

Chapter 18

Intelligence

“We exist to support a transforming Army by fielding and sustaining the world’s premier Military Intelligence Organization.”

Lieutenant General Robert W. Noonan, Jr., 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, 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 streamlining of defense organizations associated with the SecDef’s “Bureaucracy to Battlefield” initiatives. 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) A plan to create a new 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 will be staffed by officials from each of those agencies, compile a “daily threat matrix,” and serve as the intelligence basis for most executive decisions. The center will report to the Director of Central Intelligence (DCI). The plan also creates a new executive assistant director under the FBI Director who will focus on the development of that agency’s intelligence analysis capability.

(4) The internal re-organizations of many of the existing fourteen 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.

(5) The SecDef’s proposal to create an Under Secretary of Defense for Intelligence to consolidate oversight of the DOD major intelligence agencies under one high-level official.

(6) 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 to the newly created combatant command: USNORTHCOM. Both ASD/HLD and

How the Army Runs

NORTHCOM will require intelligence support to adequately protect the CONUS and its contiguous waters from external threats and attacks.

(7) The establishment of USNORTHCOM as a Combatant Command, the conversion of Joint Forces Command to a functional Combatant Command and the combining of Space Command and Strategic Command into Strategic Command all will impact DOD intelligence support.

(8) The realignment of Army major commands and field operating agencies to include aligning Intelligence and Security Command (INSCOM) under the Deputy Chief of Staff, Intelligence/G2 and moving the U.S. Army Central Personnel Security Clearance Facility from U.S. Army Military Personnel Center to a subordinate command of INSCOM.

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 Board of Directors and established a National Counterintelligence Executive.

b. Army Transformation. Military Intelligence (MI) is an essential, important and integral element of Army Transformation. Accordingly, the Army MI challenge is to develop and portray a single, cohesive picture of its future, i.e., what and who Army MI is and must be, and decide on an appropriate avenue of approach, azimuth, or vector in order to support commanders at all echelons within the transformed force. This foundation builds from a vision and guiding set of principles for MI: quality people and leadership; focused analysis and synthesis; integrated in facilitating situational understanding; gaining information superiority; support to force protection; and the ability to leverage joint and national intelligence support. Each principle provides overarching guidance and direction Army MI soldiers and civilians need to accomplish MI's mission.

(1) The requirement to transform the Army is based upon the emerging security challenges of the 21st Century and the need to respond more rapidly and decisively across the full spectrum of operations, a requirement reinforced and mandated by the continuing Global War on Terrorism (GWOT). As the Army transitions to provide rapid, decisive, and sustained land power, MI requires a new approach toward conducting intelligence operations. Intelligence is currently focused on the collection, processing, analysis, and dissemination of information as either single or multidiscipline intelligence, focused principally on collection methods and capabilities. Within this stratified and hierarchical architectural framework, the ability to rapidly share critical, time-sensitive information is hindered. The commanders' need for a shared, up-to-the minute understanding of the battlespace, coupled with the explosion of the availability of information, mandate a shift toward creating a collaborative, distributed, and integrated information environment as illustrated in Figure 18–1.

(2) Implementing this vision will require the Army to fully integrate Intelligence, Surveillance, and Reconnaissance (ISR) to help shape the battlespace from the strategic to the tactical levels; to leverage national agencies and sister services to better support the warfighter; and focus on core intelligence competencies. Changes in Army intelligence that support this vision include the use of intelligence support elements at all levels and changes to the intelligence force structure that better support a strategically deployable Army. MI, as part of the whole integrated ISR construct, is an integral element of the Army's Transformation goals and objectives. Moreover, Army ISR and Joint ISR must also become fused within a symbiotic and seamless intelligence network.

(3) As the Army transforms itself to provide rapid decisive, and sustained land combat power, MI must leverage appropriate IT and adapt or adopt innovative concepts in order to achieve interoperable, C4ISR architectures and capabilities that include a fused common operational picture that can be scaled or tailored to meet command level requirements. The need for a shared, up-to-the-minute, critical, time-sensitive understanding of the battle space, coupled with the concurrent explosion of data and information, mandate a collaborative, distributed, fused, and integrated information environment as illustrated in Figure 18–1. The development of Distributed Common Ground System (DCGS) architecture, the Army's DCGS–Army (DCGS–A), and the Global Information Grid (GIG) will facilitate interoperability and the development and dissemination of a common operating picture supporting the commanders' information needs.

