for intelligence, CI, intelligence automation, SIGINT, IMINT, MASINT, TECHINT, Open Source Intelligence (OSINT), threat validation, intelligence collection, security, meteorological, topographic, and space activities; and monitors Army intelligence training, force structure, and readiness for both the Active Army and Reserve Components. The G–2, under the general guidance and tasking of DIA, exercises general staff supervision over Army and Army-supported Intelligence Data Handling System resources and over all-source intelligence production within the Army. The G–2 is responsible for Major Force Program 31 (Intelligence) within the Army. The G–2 is also responsible for the Army's input into the DOD Consolidated Cryptologic Program; the GDIP; the FCIP; the Defense Joint Counterintelligence Program and Service funded programs supporting the Army Security and Intelligence Activities Program. In addition, the G–2 is responsible for the Army input to TROJAN, foreign language sustainment, imagery dissemination, unique MI skill sustainment for Active Army and Reserve Component soldiers, Personnel Security Investigations; and is the Army proponent for foreign languages. The G–2 serves as the ISR integrator for HQDA in coordination with the G3 and participates in the Army POM build by providing advice to senior PMs on the ranking of intelligence requirements. Moreover, the G–2 coordinates intelligence requirements with MACOMs during submission of the POM assessments.

(1) The G–2 also shares management, in the DA, with the ASA(M&RA) for the DCIPS (formerly known as the Civilian Intelligence Personnel Management System). DCIPS is the accepted service personnel management system for the management of intelligence and intelligence-related civilian personnel throughout the DOD.

(2) The baseline document for the management of intelligence and electronic warfare (IEW) within the Army is the Army Intelligence Master Plan (AIMP). The AIMP is a requirements-based, threat and technology-driven, comprehensive developmental strategy for the future. This plan provides the basis for the development of the force structure and the fiscally constrained Battlefield Awareness and Command and Control Appendices of the AMP by the Deputy Chief of Staff for Programs (DCSPRO), DA.

b. Intelligence and Security Command (INSCOM). INSCOM, a major Army command, provides a single commander for those Army intelligence and electronic warfare (IEW) units that operate at EAC. INSCOM units, which are located both in CONUS and at many overseas locations, support requirements across the operational continuum. The

operations of INSCOM units include: planning and direction, collection, processing, production and dissemination of all-source, multidiscipline intelligence.

(1) In each major overseas area, a MI brigade or group provides multidisciplined IEW support to Army EAC and joint commanders in theater, reinforces MI units organic to operational and tactical commands at the echelons below corps, and satisfies taskings from national and departmental authorities for All-Source Intelligence, SIGINT, IMINT, TECHINT, MASINT, tactical HUMINT, and CI operations in response to strategic, operational, and tactical requirements. These activities are pursued through a multidisciplined force projection brigade concept.

(2) In CONUS, single and multidiscipline INSCOM MI brigade units and other organizations, some of them strategically deployable for contingencies, provide a wide range of collection capabilities as well as threat analysis, security, and OPSEC support to national and departmental agencies, contractors for sensitive projects and systems, and CONUS-based tactical consumers, including Forces Command units and the Army component of the USCENTCOM. INSCOM also plays a significant role in training at the NTC and with its Readiness Training (REDTRAIN) Program, and supports maintenance and development of intelligence skills in EAC and echelons below corps MI units. Finally, INSCOM supports the Training and Doctrine Command (TRADOC) in the EAC IEW combat-development process with doctrinal and force structure input, and is a MATDEV for certain specialized types of intelligence-related materiel.

