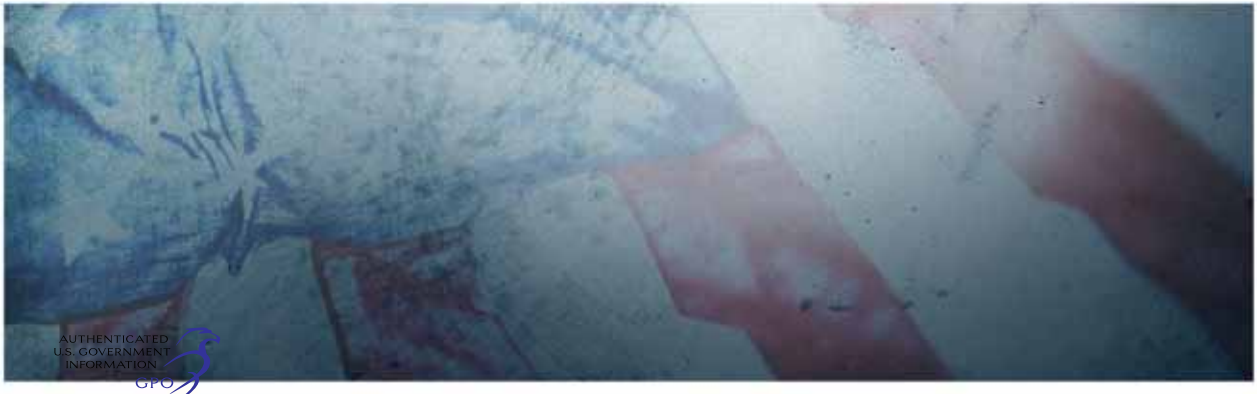
U.S. NATIONAL INTELLIGENCE

AN OVERVIEW 2011




OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA
U.S. DEPARTMENT OF HOMELAND SECURITY
THE DEPARTMENT OF THE TREASURY
1789
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY

Table of Contents

TAB 7: CAREERS IN THE INTELLIGENCE COMMUNITY

TAB 8: REFERENCES

Intelligence Overview

In the early morning hours of May 2, 2011, a U.S. military raid on an al-Qa'ida compound in Abbottabad, Pakistan, killed America's most-wanted terrorist, Usama Bin Ladin.

U.S. agencies and partners across the Intelligence Community had been collecting intelligence about the compound since it was discovered in August 2010. The raid on the compound, authorized by the President on April 29, was conducted by a small team of special operations soldiers. The raid was designed to minimize collateral damage and risk to non-combatants in the compound and Pakistani civilians in the area.

The death of Bin Ladin, al-Qa'ida's founder and only amir, or commander, in its 22-year history, marks the single greatest victory in the U.S.-led campaign to disrupt, dismantle, and eventually dissolve al-Qa'ida.

THE OPERATION THAT KILLED BIN LADIN

Courtesy of CIA

Defining and Using Intelligence

According to the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the terms "National Intelligence" and "intelligence related to national security" refer to all intelligence, regardless of the source from which it is derived and including information gathered within or outside the United States,

- that pertains, as determined to be consistent with any guidance issued by the President, to more than one U.S. Government agency; and
- that involves:
  - Threats to the U.S., its people, property, or interests;
  - The development, proliferation, or use of weapons of mass destruction; or
  - Any other matter bearing on U.S. national homeland security.

The U.S. Government uses intelligence to improve and more fully understand the consequences of its national security decisions. Intelligence informs policy decisions, military actions, international negotiations, and interactions with working-level contacts in foreign countries. In some circumstances, intelligence can also aid the efforts of homeland security providers and first responders.

What is the Intelligence Community?

The Intelligence Community (IC) is a group of Executive Branch agencies and organizations that work separately and together to engage in intelligence activities that are necessary for the conduct of foreign relations and the protection of the national security of the United States.

These activities include:

- Collection of information needed by the President, the National Security Council,

the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and fulfillment of their responsibilities.

- Production and dissemination of intelligence.
- Collection of information concerning intelligence activities directed against the United States, international terrorist and narcotics activities, and other such hostile activities carried out by foreign powers, organizations, persons, and their agents.
- The conduct of actions to protect against hostile activities directed against the United States.
- Performance of special activities.
- Performance of administrative and support activities within the United States and abroad that are necessary for the performance of various other intelligence activities.
- Performance of such other intelligence activities as the President may direct from time to time.

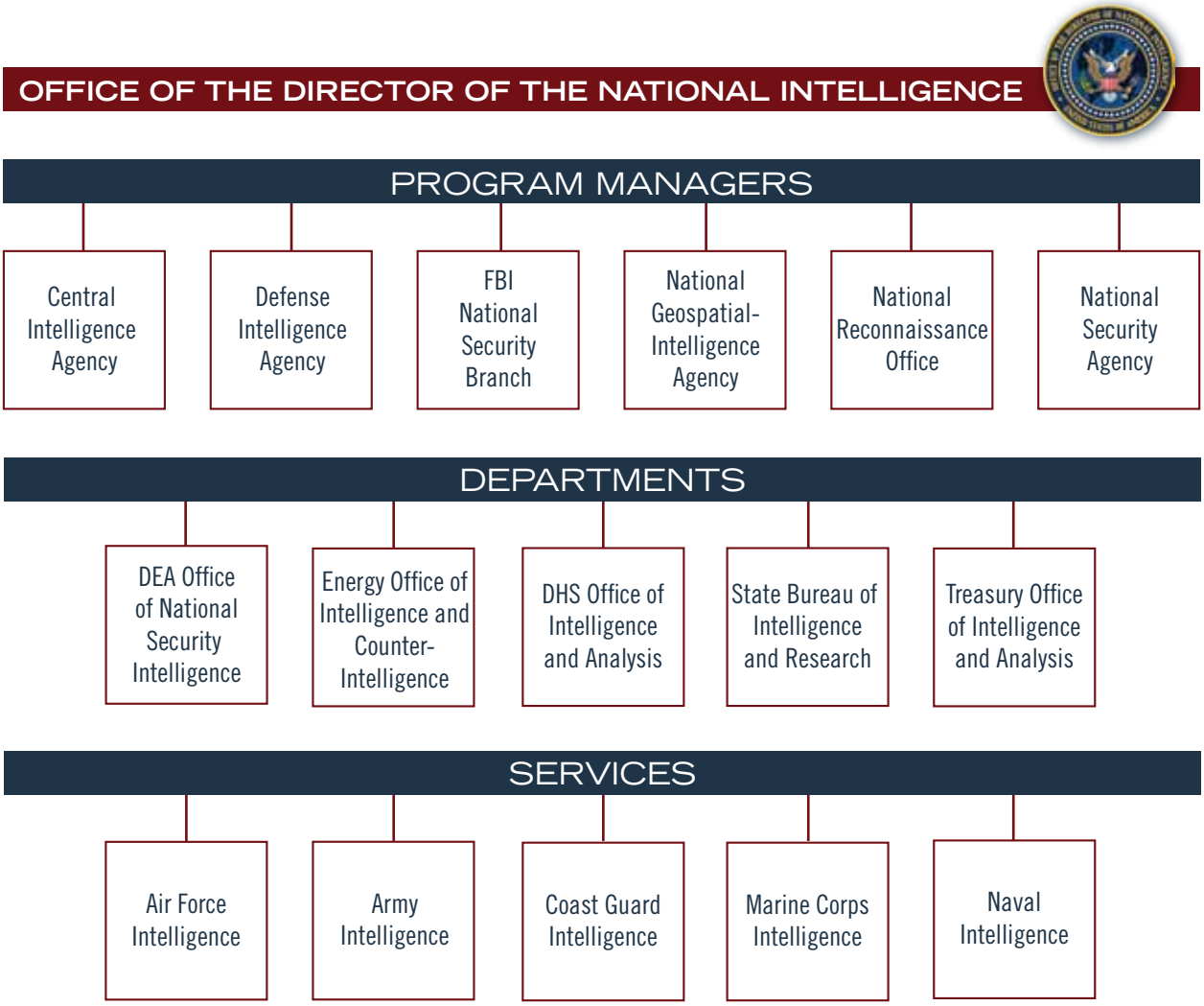
The IC is led by the Director of National Intelligence (DNI), who is the head of the Office of the Director of National Intelligence (ODNI) and whose duty is to coordinate the other 16 IC components based on intelligence consumers' needs. The other members of the IC are divided into three groups: Program Managers, Departments, and Service components.

- Program Managers advise and assist the ODNI in identifying collection requirements, developing budgets, managing finances, and evaluating the IC's performance.
- Departments are IC components embedded within Government departments (other than the Department of Defense [DoD]). These components focus on serving their parent department's intelligence needs.
- All intelligence personnel in the armed forces are members of the Service IC components, which primarily support their own Service's information needs. Each Service has at least one major intelligence organization as well as intelligence officers integrated throughout its structure.

Intelligence Integration

The core mission of ODNI is to lead the Intelligence Community in intelligence integration. Basically, intelligence integration means synchronizing collection, analysis, and counterintelligence so that they are fused—effectively operating as one team.

Unifying Intelligence Strategies (UIS) are the central critical plans for achieving intelligence integration. They cover our strategies by geography and topic. They foster an environment that encourages, enables, and recognizes integration at all levels of the IC.



National Intelligence Managers (NIMs) and their teams create UIS in line with the IC prioritized requirements. They are thus charged with leading integration across the IC by topic and region.

The Six Steps in the Intelligence Cycle

The Intelligence Cycle is the process of developing raw information into finished intelligence for use by policymakers, military commanders, and other consumers in decisionmaking. This six-step cyclical process is highly dynamic, continuous, and never-ending . The sixth step, evaluation (which includes soliciting feedback from users) is conducted for each of the other five steps individually and for the Intelligence Cycle as a whole.

The six steps that constitute the Intelligence Cycle are as follows:

PLANNING AND DIRECTION: Establish the consumer's intelligence requirements and plan intelligence activities accordingly.

The planning and direction step sets the stage for the Intelligence Cycle. It is the springboard from which all Intelligence Cycle activities are launched. Oftentimes, the direction part of the step precedes the planning part. Generally, in such cases, the consumer has a requirement for a specific product. That product may be a full report, a graphic image, or raw information that is collected, processed, and disseminated, but skips the analysis and production step. Given the customer's requirement, the intelligence organization tasked with generating the product will then plan its Intelligence Cycle activities.

COLLECTION: Gather the raw data required to produce the finished product.

Data collection is performed to gather raw data related to the five basic intelligence sources (Geospatial Intelligence [GEOINT], Human Intelligence [HUMINT], Measurement and Signature Intelligence [MASINT], Open-Source Intelligence [OSINT], and Signals Intelligence [SIGINT]). The sources of the raw data may include, but are not limited to, news reports, aerial imagery, satellite imagery, and government and public documents.

PROCESSING AND EXPLOITATION: Convert the raw data into a comprehensible format that is usable for production of the finished product.

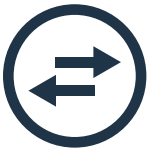
The processing and exploitation step (see the Glossary of Terms for a definition of "exploitation") involves the use of highly trained and specialized personnel and technologically sophisticated equipment to turn the raw data into usable and understandable information. Data translation, data decryption, and interpretation of filmed images and other imagery are only a few of the processes used for converting data stored on film, magnetic, or other media into information ready for analysis and production.

ANALYSIS AND PRODUCTION: Integrate, evaluate, analyze, and prepare the processed information for inclusion in the finished product.

The analysis and production step also requires highly trained and specialized personnel (in this case, analysts) to give meaning to the processed information and to prioritize it against known requirements. Synthesizing the processed information into a finished, actionable (see the Glossary of Terms for a definition of "actionable") intelligence product enables the information to be useful to the customer. Note that, in some cases, the Intelligence Cycle may skip this step (for example, when the consumer needs only specific reported information or products such as raw imagery). This was the case during the Cuban Missile Crisis (October 1962) when President Kennedy needed only the actual number of pieces of Soviet equipment in Cuba and facts concerning reports on observed Soviet activity with no analysis of that information.