(4) Implementation of this vision requires the Army to better integrate C4ISR from MI as well as non-MI sources to help depict the battle space from the strategic through the operational to the tactical levels. It also means that Army Intelligence must work with and leverage national agencies (e.g., CIA, National Imagery and Mapping Agency (NIMA) (see para 18–7e), National Reconnaissance Office (NRO) (see para 18–7f), NSA, et al), its sister Services as well as open sources to improve the fidelity of its service and better support the war fighter. Finally, it means that Army Intelligence must identify, address, and focus the major intelligence disciplines: Imagery Intelligence (IMINT), Signals

Intelligence (SIGINT), HUMINT, Measurement and Signature Intelligence (MASINT) (see para 18–4d(5)), Technical Intelligence (TECHINT), and Counterintelligence. Thus, to more adequately and better support this changed vision, Army Intelligence must design, employ, and use intelligence elements at all echelons, remodel its force structure, streamline and revamp its systems and accelerate its processes. Transformation will profoundly affect what, when, how, how much and to whom intelligence is provided to meet the critical requirements of a strategically deployable Army.

c. Need for intelligence. Timely, relevant, accurate, predictive and useable intelligence addressing the activities, capabilities, plans, and intentions of foreign leaders and their governments is needed to develop sound national security and foreign policies. It is critical to international negotiations and to the development and monitoring of international agreements. Likewise, intelligence is also critical to the successful conduct of campaigns and battles.

(1) Within the DOD, planners and managers responsible for the development of weapons systems and force structure need accurate, long-range projections of the combat capabilities and technologies of foreign powers and entities as the basis for their recommendations and decisions. Similarly, the ability of U.S. forces to deter or defend against attack requires detailed knowledge of the current deployment and capabilities of potential adversaries and their future plans.

(2) Full Spectrum Operations demand that intelligence provide a commander with information and knowledge to fully visualize the battlespace for the effective employment of his or her forces. It is a key component of battle command and provides the enemy and environment portions of the common operating picture. Finally, as our focus shifts to strategic responsiveness, the potential for rapid deployments into small scale contingencies requires detailed information on the cultural, historical, economical, technological, and political factors of the deployment area. The increased resolution of intelligence required to support this level of strategic responsiveness required the extension of the "intelligence reach." The amount and fidelity of intelligence necessary to maintain strategic responsiveness and to counter asymmetric threats requires a tremendous amount of information to accurately depict the battlespace concurrently at the strategic, operational and tactical levels from strategic distances.