c. U.S. Army National Ground Intelligence Center (NGIC). The National Ground Intelligence Center (NGIC), subordinate to INSCOM, acts as the Army's production center for the DOD Shared Production Program, and provides ground intelligence to U.S. Government agencies and decision makers. NGIC produces all-source scientific, technical, and general MI on foreign ground forces capabilities and systems in support of Army Title 10 requirements. This intelligence supports customers at all echelons, including Army and DOD force planners, wargamers, doctrinal developers, force modernizers, warfighters and theater joint intelligence centers with a wide range of futures-oriented threat assessments. The NGIC key products and production programs include order-of-battle and TOE for foreign ground forces that project out 20 years; detailed assessments of future threats tactical/operational capabilities; conflict scenarios; and forecast regions of future conflict that are of interest to U.S. force planners. The NGIC also provides threat documentation for Army R&D and procurement programs. These products and programs require collection; all-source analysis, production integration; and requirements management.

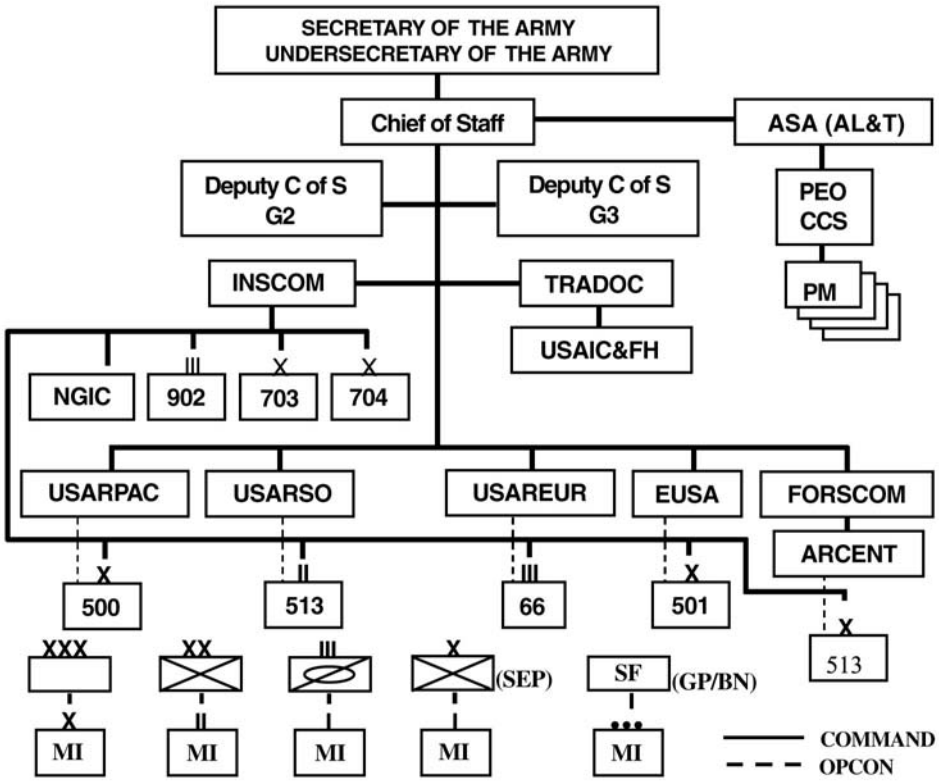

Figure 18–3. Army Intelligence Organization

18–10. General uses of intelligence

Intelligence must quickly reach, or be accessible, to leaders and their staffs who require it to plan, prepare, execute, and assess operations. Commanders, G2s/S2s, action officers, and managers must develop a broad understanding of what intelligence they need; what can be reasonably obtained; and how it can be beneficial in the development of their programs. They must clearly state, and if possible, prioritize their intelligence requirements to the appropriate organization. Along with the development of capability based forces and systems to meet needs in the 21st century, the following are a few examples of program areas in which intelligence can have a significant impact.

a. Organizational design and force structure. Force structure designers must consider the multiplicity of the threats and must also include non-threat factors such as the deployment capabilities and limitations of allied forces. There must also be balance between the greatest threat or enemy capability and the most imminent threat in the development of a force structure. The force planner must include intelligence participation in every phase of his or her planning and decision-making. To do this, he or she must be aware of the intelligence support available and how to task the system.

b. Materiel acquisition and force modernization. The product/project/program manager must consider technical developments in foreign countries, new foreign weapons systems and countermeasures developments and future developments, as well as terrain and weather considerations. This includes an assessment of how an adversary may react to the development of a new, friendly system. The product/project/program manager must have the latest intelligence available which could affect his or her product/project/program.