DISSEMINATION: Deliver the finished product to the consumer that requested it and to others as applicable.

The consumer that requested the information receives the finished product, usually via electronic transmission. Dissemination of the information typically is accomplished through such means as websites, email, Web 2.0 collaboration tools, and hardcopy distribution. The final, finished product is referred to as "finished intelligence." After the product is disseminated, further gaps in the intelligence may be identified, and the Intelligence Cycle begins all over again.



EVALUATION: Continually acquire feedback during the Intelligence Cycle and evaluate that feedback to refine each individual step and the cycle as a whole.

Constant evaluation and feedback from consumers are extremely important to enabling those involved in the Intelligence Cycle to adjust and refine their activities and analysis to better meet consumers' changing and evolving information needs.

Intelligence Community Members

NAVAJO CODE TALKERS

Courtesy of Navajo Code Talkers

With little more than ingenious application of their native language, the Navajo Code Talkers created the only unbreakable code in modern military history. From Guadalcanal to Iwo Jima and Okinawa, the Code Talkers served with distinction in every major engagement of the Pacific Theater from 1942 to 1945. Their code, which the Japanese never managed to break, helped to end World War II and save thousands of lives.

The Code Talkers were young Navajo men who were tapped by the U.S. Marines to devise a code for radio communications. The Code Talkers' cryptographic innovation made use of a little-studied and extremely complex Native American language unlike any other. English words were spelled out using Navajo words to represent letters of the English alphabet. For instance, the words "wol-la-chee" (which means "ant" in Navajo) and "be-la-sana" (apple) both stood for the letter "A." The developers of the code also used Navajo words to represent more than 400 frequently used military terms. The word "da-he-tih-hi" (hummingbird) stood for "fighter plane," and "chay-da-gahi" (tortoise) was translated as "submarine."

Office of the Director of National Intelligence

Post 9/11 investigations proposed sweeping change in the Intelligence Community (IC), which resulted in Congressional passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). The IRTPA created the Office of the Director of National Intelligence (ODNI) to improve information sharing, promote a strategic, unified direction, and ensure integration across the U.S. Intelligence Community. The ODNI stood up on April 21, 2005; it is led by a Director of National Intelligence (DNI).

As the leader of the 17 Intelligence Community organizations, the DNI serves as the principal advisor to the President and the National Security Council for intelligence matters related to the national security, and oversees and directs the implementation of the National Intelligence Program. The President appoints the DNI with the advice and consent of the Senate. The DNI works closely with a Presidentially-appointed, Senate-confirmed Principal Deputy Director of National Intelligence to effectively integrate all intelligence related to national and homeland security in defense of the homeland and in support of United States national security interests at home and abroad.

The core mission of the ODNI is to lead the IC in Intelligence Integration, forging a community that delivers the most insightful intelligence possible. Intelligence Integration is the key to ensuring that the highest quality of intelligence is delivered with the right inputs, at the right time, in defense of the Homeland.

The ODNI is also comprised of several statutory components, to include the National Counterterrorism Center (NCTC), the National Counterproliferation Center (NCPC), the National

Counterintelligence Executive (NCIX), and the National Intelligence Council (NIC).

National Counterterrorism Center

The National Counterterrorism Center (NCTC), which resides within the ODNI, has primary responsibility within the U.S. Government for counterterrorism intelligence analysis and counterterrorism strategic operational planning.

NCTC's components are the Directorate of Intelligence, Directorate of Strategic Operational Planning, Directorate of Operations Support, Directorate of Terrorist Identities, and the Office of National Intelligence Management. Their functions are:

- Directorate of Intelligence: Leads the production and integration of counterterrorism analysis for the U.S. Government.
- Directorate of Strategic Operational Planning: Directs the U.S. Government's planning efforts to focus all elements of national power against the terrorist threat.
- Directorate of Operations Support: Provides the common intelligence picture for the counterterrorism community with 24 hours a day/7 days a week situational awareness; terrorism threat reporting; management and incident information tracking; and support for worldwide, national, and international special events.
- Directorate of Terrorist Identities: Maintains a consolidated repository of information on international terrorist identities and ensures Federal agencies can access the information they need through the Terrorist Identities Datamart Environment (TIDE).
- Office of National Intelligence Management: Provides strategic management of all national intelligence related to the IC's counterterrorism mission to set analytic and collection priorities; advance analytic tradecraft and training; and lead strategic planning, evaluation, and budgeting.

National Counterproliferation Center

The National Counterproliferation Center (NCPC) is the bridge from the IC to the policy community for activities within the U.S. Government associated with countering the proliferation of weapons of mass destruction (WMD). NCPC conducts strategic counterproliferation planning for the IC to support policy efforts to prevent, halt, or mitigate the proliferation of WMDs, their delivery systems, and related

materials and technologies. This includes both states of concern and, in partnership with the National Counterterrorism Center, non-state actors. NCPC achieves this by drawing on the expertise of counterproliferation professionals in the IC, the U.S. Government, industry, and academia. These relationships foster an atmosphere of collaboration and intelligence sharing in order to protect the U.S.'s interests at home and abroad.

National Counterintelligence Executive

The National Counterintelligence Executive (NCIX) serves as the head of national counterintelligence and security for the U.S. Government. Per the Counterintelligence Enhancement Act of 2002, the NCIX is charged with promulgating an annual strategy for all counterintelligence elements of the U.S. Government. The Office of the NCIX is charged with integrating the activities of all counterintelligence programs to make them coherent and efficient. They also coordinate counterintelligence policy and budgets to the same end. It is also responsible for evaluating the performance of the counterintelligence community against the strategy. ONCIX's Special Security Division is responsible for security policy and uniformity across the U.S. Government.

National Intelligence Council

The National Intelligence Council (NIC), a Congressionally-mandated council, is a component of the ODNI that conducts mid- and long-term strategic analysis through the use of all-source intelligence. Since its formation in 1979, the NIC has been a source of deep substantive expertise on intelligence matters and a facilitator of integrated, IC coordinated strategic analysis on issues of key concern to senior U.S. policymakers. Some of the NIC's core functions are to:

- Produce National Intelligence Estimates (NIEs) — the IC's most authoritative written assessments on national security issues, as well as a broad range of other Community coordinated products.
- Foster outreach to nongovernmental experts in academia and the private sector to broaden the IC's perspective.
- Articulate substantive intelligence priorities to guide intelligence collection and analysis.

Central Intelligence Agency

The Central Intelligence Agency (CIA) is the largest producer of all-source national security intelligence for senior U.S. policymakers. The CIA's intelligence analysis on overseas developments feeds into the informed decisions by policymakers and other senior decisionmakers in the national security and defense arenas. The CIA does not make foreign policy.

The Director of the CIA (DCIA) is the National Human Intelligence Manager and serves on behalf of the DNI as the national authority for coordination, de-confliction, and evaluation of clandestine HUMINT operations across the IC, consistent with existing laws, Executive Orders, and interagency agreements.

CIA is headquartered in McLean, Virginia.

Organization

The National Clandestine Service (NCS) has responsibility for the clandestine collection (primarily human source collection, or HUMINT) of foreign intelligence that is not obtainable through other means. The NCS engages in counterintelligence activities by protecting classified U.S. activities and institutions from penetration by hostile foreign organizations and individuals. NCS also carries out covert actions in support of U.S. policy goals when legally and properly directed and authorized by the President.

The Directorate of Intelligence (DI) analyzes all-source intelligence and produces reports, briefings, and papers on key foreign intelligence issues. This information comes from a variety of sources and methods, including U.S. personnel overseas, human intelligence reports, satellite photography, open source information, and sophisticated sensors.

The Directorate of Science and Technology (DS&T) accesses, collects, and exploits information to facilitate the execution of the CIA's mission by applying innovative scientific, engineering, and technical solutions to the most critical intelligence problems.

The Directorate of Support (DS) delivers a full range of support, including acquisitions, communications, facilities services, financial management, information technology, medical services, logistics, and the security of Agency personnel, information, facilities, and technology. DS services are both domestic and international in focus and are offered 24 hours a day/7 days a week.

CIA is the Executive Agent for In-Q-Tel, the nonprofit, strategic venture capital firm chartered to connect the technology demands of the CIA and IC partners' intelligence missions with the emerging technology of the entrepreneurial community.

The Open Source Center

The Open Source Center (OSC), under the DNI, is the U.S. Government's center for open source intelligence. The Director of the CIA serves as the Executive Agent for the DNI in managing the OSC. It is charged with:

- Collecting, translating, producing, and disseminating open source information that meets the needs of policymakers, the military, state and local law enforcement, operations officers, and analysts throughout the U.S. Government.
- Helping to enable open source capabilities in other parts of the Government and military.
- Hosting open source material on OpenSource.gov for Government-wide use.

About OSC: OSC produces more than 2,300 products daily, including translations, transcriptions, analyses, reports, video compilations, and geospatial intelligence, to address short-term needs and longer-term issues. Its products cover issues that range from foreign political, military, economic, science, and technology topics, to counterterrorism, counterproliferation, counternarcotics, and other homeland security topics.

OSC also collects "gray literature," which is material with very limited distribution, such as academic papers, brochures, leaflets, and other publicly distributed materials.

OSC provides training through its Open Source Academy, consultative services, and personnel exchanges.

Defense Intelligence Agency

The Defense Intelligence Agency (DIA) collects, produces, and manages foreign military intelligence for policymakers and military commanders. It has major activities at the Defense Intelligence Analysis Center (DIAC), Joint Base Anacostia-Bolling, in Washington, D.C.; the Missile and Space Intelligence Center (MSIC), in Huntsville, Alabama; the National Center for Medical Intelligence (NCMI), in Frederick, Maryland; Rivanna Station near Charlottesville, Virginia; and Quantico Marine Corps Base, Virginia. Approximately 30 percent of DIA's employees are military, and approximately 70 percent are civilians.

The DIA Director is a senior military intelligence advisor to the Secretary of Defense and the DNI. In addition, the DIA Director is the program manager for the General Defense Intelligence Program (GDIP); program manager for the DoD Foreign Counterintelligence Program; functional manager for Measurement and Signatures Intelligence (MASINT) and, since 2006, program coordinator for the DIA and Combatant Command portion of the Military Intelligence Program (MIP). The DIA Director also serves as commander of the Strategic Command's Joint Functional Component Command for Intelligence, Surveillance and Reconnaissance.

Organization

The Directorate for Analysis (DI) assesses foreign militaries with focus on weapons of mass destruction (WMD), missile systems, terrorism, infrastructure systems, and defense-related medical issues. The Deputy Director for Analysis is dual-hatted as the Functional Manager for Analysis for the Defense Intelligence Analysis Program.

The Directorate for Intelligence, Joint Staff (J2) provides foreign military intelligence to the Joint Chiefs of Staff and senior DoD officials.

The Defense Counterintelligence and Human Intelligence Center (DCHC) directs, manages and conducts Defense Counterintelligence (CI) and Human Intelligence (HUMINT) activities to meet Defense requirements. The DCHC is organized to direct, coordinate and deconflict CI and HUMINT issues across Defense, combatant commands and the service CI/HUMINT organizations.

The Directorate for MASINT and Technical Collection (DT) is the defense intelligence center for Measurement and Signatures Intelligence (MASINT). It collects and analyzes MASINT, and also develops new MASINT capabilities.

"United in Memory – Committed to Freedom" is a memorial dedicated to the seven DIA employees who lost their lives on 9/11 at the Pentagon.