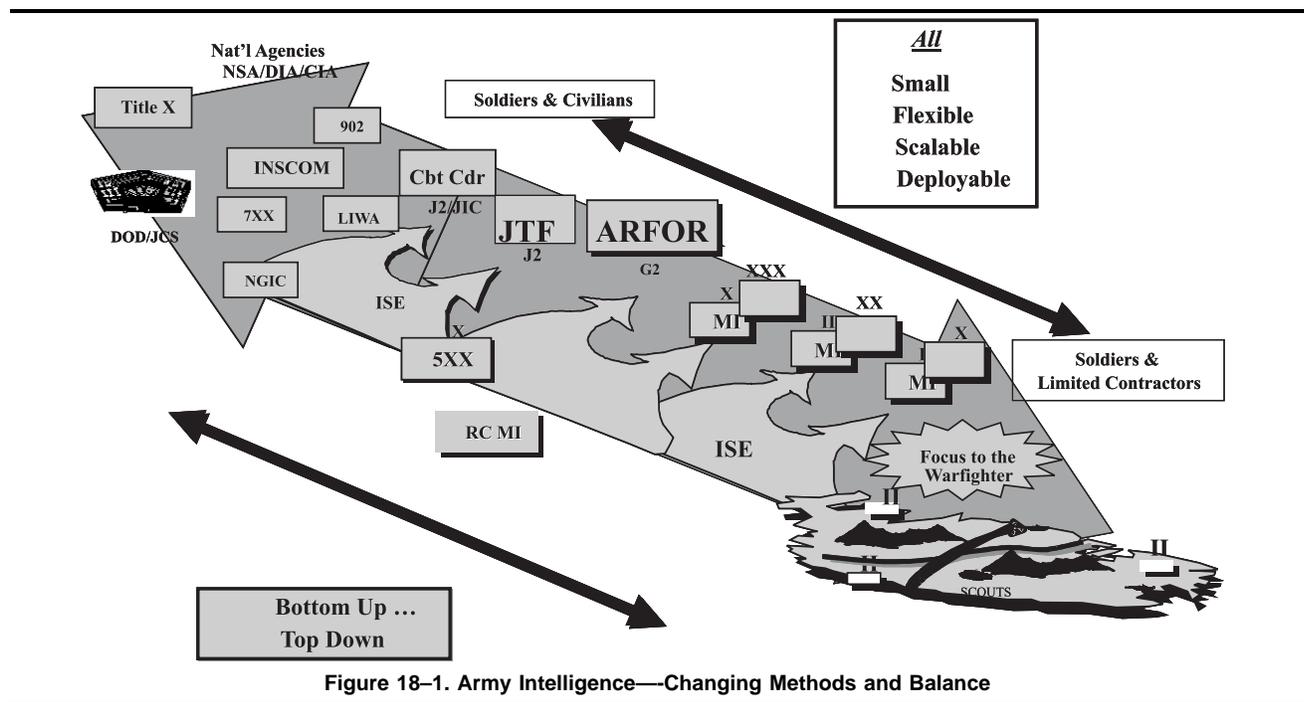


Figure 18–1. Army Intelligence—Changing Methods and Balance

18–4. Intelligence products

a. Categories of intelligence. 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.

How the Army Runs

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 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 Central Intelligence (DCI). Various finished all-source intelligence products of the CIA which are approved by the DCI 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. Where the TTIC will fall in this hierarchy is not yet clear, although the current DCI Counterterrorist Center around which the TTIC is likely to be built is considered a producer of national intelligence.

(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.

(1) Strategic intelligence is intelligence required for the formulation of strategy, policy, and military plans and operations at theater level and above. Strategic intelligence—

- Concentrates on the national political, economic, and military considerations of a state or entity
- Identifies a nation's ability to support U.S. Forces and operations (for example, ports and transportation infrastructure)
- Predicts other nations and entities responses to U.S. operations.

(2) Operational intelligence is the intelligence required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or areas of operations. Intelligence at this level serves as a bridge between strategic and tactical levels. Operational intelligence—

- Supports friendly campaigns and operations by predicting the enemy's campaign plans, identifying their military centers of gravity, lines of communication, decisive points, pivots of maneuver, and other components necessary for campaign design.
- Focuses primarily on the intelligence needs of commanders from theater through corps and task force.

(3) Tactical intelligence is intelligence required for planning and conducting tactical operations as an integral part of battle command. Intelligence provides the tactical commander with the information and knowledge that is needed to reach situational understanding and employ allocated forces in order to meet assigned objectives. Tactical intelligence is distinguished from other levels by its perishability and ability to quickly influence the outcome of the commander's mission.

c. Types of intelligence.

(1) Basic intelligence is encyclopedic type information, which is not time-sensitive and describes all aspects of a nation - physical, social, economic, political, geographical, cultural, and military which is used as a base for intelligence products in support of planning, policymaking, and military operations.

(2) Current intelligence includes all types and forms of perishable, time-sensitive, information of immediate value and interest to specific consumers. It may be disseminated without complete evaluation, interpretation, analyses, or integration.

(3) Estimative intelligence is that intelligence which projects forward in time and is predictive in nature.

(4) Crisis intelligence is comprised of specific types and forms of very perishable, time-sensitive information of immediate value, and usually intense interest at the international, national, and theater levels. It is narrowly focused on a precise area, individual(s), or event, which is closely monitored until termination or closure. Usually after 30 days, this type of intelligence becomes current intelligence and eventually basic intelligence.

(5) Combat information is data obtained through various MI and non-MI collection sources and methods, which are passed rapidly to the user without benefit of analysis, interpretation, or integration. A sensor-to-shooter system transmitting highly perishable, potential targeting data is an example of this data. Tactical commanders often must make decisions based on the immediate access to and availability of combat information. Crisis intelligence and combat information often benefit from the data developed for basic and current intelligence and associated databases.

(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.

(1) Intelligence is 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.

(2) HUMINT is a category of intelligence derived from information collected and provided by human sources as opposed to technical sources. HUMINT includes such overt activities as attaché duty, liaison functions, interrogation of prisoners of war, debriefing of displaced persons/refugees/evacuees/and line crossers, solicitation of information from indigenous persons, document exploitation, and controlled collection operations such as clandestine operations. A HUMINT collector is a person, who by training is tasked with and engages in the collection of information from individuals for the purpose of answering specific intelligence requirements.

(3) Imagery intelligence (IMINT) is intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. The resulting imagery may be analyzed in either hard-copy (photographic) or soft-copy (electronic display) format for distribution.

(4) Signals intelligence (SIGINT) is intelligence obtained through the exploitation and analysis of electromagnetic emissions and includes communications intelligence, electronic intelligence, and foreign instrumentation SIGINT.