(1) The CBTDEV must also be aware of technical developments and must work closely with the MATDEV to ensure that a product/project/program will counter or surpass assessed threat capabilities. Both must be prepared to amend a product/project/program prior to its completion to counter a new threat capability. Intelligence requirements are not limited to hostile forces.

(2) Technological breakthroughs in friendly or neutral nations must also be factored into materiel acquisition planning. Managers of systems of breakthrough technology must use available intelligence support to protect characteristics of the developing system as a measure of OPSEC in the R&D arena.

(3) In addition to the intelligence needs stated, the product/project/program manager must also have high quality up-to-date intelligence on the foreign collection threat directed at the product/project/program. Threats from both foreign government and non-government sponsored collection make up this category. These threats must be identified, collected against, and neutralized by CI assets on behalf of the MATDEV. It is important to keep the Army materiel development community continually aware of and safe from technological loss from foreign directed and controlled collection services. This strengthens the Army's technical base against illegal technology transfer and markedly improves the Army's ability to maintain technological superiority.

(4) Other factors that should be taken into account in these processes include long-range planning and consideration of opponent's strengths, weaknesses, and vulnerabilities. As the rate of technological growth continues to increase and as the threat becomes harder to define, material developers lean toward generic threats defined in technical terms, thereby avoiding the potential trap of being locked to a specific adversary or region.

c. Doctrine and training systems development. Doctrine and training decisions must be based on sound intelligence. Foreign military capabilities and deployments are dynamic, and U.S. Army doctrine and training decisions must be equally dynamic. To be effective in battle, U.S. soldiers must know the enemy, including the enemy's doctrine, tactics, equipment, strengths, weaknesses, and vulnerabilities, and if possible, the enemy's intentions and expectations. Doctrine and training development and implementation must be closely tied to materiel systems management. Training to operate in a hostile information warfare environment anywhere in the world places a heavy emphasis on learning about a broad range of technical command and control capabilities. Future adversaries may employ combinations of hostile, friendly, and neutral command and control systems, as well as commercial products.

d. Information Operations (IO). Information Operations requires intelligence derived from very diverse sources of information, which are then integrated to develop an accurate description of adversaries and the information environment throughout the area of interest. Although IO is an operations function, intelligence is an integral part of IO planning, execution, and assessment. Intelligence support to IO is accomplished as part of the overall intelligence effort, using the all source, multi-disciplined intelligence approach. Intelligence staffs conduct analysis of the information environment as part of the overall Intelligence Preparation of the Battlefield (IPB) process. Successful IO requires the successfully application of IO to each IPB task. IPB should address the information environment (in addition to Land, Sea, Air, & Space) in order to gain an understanding of the friendly information environment and how the threat will operate in that environment. Such aspects as decision-making, the information infrastructure, and information tactics should be templated, with the endstate being the identification of threat vulnerabilities friendly forces can exploit with IO and identification of threat information capabilities against which friendly forces must defend.

(1) Information Operations are actions taken to affect potential adversaries, decision-making processes, and information and information systems while protecting one's own information systems. The goal of IO is to gain and maintain information superiority, a condition that allows commanders to seize and retain the initiative. IO involves a constant

effort to deny adversaries the ability to detect and respond to friendly operations while simultaneously retaining and enhancing friendly force freedom of action. The art of IO combines the effects of offensive and defensive IO to produce information superiority at decisive points. Offensive and defensive IO use complementary, reinforcing, and asymmetric effects to attack the enemy, influence adversaries and others, and protect friendly forces. The IO core capabilities are:

- Psychological operations
- Counterpropaganda
- Operations security
- Electronic warfare (electronic protection, electronic warfare support, electronic attack)
- Military deception
- Computer Network Operations (Computer Network Attack, Computer Network Defense, Computer Network Exploitation)

(2) Supporting IO capabilities are physical destruction, physical security, information assurance, counterpropoganda, counterdeception, and copunterintelligence.