The Directorate for Information Management and the Chief Information Office serves as DIA's information technology component. It manages the Department of Defense Intelligence Information System (DoDIIS) and operates the Joint Worldwide Intelligence Communications System (JWICS).

The Underground Facilities Analysis Center

The Underground Facilities Analysis Center (UFAC) uses national intelligence and non-intelligence resources to find, characterize, and assess underground facilities (UGFs) used by adversarial state and non-state actors. UFAC coordinates IC efforts to detect, analyze, collect, and report on UGF programs in support of U.S. policymakers, warfighters, and the defense acquisition community. The UFAC Director reports jointly to the Secretary of Defense and the DNI through DIA. UFAC is composed of elements from DIA, Defense Threat Reduction Agency (DTRA), NGA, and NSA.

National Media Exploitation Center

The National Media Exploitation Center (NMEC) ensures the rapid collection, processing, exploitation, dissemination, and sharing of all acquired and seized media across the intelligence, counterintelligence, military, and law enforcement communities. These tasks include the collection, receipt, cataloging, initial processing, and transmission of information; forensic analysis and translation; and reporting, storage, dissemination, and sharing. NMEC is a DNI Center, and DIA is its Executive Agent.

National Geospatial-Intelligence Agency

The National Geospatial-Intelligence Agency (NGA) is the nation's premier source of geospatial intelligence.

As a Department of Defense combat support agency and a member of the U.S. Intelligence Community, NGA provides imagery, geospatial, and targeting analysis, along with image sciences and modeling for U.S. national defense, disaster relief, and safety of navigation.

The vision of NGA is to put the power of Geospatial Intelligence (GEOINT) into its customers' hands

- By providing online, on-demand access to its content, services, expertise, and support, along with the tools that allow users to serve themselves, and
- By broadening and deepening its analytic expertise, providing anticipatory analysis, and moving from a target-based model to an issue-driven, activity-based environment.

NGA seeks to know the Earth, show the way, and understand the world.

Headquartered in Springfield, Virginia, NGA also has facilities in St. Louis, Missouri. NGA support teams are located worldwide to provide direct GEOINT services to NGA customers and partners.

National Reconnaissance Office

The National Reconnaissance Office (NRO) was established in September 1961 as a classified agency of the Department of Defense (DoD). The existence of the NRO and its mission were declassified in September 1992.

Headquartered in Chantilly, Virginia, the NRO develops and operates unique and innovative overhead reconnaissance systems and conducts intelligence-related activities for U.S. national security. The NRO is staffed by members of the armed services as well as civilians from the Central Intelligence Agency and the DoD. The NRO is managed by a Director, a Principal Deputy Director, and a Deputy Director.

NRO systems provide SIGINT (enemy communications, signals from foreign weapons systems, and other signals of interest) and GEOINT (imagery) intelligence data. NRO satellites are frequently the only collectors able to access critical areas of interest in support of covert and high priority operations.

Key customers and mission partners of the NRO include: policymakers, the Armed Services, the Intelligence Community, Departments of State, Justice, and the Treasury, and civil agencies. All of them depend on NRO systems to help attack hard problems such as:

- Countering the Improvised Explosive Device (IED) threat
- Capturing terrorists
- Warning of enemy attacks
- Combating WMD proliferation
- Combating drug trafficking
- Supporting natural disaster response

The NRO is funded through the National Intelligence Program (NIP) and the Military Intelligence Program (MIP) consistent with the priorities and processes established by the DNI and the Under Secretary of Defense for Intelligence (USD(I)).

National Security Agency

The National Security Agency and its military partner, the Central Security Service, leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (NCO) in order to gain a decision advantage for the nation and our allies under all circumstances.

NSA is part of the Department of Defense, and is staffed by a combination of civilian and military personnel.

The Central Security Service (CSS) provides timely and accurate cryptologic support, knowledge, and assistance to the military cryptologic community. It promotes full partnership between NSA and the cryptologic elements of the Armed Forces, and teams with senior

military and civilian leaders to address and act on critical military-related issues in support of national and tactical intelligence objectives. CSS coordinates and develops policy and guidance on the Signals Intelligence and Information Assurance missions of NSA/CSS to ensure military integration.

NSA/CSS has an extensive consumer outreach system, with representatives in many intelligence consumer organizations in the Washington, D.C., area, in other parts of the U.S., and around the world. NSA's headquarters is at Fort Meade, Maryland.

Organization

The Signals Intelligence Directorate is responsible for collecting, processing, and disseminating information from foreign signals for intelligence and counterintelligence purposes and to support military operations.

Operating under the authority of the Secretary of Defense, the Information Assurance Directorate ensures the availability, integrity, authentication, confidentiality, and nonrepudiation of national security and telecommunications and information systems (national security systems).

The National Security Operations Center (NSOC) is a 24 hours a day/7 days a week operations center that provides total situational awareness across the NSA/CSS enterprise for both foreign Signals Intelligence and Information Assurance, maintains cognizance of national security information needs, and monitors unfolding world events.

The NSA/CSS Threat Operations Center (NTOC) uses both Information Assurance and Signal Intelligence information and authorities to uncover and characterize cyberthreats and to provide situational awareness for network operators and defenders.

The Research Directorate is the only "in-house" organization in the Intelligence Community dedicated to advancing intelligence through science. They create research breakthroughs in mathematics, science, and engineering that enable NSA/CSS to achieve and sustain advances for the Intelligence Community.

Department of Energy

Office of Intelligence and CounterIntelligence

The Department of Energy (DOE) is responsible for U.S. energy policy.

The Department of Energy also has a system of National Laboratories and Technical Centers,

which are primarily operated by private corporations and universities. They conduct scientific research in the national interest.

The Office of Intelligence and Counterintelligence (IN) is DOE's intelligence office and IC component. It focuses on assessing worldwide nuclear terrorism threats and nuclear counterproliferation, and evaluating foreign technology threats. This office also provides the IC with access to DOE's energy information and technical expertise.

Department of Homeland Security

Office of Intelligence and Analysis

The Department of Homeland Security (DHS) is responsible for leading the unified national effort to secure the United States by preventing and deterring terrorist attacks and responding to threats and hazards.

The Office of Intelligence and Analysis (I&A) provides intelligence support across the full range of Homeland Security missions, as defined in the Quadrennial Homeland Security Review. I&A ensures that information related to homeland security threats is collected, analyzed, and disseminated to all relevant customers. The I&A mission is to equip the Homeland Security Enterprise with the intelligence and information it needs to keep the homeland safe, secure, and resilient. I&A's mission is supported by four strategic goals:

- Promote understanding of threats through intelligence analysis
- Collect information and intelligence pertinent to homeland security
- Share information necessary for action
- Manage intelligence for the homeland security enterprise

I&A is a member of the Intelligence Community and part of a larger Homeland Security Enterprise that includes Departmental leaders and components, state, local, tribal, territorial and private sector partners and other IC members, all of whom require and generate homeland security intelligence and information. The Under Secretary for I&A (U/SIA) also serves as DHS' Chief Intelligence Officer and is responsible to both the Secretary of Homeland Security and the Director of National Intelligence. I&A's budget is 100 percent funded in the National Intelligence Program (NIP).

I&A has a unique mandate within the Intelligence Community and the Federal Government

lead for sharing information and intelligence with state, local, tribal, and territorial governments and the private sector. I&A serves as the information conduit and intelligence advocate for state, local, tribal, and territorial governments. I&A supports 72 recognized state and major urban area fusion centers with deployed personnel and systems, training, and collaboration. This national network of fusion centers is the hub of much of the two-way intelligence and information flow between the Federal Government and our state, local, tribal, and territorial partners. The fusion centers represent a shared commitment between the federal government and the state and local governments who own and operate them.

Although they are not part of the IC, several of DHS's other components have extensive interactions with the IC, including Immigration and Customs Enforcement, Customs and Border Protection, Transportation Security Administration, U.S. Secret Service, and U.S. Citizenship and Immigration Services.

In addition, the U.S. Coast Guard, a DHS component, is a member of the IC.

Fusion Centers

State and major urban area fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government and state, local, tribal, territorial, and private sector partners.

Located in states and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, Critical Infrastructure and Key Resources (CIKR) protection, and private sector security personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities. Fusion centers provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism.

Fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding.

Interagency Threat Assessment and Coordination Group

The ITACG consists of state, local, and tribal first responders from around the United States and federal intelligence analysts from the Department of Homeland Security, Federal Bureau of Investigation, and National Counterterrorism Center working to enhance the sharing of federal information on counterterrorism, homeland security, and weapons of mass destruction with state, local, and tribal consumers of intelligence.

Coast Guard

The Coast Guard Intelligence and Criminal Investigations Enterprise, as the intelligence element of the Coast Guard, provides timely, actionable, and relevant intelligence and criminal investigative expertise and services to shape Coast Guard operations, planning, and decisionmaking, and to support national and homeland security intelligence requirements.

As the principal federal agency responsible for maritime safety, security, and stewardship, the Coast Guard protects the vital economic and security interests of the United States. The Coast Guard is a multi-mission agency with responsibilities including the safety and security of the public, our natural and economic resources, the global maritime transportation system, and the integrity of our maritime borders. The Coast Guard Intelligence and Criminal Investigations Enterprise develops actionable intelligence to support the Coast Guard in all eleven of its statutory missions.

The Coast Guard fills a unique niche within the Intelligence Community. As a result of its diverse authorities and missions, the Coast Guard maintains broad awareness of the maritime environment. As a military service operating within the Department of Homeland Security, the Coast Guard operates at the intersection between homeland security and national defense. As a law enforcement agency and a national intelligence community member, the Coast Guard also bridges between these two communities. The Coast Guard is also a federal regulatory agency with robust interaction with industry and regional groups.

The nation depends on the Coast Guard's access, operations, and expertise in the maritime environment. We protect citizens from the sea, we protect America from threats delivered by sea, and we protect the sea itself.

Organization

The Assistant Commandant for Intelligence and Criminal Investigations is the Intelligence Community Element Head for the Coast Guard.

The Coast Guard Intelligence and Criminal Investigations Enterprise includes the Coast Guard Investigative Service, Coast Guard Counterintelligence Service, Coast Guard Cryptologic Group, Coast Guard Cyber Command, and the Intelligence Coordination Center. Actionable intelligence is also provided by intelligence staffs on each coast at the two Areas—Pacific and Atlantic, Regional Districts, and Local Sector Commands, and by a Maritime Intelligence Fusion Centers.

Department of Justice

Drug Enforcement Administration

The Drug Enforcement Administration (DEA) is responsible for enforcing the controlled substance laws and regulations of the United States. It brings to the criminal and civil justice system of the United States or any other competent jurisdiction, those organizations and the principal members of those organizations involved in or facilitating the growing, manufacturing, or distribution of controlled substances appearing in or destined for illicit traffic in the United States. DEA also has important responsibilities for the oversight and

enforcement of laws pertaining to controlled pharmaceuticals (including, for example, prescription narcotic drugs, such as those derived from oxycodone and hydrocodone) under the Controlled Substances Act. In addition, DEA recommends and supports non-enforcement programs aimed at reducing the availability of illicit controlled substances on domestic and international markets.

DEA has 21 field divisions in the U.S. and more than 80 offices in more than 60 countries worldwide.

Office of National Security Intelligence

DEA's Office of National Security Intelligence (ONSI) became a member of the IC in 2006. Located at DEA Headquarters in Arlington, Virginia, ONSI facilitates full and appropriate intelligence coordination and information sharing with other members of the U.S. Intelligence Community and homeland security elements. Its goal is to enhance the U.S.'s efforts to reduce the supply of drugs, protect national security, and combat global terrorism.

Department of Justice

Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI), as an intelligence and law enforcement agency, is responsible for understanding threats to our national security and penetrating national and transnational networks that have a desire and capability to harm the U.S. The FBI coordinates these efforts with its IC and law enforcement partners. It focuses on terrorist organizations, foreign intelligence services, Weapon of Mass Destruction (WMD) proliferators, and criminal enterprises.