(5) MASINT is technically-derived platform-independent intelligence (excluding traditional imagery and SIGINT) which when collected, processed, and analyzed, results in intelligence that detects, tracks, identifies, or describes the signatures (distinctive characteristics) of fixed or dynamic target sources. MASINT includes the advanced processing and exploitation of data derived from IMINT and SIGINT collection sources. MASINT sensors include, but are not limited to, radar, optical, infrared, acoustic, nuclear radiation detection, spectroradiometric, and seismic systems as well as gas, liquid, and solid material sampling systems.

(6) TECHINT is a multidiscipline function that supports commanders by either identifying or countering an enemy's momentary technological advantage, or by maintaining a technological advantage. The two parts of TECHINT are battlefield TECHINT and scientific TECHINT. TECHINT is also derived from the exploitation of foreign material produced for strategic, operational, and tactical commanders.

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 National 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 14 intelligence agencies, including those in the Departments of Defense, Homeland Security, Justice, Treasury, Energy, and State, and the CIA. To reach its goals, the U.S. IC is directed and organized as shown in Figure 18–2.

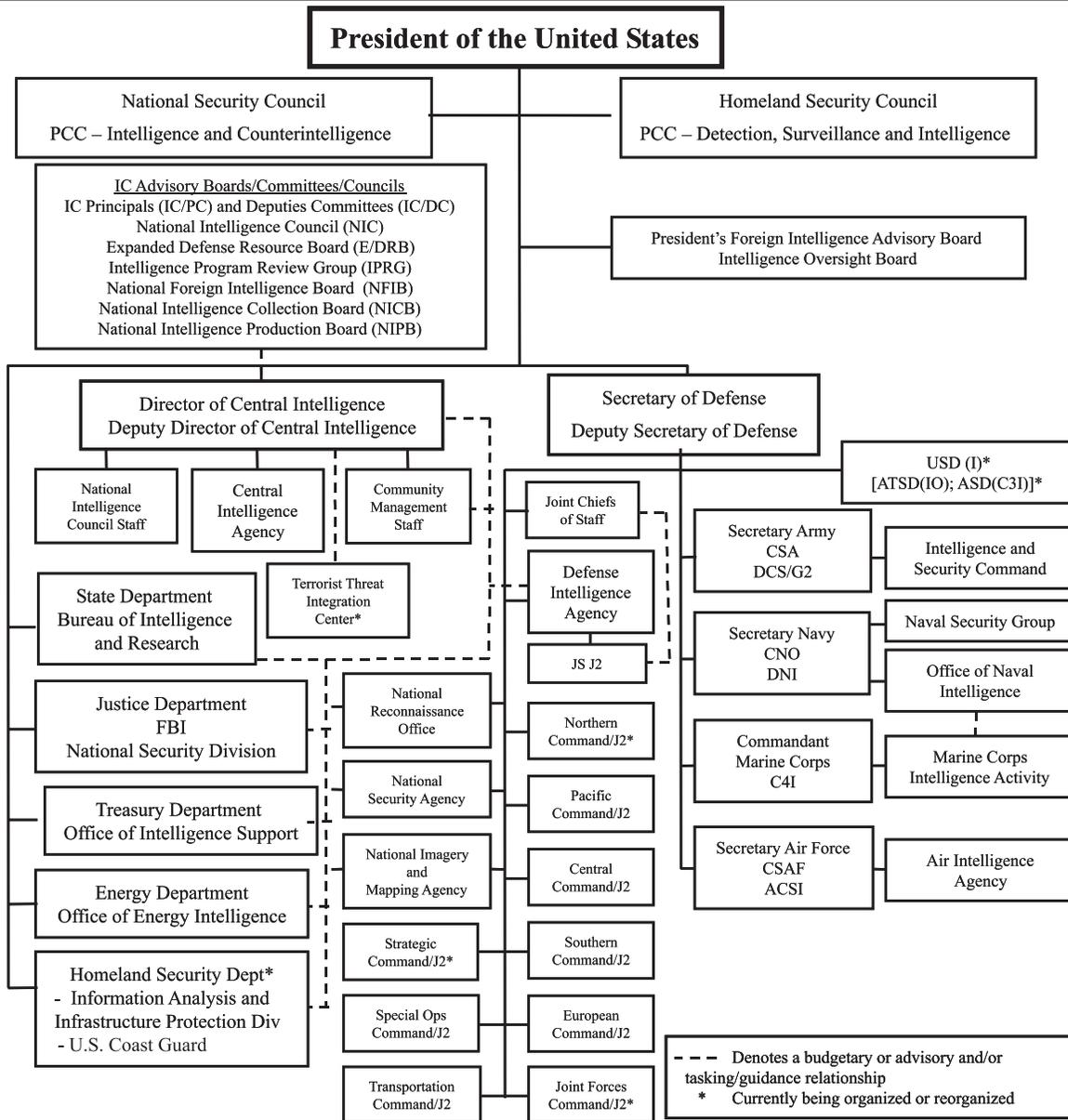


Figure 18-2. Organization of the National Intelligence System

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 the Office of Homeland Security (now transitioning to the 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 DCI, 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. The Director of Central Intelligence (DCI). The DCI is concurrently Director, CIA, and is directly responsible to the President, the Homeland Security Council and the NSC. The DCI is the primary adviser to the President and other members of the NSC/HSC on national foreign intelligence and is the intelligence system's principal spokesman to Congress. The DCI develops objectives and prepares guidance for the IC to enhance its capabilities for responding to expected future needs for foreign national intelligence, formulates policies concerning intelligence arrangements with foreign governments, and coordinates intelligence arrangements between agencies of the IC and the intelligence or internal security services of foreign governments. The DCI is responsible for the development, presentation, and justification of the National Foreign Intelligence Program (NFIP) budget. A complete list of DCI responsibilities is contained in EO 12333.

(1) Other senior officials are responsible for contributing, within their areas of capability, to the national foreign intelligence collection effort and for cooperating with other IC members to achieve efficiency and provide mutual assistance. In addition, they are responsible for management of the collection of departmental intelligence.

(2) Pursuant to EO 12333, the DCI establishes boards, councils, committees, or groups as required for the purpose of obtaining advice from within the IC. The advisory boards the DCI chairs are the National Foreign Intelligence Board, the Intelligence Community Principals Committee and the Expanded DRB (co-chair with DepSecDef).

e. DCI Subordinate Agencies and Activities.