(3) Related IO activities are Public Affairs (PA) and Civil Military Operations (CMO). PA and CMO create conditions that can contribute to information superiority. They sustain support of Army operations by American and international audiences, and maintain relations with the civilian populace in the AO. Their effectiveness is dependent upon their credibility.

(4) The 1st Information Operations Command (Land) (1st IO Cmd (Land)), formerly known as the Land Information Warfare Activity (LIWA), provides support to land component and Army commands to facilitate planning and execution of IO and enhances worldwide force protection by carrying out a proactive defense of Army information and information systems. As the chief integrator of IO into Army operations, The 1st IO Cmd (Land) provides IO-focused, multi-disciplined technical expertise to commanders' staffs. Additionally, 1st IO Cmd (Land) interfaces with other commands, service components, and national, defense department, and joint information centers. 1st IO Cmd (Land) personnel deploy worldwide, providing a unique knowledge base through multifaceted Field Support teams, Vulnerability Assessment Red and Blue teams, and SMEs in advanced systems and all source databases. The 1st IO Cmd (Land) is part of the Intelligence and Security Command (INSCOM) and receives operational taskings from the Army G–3.

e. Support to the tactical commander. Commanders use intelligence support to anticipate the battle, understand the battlespace, and influence the outcome of operations. The preeminent function of Army intelligence is to support the tactical commanders' decision-making process. The tactical commander drives the Army intelligence effort; the G2/S2 and the intelligence unit commander, are responsible for planning and directing, collecting, processing, analyzing and producing, and disseminating intelligence within the command. At corps, division, ACR, BCT/Stryker brigade, and special operations forces group/battalion, a MI unit is organic to the command, as shown in Figure 18–3. The MI unit commander plays an integral part in the intelligence mission through command and control of collection operations and by training and maintaining the organic and attached intelligence assets. Additional assets leverage national, theater, sister Service, and other intelligence systems to provide intelligence to the tactical commanders at all echelons. *FM 2–0, Intelligence*, the keystone intelligence manual, expands upon *FM 3–0, Operations*, and provides details on the doctrinal foundations for intelligence operations and the employment of tactical MI units.

f. Reserve Component (RC) support. The Reserve Components (RC) participate with Active Army MI units at all echelons and are involved in virtually every aspect of MI operations. In certain areas, USAR and National Guard MI capabilities including scientific & technical analysis, political-military estimates, and substantive basic intelligence, are equal to and even exceed those in the active force. This is attributable to the fact that many MI reservists, officer and enlisted, are professional civilian intelligence employees of the national intelligence and reconnaissance agencies, the Services' intelligence departments and agencies, federally funded research centers, colleges and universities, and other U.S. Government departments performing similar activities. Consequently, their exposure to, and involvement in, intelligence operations on a daily basis rival their uniformed counterparts. Additionally, the RC's contributions to filling the Army's linguist requirements are critical. The RC MI force is also in the process of increasing its capacity for timely response to intelligence production requirements. RC MI centers across the country are now connected to DOD telecommunications networks. This connectivity allows RC MI units and soldiers to receive tasks from Active Army intelligence organizations, perform research and analysis within DOD databases, and file production reports back to the Active Army organization-all within a relatively short time. RC MI is moving rapidly to a force architecture that will integrate it more fully into the operational capabilities of the Active Army, making the Reserve Components an increasingly valuable partner.