The FBI is headquartered in Washington, D.C. It has 56 field offices and more than 400 satellite offices throughout the U.S. The FBI also has more than 60 international offices, known as Legal Attaches, in embassies worldwide.

National Security Branch

The National Security Branch (NSB) oversees the FBI's national security programs. It includes four divisions, plus the Terrorist Screening Center (TSC).

The Counterterrorism Division (CTD) focuses on both domestic and international terrorism. It oversees the Joint Terrorism Task Forces (JTTFs).

The Counterintelligence Division (CD) prevents and investigates foreign intelligence activities within the U.S. and espionage activities in the U.S. and overseas.

The Directorate of Intelligence (DI) is the FBI's intelligence analysis component. It has embedded employees at FBI Headquarters and in each field office through Field Intelligence Groups (FIGs) and fusion centers.

The Weapons of Mass Destruction Directorate (WMDD) prevents individuals and groups from acquiring WMD capabilities and technologies for use against the U.S., and links all operational and scientific/technology components to accomplish this mission.

The Terrorist Screening Center (TSC) was created to consolidate the Government's approach to terrorist screening and create a single comprehensive watch list of known or suspected terrorists. The TSC helps ensure that federal, local, state, and tribal terrorist screeners have ready access to information and expertise.

Joint Terrorism Task Force

Joint Terrorism Task Forces (JTTFs) are FBI-led multi-organization task forces composed of local, state, and federal entities. They were established by the FBI to conduct operations to predict and disrupt terrorist plots. JTTFs are in more than 100 cities nationwide; in addition, there is at least one in each of the FBI's 56 field offices. The National Joint Terrorism Task Force (NJTTF), in Washington, D.C., coordinates all the JTTFs.

The National Virtual Translation Center

The National Virtual Translation Center (NVTC) was established in 2003 to provide timely and accurate translations in support of national security. Its mission includes acting as a clearinghouse for facilitating interagency use of translators; partnering with elements of the U.S. Government, academia, and private industry to identify translator resources and engage their services; building a nationwide team

of highly qualified, motivated linguists and translators, connected virtually to the program office in Washington, D.C.; and applying state-of-the-art technology to maximize translator efficiency. NVTC is a DNI Center, and the Federal Bureau of Investigation is its Executive Agent.

Department of State

Bureau of Intelligence and Research

The Department of State is the lead agency for U.S. foreign policy and diplomacy. Its intelligence support component is the Bureau of Intelligence and Research (INR).

The Bureau of Intelligence and Research provides intelligence support to the Secretary of State and other State Department policymakers, including ambassadors, special negotiators, country directors, and desk officers. As the senior intelligence official at the State Department, INR's Assistant Secretary ensures that intelligence informs policy and that intelligence activities support American diplomatic objectives.

INR supports the Secretary of State's global responsibilities by:

- Analyzing foreign events, issues, and trends.
- Coordinating intelligence policy and activities.
- Surveying foreign public opinion and analyzing foreign media.
- Organizing conferences to benefit from outside expertise, managing the Intelligence Community Associate's Program, and administering the Title VIII grant program on Eurasian and East European Studies.
- Analyzing foreign humanitarian challenges.

INR has approximately 300 personnel drawn principally from the Civil Service and the Foreign Service.

Department of the Treasury

Office of Intelligence and Analysis

The Office of Intelligence and Analysis (OIA) represents the Department of the Treasury in the Intelligence Community and is responsible for all intelligence and counterintelligence

activities related to the operations and responsibilities of the Department. It is OIA's mission to advance national security and protect the integrity of the financial system by informing Treasury decisions with timely, relevant, and accurate intelligence and analysis. OIA supports the formulation of policy and the execution of the Treasury Department's authorities by providing expert analysis and intelligence production on financial and other support networks for terrorist groups, proliferators, and other key national security threats. OIA also assists departmental customers in maintaining situational awareness on the full range of economic, political, and security issues by providing current intelligence support and facilitating access to Intelligence Community production on strategic issues.

Army

The Department of the Army's IC component is called Army Military Intelligence (Army MI). It is fully integrated into Army forces. Army MI's goal is to provide all-source intelligence that is relevant, useful, and timely, to the Army and other military personnel at all levels.

Organization

The Deputy Chief of Staff, G-2, is the senior intelligence officer in the U.S. Army and is responsible for Army intelligence activities. This includes policy formulation, planning, programming, budgeting, management, staff, supervision, evaluation, and oversight. As the Deputy Chief of Staff, G-2, his or her staff is also responsible for coordinating all Army intelligence.

National Ground Intelligence Center

The National Ground Intelligence Center (NGIC) produces and disseminates scientific and technical intelligence and military capabilities analysis on foreign ground forces required by war fighting commanders, the force modernization and research and development communities, Defense Department, and national policymakers to ensure that U.S. forces have a decisive edge in current and future military operations. NGIC, headquartered in Charlottesville, Virginia, is a major subordinate command under the U.S. Army INSCOM. Its mission includes irregular and conventional warfare analysis examining foreign ground forces from a perspective that includes battlefield operating systems, doctrine, tactics, techniques and procedures, training, maintenance, logistics and order of battle.

Intelligence and Security Command

The U.S. Army Intelligence and Security Command (INSCOM), the Army's operational intelligence force, is headquartered at Fort Belvoir, Virginia. It is a global command with major subordinate commands that tailor their support to the specific needs of different theaters of operation (e.g. Europe, South America, South West Asia). INSCOM's strategic organization of 16,800 Soldiers, civilians, and contractors at more than 180 locations around the globe ensures that leaders at all levels have access to the intelligence information they need, when and where they need it.

Navy

Naval Intelligence's mission is to support maritime operations worldwide in defense of the United States. Naval intelligence professionals, who are all members of the Information Dominance Community, are deployed throughout the Navy and the Department of Defense.

Organization

The Director of Naval Intelligence is also designated as the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) and reports to the Chief of Naval Operations (CNO).

Office of Naval Intelligence

The Office of Naval Intelligence (ONI), headquartered at the National Maritime Intelligence Center (NMIC) in Suitland, Maryland, is a major production center for maritime intelligence. It produces intelligence on seaborne terrorism, weapons and technology proliferation, and narcotics and smuggling operations. ONI also analyzes foreign naval strategies, capabilities, operations, characteristics, and trends to support Navy, Department of Defense, and national needs.

ONI and the Coast Guard Intelligence Coordination Center (USCG-ICC) both have a maritime mission, and they share an intelligence partnership that started in the early 1970s. They are identified as the core element of the Global Maritime Intelligence Integration (GMII) Plan. That plan is a component of the National Strategy for Maritime Security, which was signed by the President in late 2005. ONI and

USCG-ICC man an around-the-clock maritime watch in the NMIC, which tracks over 18,000 vessels worldwide.

Air Force

The Air Force Intelligence, Surveillance, and Reconnaissance (AF ISR) is the Air Force's IC component.

Organization

The Air Force Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (A2) provides policy, oversight, and guidance to all Air Force intelligence organizations.

The Air Force ISR Agency organizes, trains, equips, and presents forces to conduct intelligence, surveillance, and reconnaissance for combatant commanders and the nation. Air Force ISR is also responsible for implementing and overseeing policy and guidance, and expanding AF ISR capabilities to meet current and future challenges. The AF ISR Agency commander serves as the Service Cryptologic Element under NSA, and oversees Air Force Signals Intelligence activities.

The AF ISR Agency has more than 19,000 military and civilian members serving at 72 locations worldwide and commands several subcomponents, including the 70th ISR Wing, The 480th ISR Wing, the 361st ISR Group, the Air Force Technical Application Center, and the National Air and Space Intelligence Center.

Marine Corps

The U.S. Marine Corps (USMC) produces tactical and operational intelligence for battlefield support. Its IC component is comprised of all intelligence professionals in the Marine Corps. Most Marine Corps intelligence professionals are integrated into operating forces.

Organization

The Marine Corps' Director of Intelligence (DIRINT) is its principal intelligence staff officer, and is the service's functional manager for intelligence, counterintelligence, and cryptologic matters.

Marine Corps Intelligence Activity

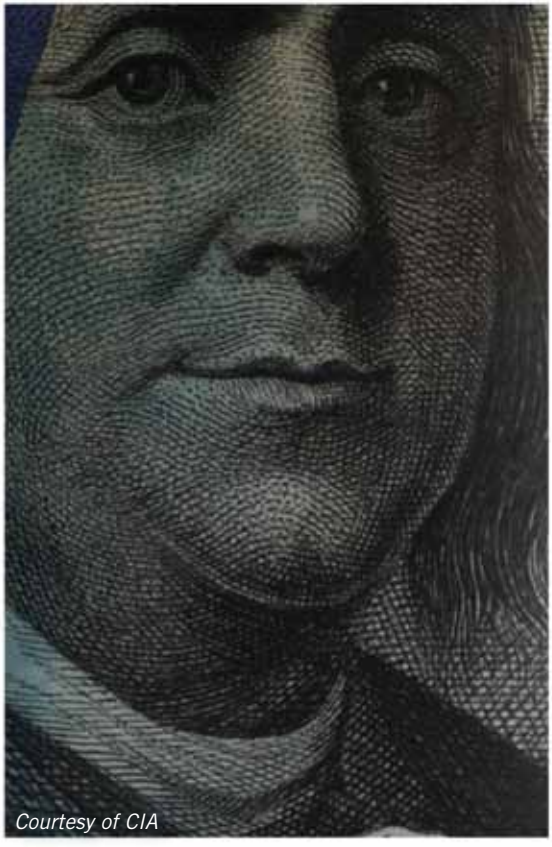
Marine Corps Intelligence Activity (MCIA), in Suitland, Maryland, and Quantico, Virginia, is the USMC service production center. In addition, MCIA supports other services as appropriate. It provides the Marine Corps with intelligence for planning, training, operations, and exercises. MCIA can be tasked to provide expeditionary warfare intelligence to support any national, theater, or operational command in the U.S. Armed Forces. MCIA's analysis and production support not only the Marine Corps, but also the national decisionmaker, theater commander, and operational warfighter.

MCIA is a major production organization for expeditionary intelligence and cultural intelligence.

Requirements, Planning, and Direction

Inventor, Writer, Publisher, Diplomat, Statesman and...Spy!

BENJAMIN FRANKLIN



Courtesy of CIA

Although most people know of Benjamin Franklin as a prolific inventor, scientist, author, and signer of the Declaration of Independence, few know that "spy" can be added to the list. He served on a number of committees of the Second Continental Congress, including the Committee of Secret Correspondence, which was essentially the country's first foreign intelligence directorate. The group employed numerous agents abroad and established a secret Navy for receipt of information and supplies. Franklin also served on another secret committee that clandestinely obtained and distributed military supplies and sold gunpowder to privateers hired by the Continental Congress.

During a diplomatic mission to France, Franklin gathered intelligence, distributed propaganda, and coordinated aid from America's secret allies (and also discovered that several of his employees, including a secretary and courier, were, unfortunately, British agents).

Franklin also was a crafty propagandist. To weaken enemy forces, he reportedly distributed leaflets disguised as tobacco packets that promised American land grants to deserting soldiers.

What Intelligence Can (and Cannot) Do

"The United States Intelligence Community must constantly strive for and exhibit three characteristics essential to our effectiveness. The IC must be integrated: a team making the whole greater than the sum of its parts. We must also be agile: an enterprise with an adaptive, diverse, continually learning, and mission-driven intelligence workforce that embraces innovation and takes initiative. Moreover, the IC must exemplify America's values: operating under the rule of law, consistent with Americans' expectations for protection of privacy and civil liberties, respectful of human rights, and in a manner that retains the trust of the American people."