(1) *The Community Management Staff (CMS).* The CMS is an independent element and its head is the Deputy Director of Central Intelligence/Community Management (DDCI/CM). The DDCI/CM serves as the DCI's chief advisor on IC policy, planning, resource, and management issues and is assisted by the Assistant Director of Central Intelligence and primarily by the Executive Director for Intelligence Community Affairs (EXDIR/ICA). The DDCI/CM directs operations of the CMS including the overall management of the NFIP and IC personnel and resources. The DDCI/CM also ensures the effective collection of national intelligence through the Assistant Director of Central Intelligence (ADCI) for Collection and conducts oversight of intelligence analysis and production by IC component agencies through the ADCI for Analysis and Production. The CMS is charged with developing, coordinating, and executing the DCI's community responsibilities for resource management; program assessment and evaluation of policies; and collection requirements management. It also performs other functions and duties as determined by the DCI, Federal statutes, or executive action.

(2) *The National Intelligence Council (NIC).* The Chairman of the NIC, who is also the ADCI/Analysis & Production, is responsible for intelligence analysis and production to include: evaluating community-wide production of intelligence; assessing the analytical capabilities of the IC community; developing DCI 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 DCI 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 DCI 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 DCI'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 our senior consumers.

(3) *ADCI/Collection Staff.* The Staff assists the ADCI/Collection in the efficient and effective collection of national intelligence.

f. IC Committees and Boards.

(1) *Intelligence Community Principals and Deputies Committee (IC/PC & IC/DC).* Chaired by the DCI, the IC/PC serves as the senior advisory board to the DCI on intelligence planning, needs management and evaluation, and decisions affecting NFIP programs. The IC/PC is the principal forum through which major policy issues impacting the IC are addressed. Permanent IC/PC members include the DCI; DDCI; VCJCS; Director, NSA; Director, DIA; Assistant

How the Army Runs

Secretary of State for INR; Director, NRO; Director, NIMA; Chairman, NIC; Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD (C3I) likely changing to or in addition to USD (I)); and DDCI/CM. Similarly, the IC Deputies Committee (IC/DC) provides another venue for senior-level coordination and addresses major policy issues affecting the IC. It is chaired by the DDCI (or DDCI/CM in the DDCI's absence) 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 DCI chairs the NFIB and the DDCI serves as the Vice Chairman. The NFIB is responsible for approving all 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 PPBS to deliberate on major issues involving all DOD NFIP 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 DCI and several IC officials to make recommendations to the DCI and DepSecDef 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 (NFIP, JMIP, TIARA) by reviewing issues, analyzing priorities, and examining funding alternatives. The EXDIR/ICA Chairs the IPRG and it is supported by the CMS staff that serves 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 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. 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.