Section IV
Summary and References

18–11. Summary

Intelligence is vital to preserving the national security of the United States, and to the accomplishment of U.S. national

and military security objectives. The U.S. intelligence organizations and management will continue to transform at every level to meet the needs of U.S. policy officials and military leaders faced with the uncertain environment of the 21st century and the demands of a knowledge oriented era.

18–12. References

a. National Security Act of 1947.

b. Title 10, United States Code.

c. The Intelligence Organization Act of 1992, *Title VII, Public Law 102–496.*

d. The Intelligence Renewal and Reform Act of 1996, *Title VII, Section 805.*

e. The Intelligence Reform and Terrorism Prevention Act of 2004, *S. 2845/Public Law 108–458.*

f. Executive Order 12333, *United States Intelligence Activities*, 4 December 1981.

g. Executive Order 13356, *Strengthening the Sharing of Terrorism Information To Protect Americans*, 27 August 2004.

h. Homeland Security Presidential Directive-1, *Organization and Operation of the Homeland Security Council*, 29 October 2001.

i. National Security Presidential Directive-1, *Organization of the National Security Council System*, 13 February 2001.

j. President George W. Bush, *State of the Union Address*, 28 Jan 2003.

k. DOD Directive 5105.21, *Defense Intelligence Agency.*

l. DOD Directive 5105.56, *National Imagery and Mapping Agency (NIMA).*

m. DOD Directive 5137.1, *Assistant Secretary of Defense, Command, Control, Communications and Intelligence.*

n. Joint Publication 1–02, *DOD Dictionary of Military and Associated Terms*, June 1999.

o. Joint Publication 2–0, *Joint Doctrine for Intelligence Operations*, January 2000.

p. Joint Publication 2–01, *Joint Intelligence Support to Military Operations*, 20 Nov 1996.

q. Joint Publication 2–02, *National Intelligence Support to Joint Operations*, 28 Sep 1998.

r. Joint Publication 2–01.1, *Joint Tactics, Techniques and Procedures for Joint Intelligence Support to Targeting*, 9 Jan 2003.

s. Joint Publication 2–01.3, *Joint Tactics, Techniques and Procedures for Joint Intelligence Preparation of the Battlespace*, 24 May 2000.

t. Field Manual 1–02/MCRP 5–2A. *Operational Terms and Symbols* (Drag Draft), 21 Feb 2003.

u. Field Manual 2–0, *Intelligence*, 17 May 2004.

v. Field Manual 2–19.402, *STRYKER Brigade Combat Team Intelligence Operations*, 1 March 2003.

w. Field Manual 2–19.602 *Surveillance Troop*, 1 March 2003.

x. Field Manual 2–33.5/ST, *Intelligence Reach Operations*, 1 June 2001.

y. Field Manual 3–13, *Information Operations*, 28 Nov 2003

z. Field Manual 34–8–2, *Intelligence Officer's Handbook*, 1 May 1998.

aa. Field Manual 34–37, *Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations*, 15 Jan 1991.

b. Department of the Army, *Transformation Road Map.*

c. Department of the Army, *White Paper: Concepts for the Objective Force.*

d. TRADOC Pam 525–3–0, *Future Force: Operational and Organizational Concept (Draft).*

e. Army Regulation 38–10, *U.S. Army Intelligence Activities*, 1 July 1984.

f. Army Magazine, *Army Intelligence Provides the Knowledge Edge, April 2002.*

g. Director of Central Intelligence Directive 1/1, *The Authorities and Responsibilities of the Director of Central Intelligence as Head of the U.S. Intelligence Community, 19 November 1998.*

h. Director of Central Intelligence Directive 3/2, *Intelligence Community Policy and Planning Committees*, 28 July 1997.

i. Director of Central Intelligence Directive 3/3, *Community Management Staff*, 12 June 1995.

j. U.S. Commission on National Security/21st Century, *Volume VI–Intelligence Community*, 15 April 2001.