National Intelligence Strategy 2009

Intelligence can be an extremely powerful tool, but it is most useful when the consumer has a clear understanding of its limits. With the ever-changing laws, policies, capabilities, and standards affecting the production and dissemination of intelligence, these general guidelines can help consumers know what to expect from this valuable resource.

What Intelligence Can Do

Intelligence can:

- Provide an advantage in dealing with foreign adversaries by supplying information and analysis that can enhance the intelligence consumer's understanding.
- Warn of potential threats and opportunities.
- Provide insight into the causes and consequences of current events.
- Enhance situational awareness.
- Assess long-term strategic issues and alternative futures.
- Assist in preparation for international or planning meetings.
- Inform official travelers of security threats.
- Report on specific topics, either as part of routine reporting or upon request.
- Compile information on persons of interest.

What Intelligence Cannot Do

Predict the Future or Know about Everything

- Intelligence can provide assessments of likely scenarios or developments, but it cannot provide predictions of what will happen with absolute certainty. The IC's resources and capabilities are limited by:
  - Numerous priorities competing for finite budget dollars, personnel, and capabilities.
  - Limited access to denied areas.
  - Technological limitations of some IC systems.
- The IC must maintain its ability to obtain useful information.
  - The need to protect information and intelligence sources and methods may limit the sharing or use of some reports.

Violate U.S. law or the U.S. Constitution

The activities of the U.S. IC must be conducted in a manner consistent with all applicable laws and Executive Orders (see a listing of Executive Orders in Tab 8). The IC is particularly aware of the importance of ensuring:

- Civil liberties and the privacy of U.S. citizens and lawful U.S. residents.
- Confidentiality of sources and the identities of IC personnel and protection of privileged information.
- Appropriate conduct of IC personnel and activities.

Who Uses U.S. Intelligence?

The IC serves a wide range of consumers, both within and outside the U.S. Government, with the level of intelligence services varying according to the customers' responsibilities and the specific circumstances. The IC's customers include the following:

- The White House, particularly the President, Vice President, and National Security Staff.
- Executive Branch Departments and Agencies, including the Departments of State, Defense, Homeland Security, the Treasury, Energy, Commerce, Justice, and others.
- Military unified commands, services, and deployed forces.
- The Intelligence Community itself, for IC internal operations, special activities, acquisition, and policy support.
- The Legislative and Judicial branches for oversight and to inform and protect.
- State, local, tribal and territorial officials, especially law enforcement and emergency planning and response personnel.
- The U.S. public, including commercial entities and academia.
- Allied governments.
- International organizations, especially for such activities as treaty monitoring.

Types of Customers

While intelligence users can easily be grouped by organization (e.g., Department of State), level of seniority (e.g.Assistant Secretary), or discipline (such as diplomacy), grouping customers according to the purpose to which they are applying intelligence (also known as a "segment") is a more useful categorization. The segment determines the characteristics that will make an intelligence product or service effective. A customer may change segments, depending on the specific activity. In such cases, the customer's needs also change. For instance customer segments might include the following:

National Interagency Action, e.g., Deputy National Security Advisor for Combating Terrorism

- Requires coordination of multiple agencies or partners.
- Needs to understand what is important to each colleague.

Organizational Policy and Decisionmaking, e.g., State Department Assistant Secretary for European Affairs

- Focused on a single agency mission.
- Finished, all-source, tailored analysis.

- Time sensitivity and need to share vary

Negotiation, e.g., U.S. Trade Representative

- Is extremely time sensitive and close hold.
- Raw, tactical, narrow collection reports.

Strategic Resource Deployment and Acquisition, e.g., DoD Under Secretary for Acquisition, Technology, and Logistics

- Long-range planning.
- The intelligence is often critical to countering an adversary's capabilities.
- Thorough analysis.

Threat Preparedness and Prevention, e.g., DHS Assistant Secretary for Infrastructure Protection

- Plan to respond to threats or to more fully understand potential threats.
- Widely shareable analysis.

Threat Response and Tactical Deployment, e.g., military forces engaged in combat or a city police force responding to an event

- Operational activities.
- Raw, specific, timely collection reports and analysis.

Ways to Interact with the Intelligence Community

IC personnel interact with many customers, and due to the size and wide range of responsibilities of the IC, many customers work with multiple IC personnel, including analysts, security and counterintelligence personnel, and managers of intelligence operations. Overall, the IC interacts with its customers in the following ways:

Supports customers' decisionmaking and operations by:

- Informing customers of factual developments, generally through dissemination of collection reports.
- Processing, aggregating, and interpreting facts in light of extensive knowledge to ultimately evaluate events and trends.
- Conducting research in response to customers' specific requests for information.
- Consulting or collaborating with customers to more fully understand an issue and to provide ongoing expertise.

Works with customers by:

- Apprising customers of ongoing IC operations that might intersect with customers' operations and by playing a supporting role in customers' operations.
- Harvesting information with intelligence value that customers collect in the course of their normal operations.
- Planning for future collection, analysis, or other resource deployment by specifying

and transmitting customers' requirements and priorities.

- Evaluating the effectiveness of IC support to improve service to customers.
- Training customers in intelligence, security, and special technologies.

Protects customers by:

- Identifying, deceiving, exploiting, or disrupting efforts aimed against customers by hostile intelligence services.
- Protecting sensitive data by, for example, providing secure facilities or granting security clearances.
- Providing secure communications, including information technology for securing Sensitive Compartmented Information (SCI).
- Providing crisis and consequence management support during national security special events and emergencies.

Roles, Responsibilities, and Expectations of Customers

Customers themselves play a vital role in ensuring that IC support meets their needs. Good communication between the customer and the IC, often through the agency intelligence office of the customer, will improve intelligence support. For the best possible assistance, customers should:

- Integrate the IC into their operational cycle and processes.
  - Early integration of the IC into a customer's operations helps the IC deliver better service more quickly.
- Expect intelligence support to be a push-and-pull process.
  - The IC should flag emerging issues as well as answer customers' questions as they arise.
  - Answers to customers' questions can be delivered in various formats (for example, in briefs, papers, graphics, or simulations) depending on the most expedient and effective way to supply the information.
- State their requests specifically.

- The customer should specify their current understanding of an issue or problem.
- The customer should specify exactly what they need to know.
- The customer should specify the context of the request (for example, to support a meeting, an event, or decisionmaking).

- Share what they know.
  - National security information is everywhere; the IC has no monopoly.
  - Shared information can inform opportunity analysis, communicate the intended direction of policy or operational endeavors, or options under consideration.
- Share their timeline.
  - Customers should specify the factor or factors that are influencing the timeline so that the intelligence effort can be scoped and scaled accordingly.
  - Customers should understand that declassification or downgrading of information takes some time to complete.
- Provide feedback on the utility of IC products and services.
  - Customer feedback helps the IC to refine its approach.

Intelligence Planning, Programming, Budgeting, and Evaluation

The Assistant Director of National Intelligence for Systems and Resource Analyses (ADNI/SRA) manages the integration and synchronization of the Intelligence Planning, Programming, Budgeting, and Evaluation (IPPBE) system. This system is employed to effectively shape intelligence capabilities through the development of the National Intelligence Program (NIP) and budget in a manner consistent with the National Intelligence Strategy (NIS).

The IPPBE process comprises the interdependent phases of planning, programming, and budgeting that are linked by the ongoing evaluation phase. Each phase is informed and guided by the products and decisions of each of the other phases:

- Planning: The planning phase identifies Director of National Intelligence (DNI) strategic priorities and major issues to be addressed in the programming phase.
- Programming: The programming phase provides options to frame DNI resource decisions through analyses of alternatives and studies that assess cost-versus-performance benefits.
- Budgeting: The budgeting and execution activities are addressed in IPPBE in a manner consistent with the policy principles of Intelligence Community Directive

(ICD) 104, with the goal of producing and implementing an annual, consolidated NIP budget.

- Evaluation: The evaluation phase assesses the effectiveness of IC programs, activities, major initiatives, and investments in implementing DNI guidance in the context of original objectives, measures of effectiveness, metrics, outcomes, benefits, shortfalls, and costs.

The IPPBE system ensures a predictable, transparent, and repeatable end-to-end process to collect and prioritize critical intelligence requirements within the context of the strategic objectives of the DNI and the IC. In addition, the IPPBE framework supports the DNI's participation in the development of the Military Intelligence Program (MIP).

Acquisition/Science and Technology: Delivering Technical Capabilities

Major System Acquisitions

At any given time, several dozen Major System Acquisitions (MSAs) are underway at agencies throughout the IC. MSAs cost hundreds of millions or billions of dollars, and they typically take years to develop, build, and deliver. MSAs are usually either Platform and Payload systems, such as satellites and surveillance ships, or information technology (IT) systems, including infrastructure (hardware and platforms), applications (automated processes and user tools), and human interfaces. Each MSA is run by an IC agency team of highly skilled professionals, including scientists, technicians, engineers, and mathematicians. They manage the significant systems engineering effort that is required to reliably deliver MSA capabilities.

Intelligence Community Science and Technology

Many IC elements conduct science and technology (S&T) research in their own laboratories, and almost all IC elements sponsor research conducted by universities, industry, or Department of Energy (DOE) national labs. IC S&T leads the world in some areas of research specific to IC missions and works with industry to develop other new technologies that have limited commercial applications. Rather than invest research in technologies that industry develops for consumers, IC S&T monitors commercial products and looks for ways to adapt them to the specific operational and security requirements of IC operations. IC S&T research can lead directly to IT products, may result in a capability within an MSA, or may generate specialty applications, relatively low-cost technologies such as miniaturized tracking or collection devices, which are produced in small numbers and deployed to address a specific intelligence problem. IC S&T also conducts basic research into areas such as cryptology and computer science, which generate no physical products but are essential to intelligence work.

Procurement and Contracting

All IC agencies have offices that manage the contracts through which the agencies purchase mass-produced technologies and manage the resources and logistics necessary to support the deployment of those technologies into operations.

Facilities

Facilities also provide an essential platform for intelligence technologies, from office buildings to ground stations to data centers.

Intelligence Community Requirements Processes

The established IC requirements processes are the primary means for developing, documenting, assessing, validating, and approving capability requirements for NIP capabilities that are mission relevant and fiscally sound. Two complementary requirements processes are used within the IC—the Intelligence Community Capability Requirements (ICCR) process, which is used largely for MSAs, and the DNI Deputy Director for Intelligence Integration (DDII) Requirements Process.

ICCR Process

The ICCR process applies to all MSA programs of special interest as designed by the DNI or the Deputy DNI for Acquisition and Technology (DDNI/A&T) that are funded in whole or in large part by the NIP. The objectives of the ICCE process staff are as follows:

- To ensure that the requirements for all NIP-funded MSA programs are validated by the Deputy Executive Committee (DEXCOM) Intelligence Resources Board (IRB).
- To work with the Joint Staff/J8 via a "gatekeeper" process on coordinating NIP- and MIP-funded programs, and to work with IC stakeholders via the Capability Requirements Working Group (CRWG).
- To provide and maintain a documented, agile, and transparent process for soliciting and approving capability-based requirements that leads to achievable system developments or non-material solutions with a positive mission impact for the IC.

DDII Requirements Process

The DDII Requirements Process applies to those programs that do not meet the MSA or special interest threshold. The DDII Requirements Process enables ODNI senior leaders to have a single, prioritized list of mission-based requirements.

The process also allows for the consideration of all mission-based requirements proposed by all stakeholders across the IC. The single, validated, prioritized, mission-based, approved intelligence requirements list is then used for NIP funding purposes.

The process involves interacting with the requesting stakeholders and mission experts and uses a common set of prioritization criteria to establish the validity of requirements. The major steps in the process are analysis and assessment, validation, prioritization, and recommendation of funding strategies.