g. *Central Intelligence Agency (CIA)*. The CIA is an independent agency, responsible to the President through the DCI, and accountable to the American people through the intelligence oversight committees of the Congress. The CIA's mission is to support the President, the NSC/HSC, and all officials who make and execute national security policy by: providing accurate, comprehensive, and timely foreign intelligence on national security topics, and by conducting CI activities, special activities, and other functions related to foreign intelligence and national security, as directed by the President. The Executive Director (EXDIR) of the CIA (appointed by the DCI) is the Agency's Chief Operating Officer. The EXDIR manages the CIA directorates (Administration, Intelligence, Science and Technology, and Operations) on a daily basis by formulating and implementing policies and programs affecting the Agency.

(1) To accomplish this mission, the CIA works closely with the other organizations in the IC to ensure that the intelligence consumer-whether a Washington policymaker or a battlefield commander- receives the best intelligence possible. As a separate agency, the CIA serves as an independent source of analysis on topics of concern to these consumers.

(2) The CIA collects foreign intelligence information through a variety of clandestine and overt means. The Agency also engages in research, development, and deployment of high-leverage technology for intelligence purposes and, in support of the DCI's role as the President's principal intelligence advisor, performs and reports all-source analysis on the full range of topics that affect national security. The CIA is organized along functional lines to carry out these activities and to provide the flexible, responsive support necessary for its worldwide mission.

(3) Throughout its history, but especially as new global realities have reordered the national security agenda, the CIA has emphasized 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.

(4) Also, the CIA contributes to the effectiveness of the overall IC by managing services of common concern in imagery analysis and open source collection, and by participating in strategic partnerships with other intelligence agencies in the areas of R&D and technical collection. Finally, the CIA takes an active part in community analytical efforts and coordinates its analytical production schedule with appropriate agencies to ensure efficient coverage of key topics.

(5) The Office of Military Affairs (OMA) was established in the CIA to support military plans and operations. 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.

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 CI 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 their framework, which deal with 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 DCI for development of the NFIP as part of the Federal budget. Within the DOD, the Assistant Secretary of Defense (C3I) is the DOD focal point for intelligence management (this may transition to the Under Secretary of Defense (Intelligence) (USD(I)) when that office is fully functional).

a. National Foreign Intelligence Program (NFIP). The NFIP provides funds for the bulk of all national-level intelligence, CI, and reconnaissance activities of the 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 Imagery and Mapping Agency Program (NIMAP), 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 who is subordinate to the Deputy Assistant Secretary of Defense (Security and Information Operations), under the ASD(C3I) (note: this may migrate to the new USD(I)). The PM for the NIMAP is the Director, NIMA and the 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 war-fighters, 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. Combatant Commanders formally participate in the Capabilities Programming and Budgeting System and influence the DOD PPBS process for intelligence resources through their Combatant Commander's IPL. Through the Command Intelligence Architecture Program, Combatant 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 PPBS through the PEGs and membership on the PPBS Council of Colonels, Planning, Programming, and Budget Committee, and Senior Resource Group.

(2) The Army participates directly in three of the programs of the NFIP: 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 DCI.

(3) In addition to the NFIP 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 NFIP. TIARA is an aggregation of portions of the DOD budget that provide tactical intelligence and related support to military operations. In contrast to the NFIP, 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 5148.12, dated 20 July 1989, established

How the Army Runs

the position and assigned its responsibilities. 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. Some or all of these functions may be transferred or consolidated under the proposed USD (I).

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

18–7. Intelligence cycle

The intelligence cycle consists of planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; and evaluation and feedback. Intelligence collection and production management guide the bulk of the process and the expenditures of resources.

a. Collection 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 collection management activities are referred to as ISR operations

(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 CIA. 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 DCI’s CMS for collection tasking.

(2) All collection operations are conducted in response to validated requirements for the production of finished intelligence. The ADCI/Collection is responsible for the efficient and effective collection of national intelligence by IC component agencies. CMS 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. 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. 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 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 DCI and is exercised through the CIA’s ADCI/Analysis and Production which establishes schedules and priorities for national intelligence production conducted by the IC. Internal to the CIA, the Directorate of Intelligence (DI), is responsible for the production and dissemination of all-source intelligence. The DI is the analytical branch of the CIA. Further, the directorate retains the resources and capability to produce intelligence assessments that are not coordinated with other elements of the IC.