The process includes the maintenance of the baseline and requirements, including both requirements to be funded and requirement on the Prioritized Unfunded Requirements List. The process also creates output to be used for other DNI processes (e.g., SRA, chief information officer [CIO], chief financial officer [CFO]), and to evaluate, review, and report on the status of requirements until their completion.

The DDII Requirements Process will be executed to coincide with major budget milestones and schedules to ensure that requirements are on track with funding cycles.

Collections Management Overview

Collection management is the process of converting intelligence requirements into collection requirements (see the Glossary of Terms for a definition of "collection"), establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring the results, and re-tasking, as required. Collection management is divided into two business areas:

- Collection Requirements Management (CRM): CRM is the authoritative development and control of collection, processing, exploration, or reporting requirements that typically result in either the direct tasking of assets over which the collection manager has authority, or the generation of tasking requests that are sent to collection management authorities at a higher, lower, or equivalent level to accomplish the collection mission.
- Collection Operations Management (COM): COM is the authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources.

Essentially, CRM is what gets done in the collection cycle, while COM is how it gets done. The collection management process is a staff activity focused on decisionmaking and choices concerning collection request (CRs) and requests for information (RFIs) from numerous sources.

A collection manager can be either a requirements expert or an operations expert. The collection manager is the individual who orchestrates and manages the analysts' needs throughout the collection cycle. A collection manager's duties include receiving CRs, researching intelligence systems, developing collection strategies or plans, developing collection requests into collection requirements, validating collection requirements, and tracking requirements through the collection cycle to determine stakeholders' satisfaction with the outcomes of the requirements.

The CRM process begins when requests are identified, logged, and initially processed. The entire process involves tracking a request from the time of its receipt, validating the request, tasking the necessary collectors, confirming fulfillment of the requestor's information need, and updating the collection plan.

The availability and capability of collection assets and resources are determined, in part, by the exchange of timely data among the operational mission planners and asset managers who update intelligence. This data helps the RMs to perform a more complete analysis of an information request, determine the most effective collection system(s) to fulfill the request, and perform a thorough, overall assessment of the unit's organic and non-organic reconnaissance and surveillance support. In addition, collection coordination supports the development of a collection strategy, including a coverage plan, selection of sources and selection of disciplines, and assessment of the efficiency of tasking assets and resources.

Because CRM is essentially a support function for expediting information collection and dissemination, the RM and staff are their own best resources for assessing CRM performance. Nevertheless, coordination with an all-source production facility can facilitate the assessment task.

The COM process is an intelligence staff function that is based on collection tasking and mission guidance developed in support of information requirements. COM relies heavily on supporting organizations that own and operate collection and exploitation assets.

COM involves several tasks, including planning, scheduling, and the control of collections operations; execution of collections operations; and exploitation and dissemination of collection results.

Collection operations personnel, who typically are intelligence operations staff members,

are responsible for detailed planning, tasking, scheduling, and control of collection operations. The operations planner reviews mission requirements, such as available assets, sensor and target range, system timelines, threats, weather, and reporting requirements and adjusts the collection plan to reflect the plan of operations, including the integration of specific reconnaissance requirements. Requirements are translated into collection-mission tasking orders, which are directed to the asset manager, who is responsible for execution of the orders.

The asset manager chooses the equipment, platform, and personnel to perform the assigned mission based on such considerations as maintenance schedules, training, and experience. The operations planner provides availability and asset location information, while the asset manager provides data related to operational constraints and timeliness of operations.

Exploitation of collected information at the tactical level is closely associated with management of collection assets and resources. The operational staff with collection capabilities also controls sensor-specific processing, exploitation, and analysis equipment. The asset manager who is responsible for executing the collection operation also controls the operation of the exploitation element. As such, exploitation is as much a part of the COM function as are mission planning and asset management.

Prioritizing Intelligence Issues: The National Intelligence Priorities Framework

The National Intelligence Priorities Framework (NIPF) is the DNI's guidance to the IC on the national intelligence priorities approved by the President.

The NIPF is the DNI's sole mechanism for establishing national intelligence priorities. The

NIPF consists of:

- Intelligence topics reviewed by the National Security Council Principals Committee and approved by the President.
- A process for prioritizing foreign countries and non-state actors that are relevant to the approved intelligence topics.
- A priorities matrix that reflects consumers' priorities for intelligence support and that ensures that long-term intelligence issues are addressed.

The NIPF is updated semiannually in coordination with IC elements, the National Intelligence Council, and other internal components of the ODNI. Ad hoc adjustments may also be made to reflect changes in world events and policy priorities.

The ODNI and IC elements use the NIPF to guide allocation of collection and analytic resources. In addition, IC elements associate intelligence collection requirements and analytic production with NIPF priorities, and they report to the DNI on their coverage of NIPF priorities.

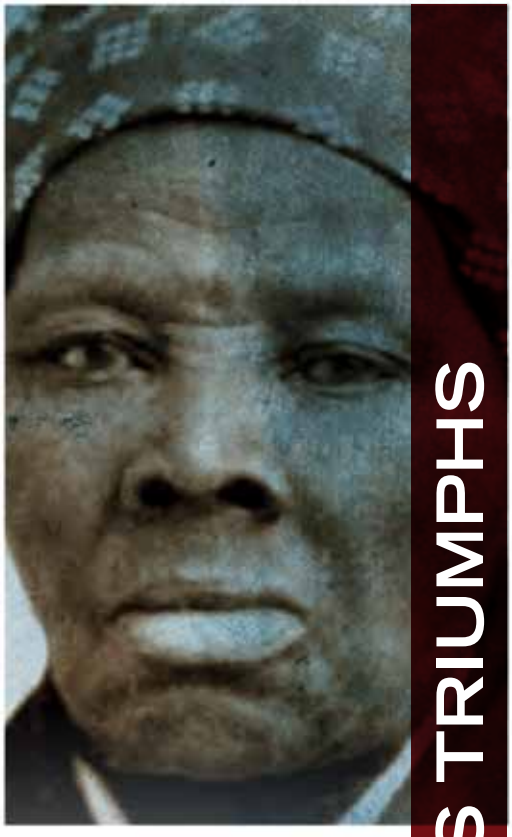
Collection, Processing, and Exploitation

TUBMAN'S TRIUMPHS

Harriet Tubman is best known for helping slaves to escape to safety through the secret network of the 1800s known as the Underground Railroad. Her involvement in intelligence collection during the Civil War, however, also is well documented. After her last secret rescue mission in 1860, Tubman was tapped by Union officials to organize and lead spying expeditions behind Confederate enemy lines.

Disguised as a field hand or poor farm wife, she led several missions while directing others from Union lines. She reported her intelligence to Col. James Montgomery, a Union officer commanding the Second South Carolina Volunteers, a black unit involved in guerrilla warfare activities.

The tactical intelligence Tubman provided to Union forces, including identification of enemy supply areas and weaknesses in Confederate troop deployments, was used effectively in military operations. When Tubman died in 1913, she was honored with a full military funeral in recognition of her intelligence activities during the war.



Courtesy of CIA

Sources of Intelligence

"National Intelligence and the term 'intelligence related to national security' refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security."

United States Congress, Intelligence Reform and Terrorism Prevention Act of 2004, Section 1012, Public Law 108-458, December 17, 2004

MASINT

Measurement and Signatures Intelligence (MASINT) is intelligence produced through quantitative and qualitative analysis of the physical attributes of targets and events to characterize and identify those targets and events.

HUMINT

Human Intelligence (HUMINT) is the collection of information—either orally or via documentation—that is provided directly by a human source. It is the only type of intelligence for which collectors speak directly to the sources

of information, control the topic of discussion, and direct the source's activities. Human sources can obtain access to information that is not obtainable any other way.

The types of HUMINT range from high-level, strategic, national security information, for example, to unit-specific information collected on the battlefield. As stated HUMINT may also be acquired overtly or clandestinely.

In overt collection, the collector meets openly with sources as a declared U.S. Government representative. Overt collection comprises many forms of information collection, including debriefings of persons who have travelled to countries of national interest, diplomatic reports from embassies on host-country officials' stated reactions to U.S. policy initiatives, and law enforcement reports on criminal activities, such as drug trafficking.

Clandestine collection is conducted in secret. A clandestine collector must locate a person with access to desired information, initiate and discreetly develop a relationship with that prospective source, and ultimately convince the source to divulge secrets. A source may or may not be told of his interlocutor's U.S. Government affiliation. After the source is recruited, contact is usually strictly controlled in an effort to elude discovery. The recruitment of a clandestine human source can take months or years, but the leak of a source's information may immediately eliminate access to that source.

GEOINT

Geospatial Intelligence (GEOINT) is the exploitation and analysis of imagery, imagery intelligence (IMINT) (see the Glossary of Terms), and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth.

OSINT

Open-Source Intelligence (OSINT) is intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. OSINT draws from a wide variety of information and sources, including the following:

- Mass Media: Newspapers, magazines, radio, television, and other computer-based information.
- Public Data: Information derived from government reports; official data, such as data on budgets and demographics; hearings; legislative debates; press conferences, speeches, directories, organizational charts, marine and aeronautical safety warnings, environmental impact statements, contract awards, and required financial disclosures, and other public sources.
- Gray Literature (or Grey Literature): Open-source material that usually is available through controlled access for a specific audience. Gray literature may include, but is not limited to, research reports, technical reports, economic reports, travel reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, studies, dissertations and theses, trade literature, market surveys, and newsletters. The material in gray literature covers scientific, political, socioeconomic, and military disciplines.
- Observation and Reporting: Information of significance, not otherwise available, that is provided by, for example, amateur airplane spotters, radio monitors, and satellite observers. The availability of worldwide satellite photography, often in high resolution, on the Web (e.g., Google Earth) has expanded the public's ability to acquire information formerly available only to major intelligence services.

SIGINT

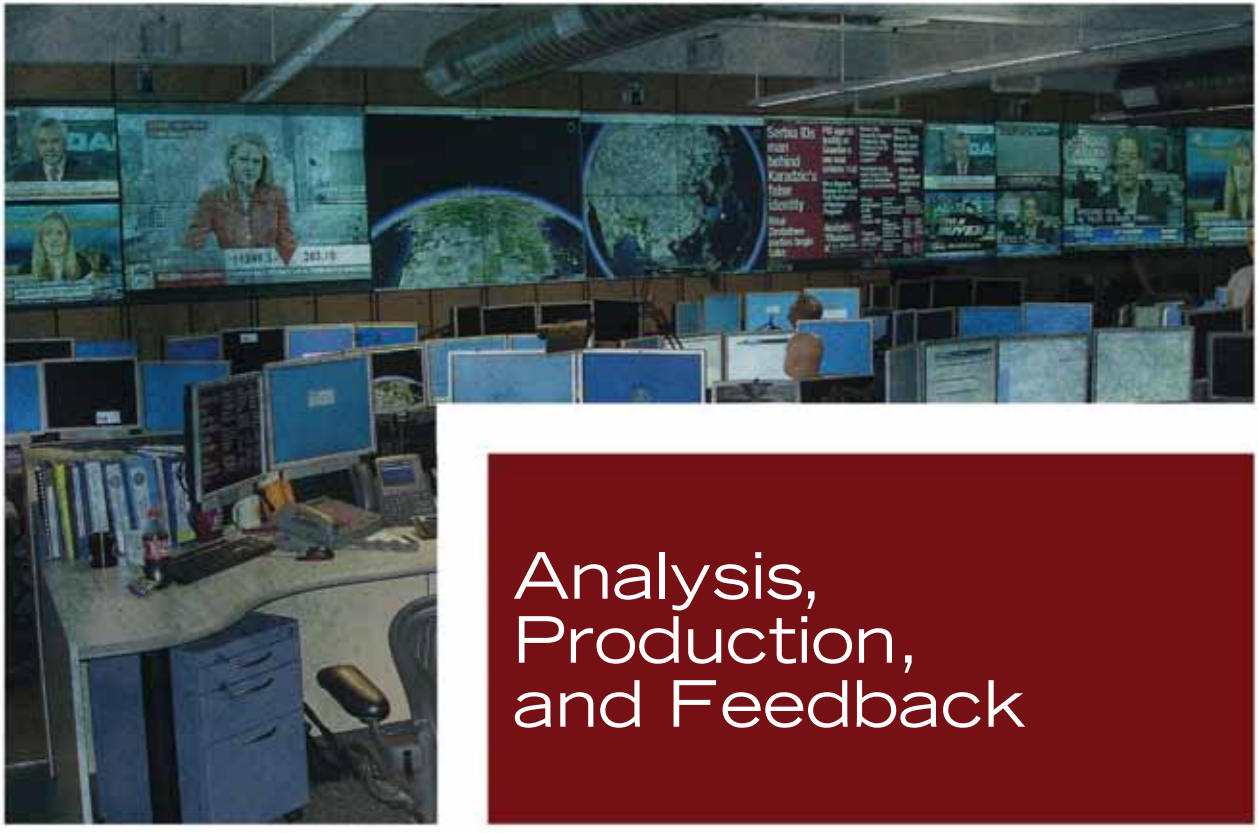
Signals Intelligence (SIGINT) is intelligence gathered from data transmissions, including Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT). SIGINT includes both raw data and the analysis of that data to produce intelligence.

- COMINT is intelligence derived from tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, and analyzing the meaning of communications.
- FISINT is information derived from the interception of foreign electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems including, but not limited to, telemetry, beaconry, electronic interrogators, and video data links.
- ELINT is information derived primarily from electronic signals that do not contain

speech or text (which are considered to be COMINT). The most common sources of ELINT are radar signals.

Processing and Exploitation

A substantial portion of U.S. intelligence resources is devoted to processing and exploitation—the synthesis of raw data into material that is usable by the intelligence analyst—and to securing the telecommunications networks that carry these data. Various activities fall under the category of processing and exploitation including, but not limited to, interpreting imagery; decoding messages; translating foreign-language broadcasts; converting telemetry into meaningful measurements; preparing information for computer processing, storage, and retrieval; and converting HUMINT-based reports into more comprehensible content.



Analysis, Production, and Feedback

JULIA CHILD: LIFE BEFORE FRENCH CUISINE

Julia Child is widely credited with bringing French cuisine into the American mainstream. But long before she gained fame as a cookbook writer and TV personality, she enjoyed a dynamic career as an intelligence officer.

During WWII, Julia wanted to serve her country. Too tall to join the military (she was 6'2"), Julia volunteered for the Office of Strategic Services (OSS), the forerunner of today's Central Intelligence Agency. She started out in the Washington, D.C., headquarters, working directly for General William J. Donovan, the head of the OSS. She joined the OSS Emergency Sea Rescue Equipment Section, where she helped to develop a repellent to keep sharks from setting off explosives before they reached their target. She also served as Chief of the OSS Registry, processing highly classified communications.

Courtesy of CIA

Julia then met and married Paul Child, an OSS officer assigned to the U.S. Information Agency in Paris, where Julia embarked on her legendary culinary career.

Julia Child's contributions to her country are well remembered and appreciated by the OSS family. She died in 2004, two days before her 92nd birthday.

Analysis and Production

Intelligence analysts are generally assigned to a particular geographic or functional specialty area. Analysts obtain information from all sources pertinent to their area of responsibility through information collection, processing, and forwarding systems. Analysts may tap into these systems to obtain answers to specific questions or to generate information they may need.

Analysts receive incoming information, evaluate it, test it against other information and against their personal knowledge and expertise, produce an assessment of the current status of a particular area under analysis, and then forecast future trends or outcomes. The analyst also develops requirements for the collection of new information.

Analysts rarely work alone; they operate within a system that includes peer review and oversight by more senior analysts.

Estimative Language

When the Intelligence Community uses words such as "we judge" or "we assess" (phrases that are used synonymously) and "we estimate," "likely" or "indicate," the IC is conveying an analytical assessment or judgment. Such statements often are based on incomplete or fragmented information and are not to be regarded as statements of fact, proof, or absolute knowledge. Some analytical judgments are based directly on collected information; others are based on assessments that serve as building blocks. In either case, the IC does not have "evidence" that shows something to be factual or that definitely establishes a relationship between two items.

Statements that address the subject of likelihood are intended to reflect the IC's collective estimate of the probability of a development or an event occurring.

The IC's use of the term "unlikely" is not intended to imply that an event definitely will not happen. By comparison, the words "probably" and "likely" indicate that a greater-than-even chance exists of a particular event occurring. The IC uses such phrases as "we cannot dismiss," "we cannot rule out," and "we cannot discount" to refer to an unlikely event whose consequences are serious enough that it warrants mentioning. Words such as "may be" and "suggest" are used when the IC is unable to fully assess the likelihood of an event because relevant information is nonexistent, sketchy, or fragmented.

The IC also refers to "high," "moderate," or "low" confidence levels that reflect the scope and quality of the information supporting its judgments.

- A high confidence level generally indicates that the IC's judgment is based on high-quality information or that the circumstances of the analysis enable the IC to render a solid judgment.
- A moderate confidence level generally indicates that the information being used in the analysis may be interpreted in various ways, or that the IC has alternative viewpoints on the significance or meaning of the information, or that the information is credible and plausible but it is not sufficiently corroborated to warrant a higher level of confidence.
- A low confidence level generally indicates that the information used in the analysis is scant, questionable, fragmented, or that solid analytical conclusions cannot be inferred from the information, or that the IC has significant concerns or problems with the information sources.

Analytic Products

Current Intelligence

Current intelligence addresses day-to-day events. It details new developments and background information related to those developments to assess their significance, warn of their near-term consequences, and signal potentially dangerous situations in the near future.

Trend Analysis

Trend analysis, also referred to as second-phase reporting, provides information on an event or series of events. A trend analysis report on an event includes an assessment of whether the relevant intelligence on the event is reliable, information on similar events, and background information to familiarize the reader with the issue. Typically, the intelligence used in trend analysis is compared with intelligence from other sources and vetted through experts within the IC. Second-phase reports are much more thorough than current intelligence/

first-phase reports and may require weeks or months to produce.

Long-Term Assessment

Long-term assessment is also known as third-phase reporting. It addresses developments within a broad-based context, assesses future trends and developments, or provides comprehensive, detailed analysis of an ongoing issue, a particular system, or some other topic. Long-term assessment reports, which can take months to produce, may be coordinated with experts from across the IC and may include projections of future developments.

Estimative Intelligence

Estimative intelligence uses future scenarios and projections of possible future events to assess potential developments that could affect U.S. national security. By addressing the implications of a range of possible outcomes and alternative scenarios, estimative intelligence helps policymakers to think more strategically about long-term threats.

Warning Intelligence

Warning intelligence "sounds an alarm" for policymakers. This type of intelligence conveys a sense of urgency and implies a possible need to respond with policy action. Warning intelligence includes the identification or forecasting of events, such as coups, third-party wars, or refugee situations, that would warrant the engagement of U.S. military forces or that would have a sudden and detrimental effect on U.S. foreign policy concerns. Warning analysis involves the exploration of alternative futures and low-probability/high-impact scenarios.

Research Intelligence

Research intelligence includes research studies that support both current and estimative intelligence.

Scientific and Technical Intelligence

Scientific and technical Intelligence includes an examination of the technical development, characteristics, performance, and capabilities of foreign technologies, including weapon systems and subsystems. This category of intelligence covers a spectrum of scientific disciplines, technologies, weapon systems, and integrated operations.

Classification

Certain information must be kept in confidence to protect U.S. citizens, institutions, homeland security, and U.S. interactions with foreign nations. The IC, in accordance with Executive Order (EO) 13526, classifies information (that is not Unclassified) as Confidential, Secret, or Top Secret. Classification may be applied only to information that is owned by, produced by or for, or is under the control of the U.S. Government. Section 1.4 of E.O. 13526 discusses classification techniques.

In EO 13526, classification levels are defined as follows:

- Top Secret: Unauthorized disclosure of the information could be expected to cause exceptionally grave damage to the national security.
- Secret: Unauthorized disclosure of the information could be expected to cause serious damage to the national security.
- Confidential: Unauthorized disclosure of the information could be expected to cause damage to the national security.

At the time that material is classified, the original classification authority must establish a specific date or event for declassification. When that date is reached or when the event occurs, the information is automatically declassified. Unless an earlier date or event can be specified, declassification must be marked for 10 years from the date of classification, or up to 25 years from the date of classification, depending on the circumstances. Upon review, the original classification may be extended for up to 25 additional years, the classification may be changed, or specific portions of the classified information may be reclassified. No information may remain classified indefinitely.

Information may not be classified or be maintained as classified information in order to:

- Conceal violations of law, inefficiency, or administrative error;
- Prevent embarrassment to a person, organization, or agency;
- Restrain competition; or
- Prevent or delay the release of information that does not require protection in the interest of the national security.

Basic scientific research information not clearly related to the national security may not be classified.

Access to Classified Information

As stated in EO 13526, a person may have access to classified information provided that:

- A favorable determination of eligibility for access has been made by an agency head or the agency head's designee (i.e., the person has been granted an appropriate security clearance);
- The person has signed an approved nondisclosure agreement; and
- The person has a need-to-know the information.

Review and Release

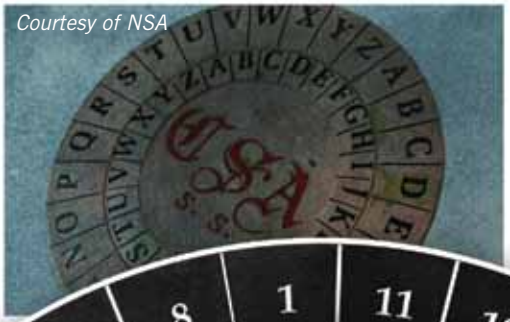
Due to the need to protect the identity of information sources and due to the potential implications of the results of IC analysis, most

intelligence reports are classified. Classification of intelligence reports can limit the customer's ability to use them, particularly when they are interacting with individuals outside the U.S. Government. In recognition of the importance of making intelligence useful to its customers, the IC has established procedures to allow for appropriate release of intelligence. General guidelines for the release of intelligence include the following:

- Some intelligence can be shared through foreign disclosure, some through discretionary release by the IC, and some through the Freedom of Information Act (FOIA) (5 U.S.C. Section 552) with redactions.
  - Different categories of review and release requests are handled differently. Some categories are handled collaboratively with the requestor, while others are handled strictly through internal IC processes.
  - The IC is working to maximize discoverability, by the by the IC and USG, of information and utility of intelligence products.
- The originators of the information will consider many factors, including:
  - The impact of release of the information.
  - The sensitivity and vulnerability of the information source or method.
  - The uniqueness or traceability of the information source.
  - The effect on external relationships.
- Specific wording may determine whether the information is releasable.
  - Less specific language and attributes are more likely to be approved for release.
  - The identification of the information source is often the most sensitive information in a report.
- The intended audience has an impact on the decision.
  - Is the intelligence being released to a federal department, a state police agency, a foreign liaison service, a foreign official, or to the public or news media?
- "Publicly Available" does not necessarily mean "Officially Acknowledged."
- The IC complies with the FOIA as written. 5 U.S.C. Section 552, as amended, provides that any person has the right to obtain access to federal agency records, except to the extent that those records, or portions of them, are protected from public disclosure by one of the nine exemptions allowed under FOIA.

- The IC classifies and declassifies national security information in accordance with EO 13526. Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security.