(1) Heading the DI is the Deputy Director for Intelligence (DDI). The DDI is responsible for the timeliness, accuracy, and relevance of intelligence analysis provided to national security policymakers and other intelligence consumers. The DDI oversees three regional offices, an office that addresses transnational issues, and another that provides information services and support.

(2) No single intelligence product format 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.

(3) The most prestigious intelligence product is the President’s Daily Brief (PDB), which is prepared by the DI for DCI approval and forwarded to the President. The PDB is the DCI’s principal daily report to the President. Other national reports include the Senior Executive Intelligence Brief (SEIB). The SEIB is produced 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 DI 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).

(4) 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 Combatant Commands and Services.

(5) 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 Combatant Commands. 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 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 15 March 1991 the SecDef approved a plan for restructuring defense intelligence. Among other changes, the DOD reorganization of defense intelligence resulted in the consolidation of existing unified and major or joint Combatant Commands and component intelligence processing, analysis, and production activities into joint intelligence centers (JICs) and joint analysis centers (JACs), and consolidation of intelligence commands, agencies, and elements into a single intelligence command/agency within each Service.

b. Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (OASD (C3I)). Currently, the ASD (C3I) has as a principal duty the overall supervision of C3I affairs of the DOD. The ASD (C3I) is the DOD principal staff assistant for the development, oversight, and integration of DOD policies and programs relating to the strategy of information superiority for the DOD. He or she 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. A recent proposal by the Sec Def is designed to separate Intelligence from ASD (C3I) and create a new Office of the Undersecretary of Defense for Intelligence to perform oversight of all DOD intelligence activities. When implemented, the ASD (C3I) would likely change to ASD (C3) and not be involved in intelligence affairs.

c. 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, Combatant 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 Combatant Commanders and U.S. Forces Korea, NATO, and Supreme Headquarters Allied Powers Europe (SHAPE), 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

How the Army Runs

Energy/State/ Treasury/ and Commerce, and the NIMA. 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 Combatant Commands are represented by DIA's Directorate for Intelligence which functions as the J2, JS. The MIB serves as the senior "Board of Governors" for the intelligence organization in DOD and advises the SecDef, CJCS, Military Service Chiefs, Combatant Commanders, and defense agencies on matters pertaining to MI. The Director DIA seeks consensus across the IC through the MIB process.

d. 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 NFIP. 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. NSA's SIGINT activities are extremely sensitive and are normally handled in special channels available to specifically designated personnel in direct support of military commanders, operations, and national foreign intelligence collection requirements. The NSA's SIGINT collection, processing, and dissemination activities involve both positive and CI information and are in direct support of military commanders and military 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 NFIP, 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.

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

(1) The NIMA 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. NIMA 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. NIMA 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 NIMA 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 NIMA establishes the architectures for imagery tasking, collection, processing, exploitation, and dissemination. NIMA 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 NIMA. NIMA also supports and conducts R&D activities related to this imagery function.

f. 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.

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.

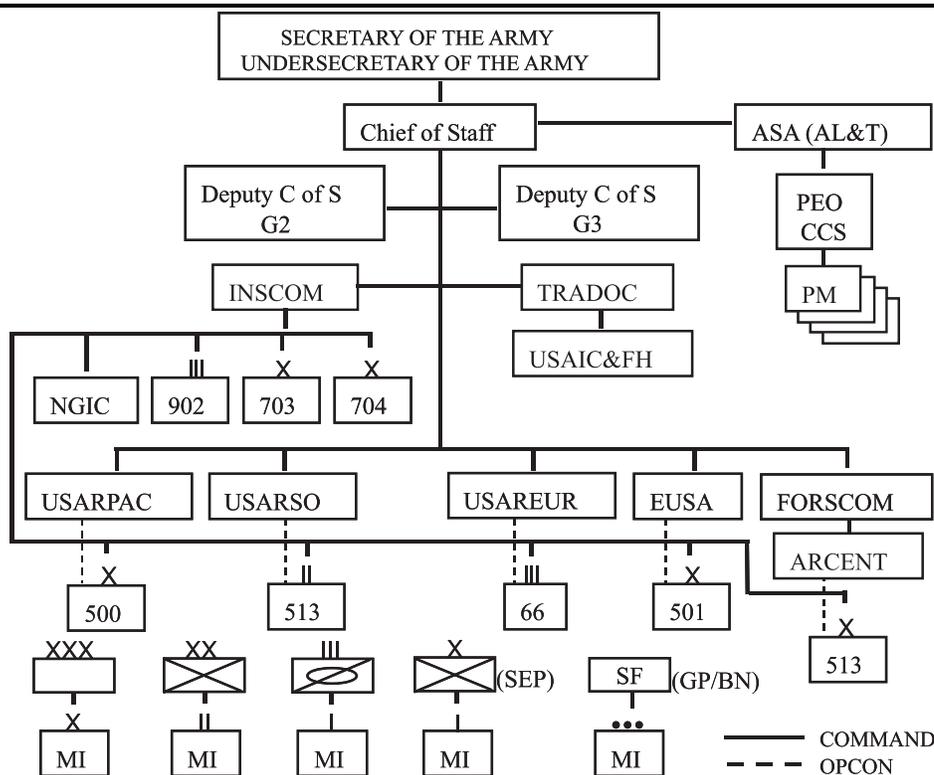


Figure 18-3. Army Intelligence Organization

a. *Deputy Chief of Staff, G-2.* The G-2 is the senior intelligence officer in 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 the 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 Army POM building 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 an excepted 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 Transformation Campaign Plan (AI TCP). The AI TCP is a requirements-based, threat and technology-driven, comprehensive developmental strategy for the future. It is not constrained by fiscal or force structure resources. This plan provides the basis for the development of the force structure and the fiscally constrained

How the Army Runs

Information Superiority Annex of the AMP by the Deputy Chief of Staff for Programs (DCSPRO), DA. The Information Superiority Annex of the AMP implements the Army's force modernization principles and is the key planning document in providing long-term continuity of effort within the IEW functional area.

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 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 USCENCOM. 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.

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. He or she must make the intelligence systems aware of his or her intelligence needs.

(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 his or her 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, materiel 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 successful 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 elements of IO are—

- Operations security
- Psychological operations
- Counterpropaganda
- Military deception
- Counter deception
- Electronic warfare (electronic protection, electronic warfare support, electronic attack)
- Computer Network Attack
- Computer Network Defense
- Physical destruction
- Information assurance
- Physical security
- Counterintelligence

(2) 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.

(3) 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)

How the Army Runs

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 G3.

e. Support to the tactical commander. Commanders use IEW 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 commander's 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, separate 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 34–1, Intelligence and Electronic Warfare Operations, the keystone intelligence manual, expands upon FM 3–0, Operations, and provides details on the doctrinal foundations for IEW 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, substantive basic intelligence, are equal to and even exceeds, 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 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.* Executive Order 12333, *United States Intelligence Activities*, 4 December 1981.
- f.* Homeland Security Presidential Directive-1, *Organization and Operation of the Homeland Security Council*, 29 October 2001.
- g.* National Security Presidential Directive-1, *Organization of the National Security Council System*, 13 February 2001.
- h.* President George W. Bush, *State of the Union Address*, 28 Jan 2003.
- i.* DOD Directive 5105.21, *Defense Intelligence Agency*.
- j.* DOD Directive 5105.56, *National Imagery and Mapping Agency (NIMA)*.
- k.* DOD Directive 5137.1, *Assistant Secretary of Defense, Command, Control, Communications and Intelligence*.
- l.* Joint Publication 1–02, *DOD Dictionary of Military and Associated Terms*.
- m.* Joint Publication 2–02, *National Intelligence Support to Joint Operations*.
- n.* Joint Publication 2–01.3, *Joint Tactics, Techniques and Procedures for Joint Intelligence Preparation of the Battlespace*.
- o.* Field Manual 34–1, *Intelligence and Electronic Warfare Operations*.
- p.* Field Manual 34–8–2, *Intelligence Officer's Handbook*.

- q. Field Manual 34–37, *Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations*.
- r. Department of the Army, *Transformation Road Map*.
- s. Department of the Army, White Paper: *Concepts for the Objective Force*.
- t. TRADOC Pam 525–3–0, *Objective Force: Operational and Organizational Concept* (Draft).
- u. Army Regulation 38–10, *U.S. Army Intelligence Activities*.
- v. Army Magazine, *Army Intelligence Provides the Knowledge Edge*, April 2002.
- w. U.S. Army Intelligence Center, *Army Intelligence Transformation Campaign Plan*.
- x. 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.
- y. Director of Central Intelligence Directive 3/2, *Intelligence Community Policy and Planning Committees*, 28 July 1997.
- z. Director of Central Intelligence Directive 3/3, *Community Management Staff*, 12 June 1995.
- aa. U.S. Commission on National Security/21st Century, *Volume VI–Intelligence Community*, 15 April 2001.