Organizational Oversight



Courtesy of NSA

The cipher disk is a deceptively simple cryptographic tool invented around 1470 by an Italian architect. Although the tool has been "re-invented" a number of times over the centuries, the basic concept of the cipher disk remains much the same. It consists of two concentric disks marked with letters, numbers, and other symbols around the edge of each disk. The smaller disk, which is mounted on the stationary larger disk, can be moved to create a cryptographic key.

The appeal of the cipher disk lies in the fact that messages can be enciphered and deciphered without the need for bulky or compromising written materials. The cipher disk first came into large-scale use in the United States during the Civil War. About a half-century later, the U.S. Army adopted a version of the device, which used both a standard and a "reverse-standard" alphabet.

The two disks may be left in the same setting to create an entire message, thereby producing the simplest possible cryptogram, or the setting may be changed with every letter of the message to create an extremely secure cipher.

THE CIPHER DISK

Oversight

Joint Intelligence Community Council

The National Security Act of 1947, as amended, establishes the Joint Intelligence Community Council (JICC), which consists of the Director of National Intelligence (DNI) (chair), Secretary of State, Secretary of the Treasury, Secretary of Defense, U.S. Attorney General, Secretary of Energy, and Secretary of Homeland Security. The JICC advises the DNI on establishing requirements, developing budgets, and managing financial matters; assists the DNI in monitoring and evaluating the performance of the Intelligence Community (IC); and ensures the timely execution of programs, policies, and directives established or developed by the DNI. The JICC is the most senior executive body for managing the IC. The JICC typically meets semiannually.

Executive Committee

For more routine management and governance of the IC, the DNI has established the IC Executive Committee (EXCOM), which is chaired by the DNI and composed of the heads of all 17 IC members plus the Under Secretary of Defense for Intelligence, the Joint Chiefs of Staff Director for Intelligence (J-2), the Principal Deputy DNI, and the Deputy DNI for Intelligence Integration. The EXCOM's role is to advise and support the DNI in the leadership, governance, and management of the IC, including advising the DNI on IC policies, objectives, and priorities and ensuring the IC's capability to fulfill its mission.

Deputy Executive Committee

Issues that the EXCOM addresses are often handled by its subordinate body, the IC Deputy

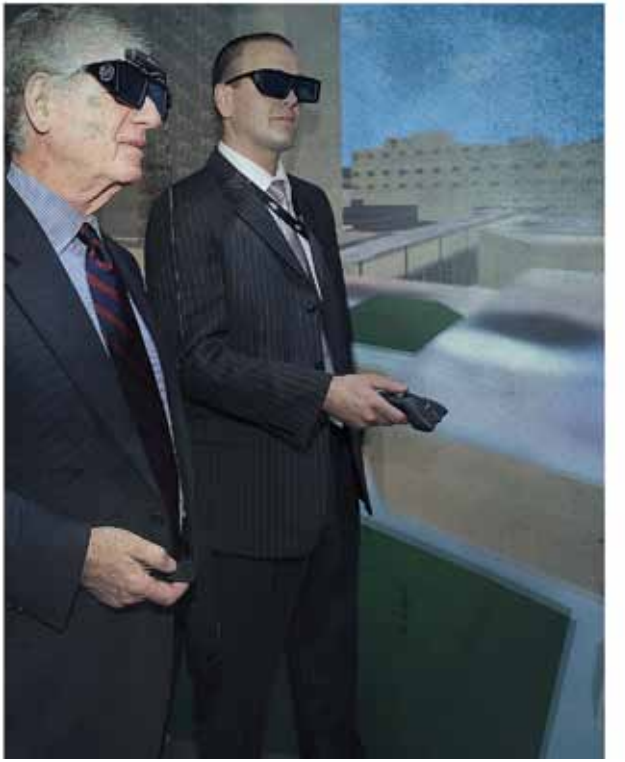
Executive Committee (DEXCOM), which is chaired by the Principal Deputy DNI and is composed of the deputy heads of the 17 intelligence organizations plus the Deputy Under Secretary of Defense for Intelligence, the Deputy Director of Intelligence of the Joint Chiefs of Staff, and the Deputy DNI for Intelligence Integration.

Legislative Oversight

The U.S. Congress has long overseen national intelligence activities. From the 1940s on, the Armed Services Committees and Appropriations Committees of the U.S. House of Representatives and U.S. Senate have exercised responsibility for oversight of national intelligence activities, although those operations were typically discrete and hidden from the public eye.

On May 19, 1976, the U.S. Senate established the Senate Select Committee on Intelligence (SSCI). The U.S. House of Representatives followed suit on July 14, 1977, by creating the House Permanent Select Committee on Intelligence (HPSCI). These committees, along with the Armed Services and the Foreign Relations and Foreign Affairs Committees, were charged with authorizing the programs of the intelligence organizations and overseeing their activities.

The 1980 Intelligence Oversight Act set forth the current oversight structure by establishing



the SSCI and HPSCI as oversight committees for the Central Intelligence Agency (CIA). Within the U.S. Congress, these committees are responsible for producing Intelligence Authorization bills, which proscribe certain activities of the IC. The SSCI also provides advice and consent on the nominations of certain presidentially appointed intelligence officials.

The Appropriations Committees, given their constitutional role to appropriate funds for all

U.S. Government activities, also exercise oversight of intelligence activities. Specifically, the House and Senate appropriations subcommittees for defense produce annual appropriations for national and military intelligence activities via the Defense Appropriations Act.

These authorization and appropriations committees are the principal Congressional recipients of IC products, briefings, notifications, and reprogramming requests. These committees routinely conduct hearings on budgetary and other oversight matters.

Other Congressional committees interact with the IC as needed.

National Security Council

The National Security Council (NSC) was established by the National Security Act of 1947. The NSC is the President's forum for discussion and examination of national security and foreign policy matters with the President's senior national security advisors and cabinet officials. The NSC also serves as the President's principal arm for coordinating foreign policy matters among various government organizations. The NSC is chaired by the President. Its regular attendees (both statutory and non-statutory) include the Vice President, Secretary of State, Secretary of the Treasury, Secretary of Defense, and Assistant to the President for National Security Affairs. The Chairman of the Joint Chiefs of Staff is the statutory military advisor to the NSC, and the Director of National Intelligence is the intelligence advisor to the NSC. The Chief of Staff to the President, Counsel to the President, and Assistant to the President for Economic Policy are invited to attend any NSC meeting. Other senior officials are invited to attend meetings of the NSC as appropriate.

The NSC drafts, coordinates, and approves National Security Presidential Directives (NSPDs), which are instruments for communicating Presidential decisions about U.S. national security policy.

President's Intelligence Advisory Board

The President's Intelligence Advisory Board (PIAB) and Intelligence Oversight Board (IOB) are tasked with providing the President with an independent source of advice on the effectiveness of the IC in meeting the nation's intelligence needs and the vigor and insight of the IC plans for the future. The PIAB provides advice to the President concerning the quality and adequacy of intelligence collection, intelligence analysis and estimates, counterintelligence, and other intelligence activities. Because the PIAB is independent of the IC and free from any day-to-day IC management or operational responsibilities, it is able to objectively render opinions on the sorts of intelligence that will best serve the country and the organizational structure most likely to achieve IC goals.

The IOB, a committee of the PIAB, informs the President of intelligence activities that it believes may be unlawful or contrary to an Executive Order (EO) or presidential directive and that are not being adequately addressed by the Attorney General, the DNI, or the head of a department concerned. The IOB also informs the President of intelligence activities that it believes should be reported to the President immediately.

The PIAB may consist of up to 16 individuals who are not full-time employees of the U.S. Government. The Board has been known as the PIAB since 2008 when the President signed EO 13462. Previously, it was known as the President's Foreign Intelligence Advisory Board (PFIAB) under EO 12863, a predecessor Executive Order.

Office of the Inspector General

The Office of the Inspector General (OIG) conducts independent investigations, audits, inspections, and special reviews of IC programs and activities that are the responsibility of and under the authority of the DNI to detect and deter waste, fraud, abuse, and misconduct, and to promote integrity, economy, efficiency, and effectiveness in the IC. The Inspector General for the IC leads the OIG, chairs the IC Inspectors General Forum, receives and investigates allegations of IC activities constituting a violation of laws, rules, or regulations; mismanagement; gross waste of funds; abuse of authority; or a substantial and specific danger to the public health and safety. The Inspector General for the IC accepts and processes notifications from IC employees or contractors who are intending to report an urgent concern to the U.S. Congress.

Financial Management and Oversight

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) provides the DNI with a significant amount of authority over the IC's budget development and ensuring the effective execution of that budget.

The National Intelligence Program (NIP), formerly known as the National Foreign Intelligence Program (NFIP), provides the resources needed to develop and maintain intelligence capabilities that support national priorities.

The Joint Military Intelligence Program and the Tactical Intelligence and Related Activities program were combined in 2005 to form the Military Intelligence Program (MIP). The MIP funds the specific intelligence needs of the Department of Defense and tactical forces. The MIP is controlled by the Secretary of Defense, and the DNI participates in the development of the MIP.

Equal Employment Opportunity and Diversity

IC EEOD serves as the principal advisor to the DNI and IC senior leaders on issues that impact diversity, inclusion, and equal opportunity across the IC. The Office is responsible for developing, implementing, and measuring performance against the five-year IC EEO and Diversity Strategic Plan and overseeing and setting IC-wide policy guidance for the development and implementation of IC agency and component plans linked to that strategy. The office also advises ODNI and IC senior leaders on highly sensitive, confidential personnel concerns and matters. In addition to its IC-wide responsibilities, IC EEOD is also responsible for providing EEO and diversity services to the ODNI workforce, including managing the EEO complaints process, Alternative Dispute Resolution activities, reasonable accommodations, workplace climate, and behavior interventions.

Aggrieved persons who believe they have been discriminated against must contact an agency EEO counselor prior to filing a formal complaint. The person must initiate counselor contact within 45 days of the matter alleged to be discriminatory.

Civil Liberties and Privacy Office

The Civil Liberties and Privacy Office (CLPO) is responsible for ensuring that civil liberties and privacy protections are appropriately incorporated into the policies and procedures of the IC. The CLPO also reviews, assesses, and investigates complaints and information indicating possible abuses of civil liberties and privacy in the administration of programs or in the operations of the ODNI.

To effectively use the tools and information that are needed for national safety and security, the IC must have the trust of the U.S. public and continually demonstrate that it is worthy of that trust. Through a framework of laws, policies, and oversight and compliance mechanisms, the CLPO works within the entire IC to maintain the public's trust by safeguarding the freedoms, civil liberties, and privacy rights guaranteed to all U.S. persons.

Careers in the Intelligence Community

HURRICANE ASSISTANCE

Courtesy of NGA

During the 2005 Atlantic hurricane season, the most destructive hurricane season on record, the National Geospatial-Intelligence agency responded with what then NGA director, James R. Clapper, called the best work by an intelligence agency that he had seen in his 42 years in the intelligence business.

The NGA's assistance to Hurricane Katrina relief efforts began before the first waves hit the Louisiana shore on August 29, 2005. For first responders and relief organizations, the agency provided scores of graphics depicting the locations of major airports, hospitals, police and fire stations, emergency operations centers, hazardous materials, highways, and schools based on imagery from commercial and U.S. Government satellites and American military airborne platforms.

In the aftermath of Hurricane Katrina and Hurricane Rita, which struck the Gulf Coast of Texas and Louisiana in September 2005, NGA forward-deployed more than two dozen analysts and two Mission Integrated Geospatial-Intelligence Systems (MIGS) to the affected areas to provide timely, on-site support.

THE BENEFITS OF WORKING IN THE IC

The U.S. Intelligence Community offers the following benefits to personnel within the IC and to individuals considering a career within the IC:

- A profession with a meaningful connection to protecting the United States and its citizens.
- Diverse work environments and corporate cultures with all members of the IC working toward a common goal.
- Work opportunities in almost every professional field imaginable.

The IC has been repeatedly recognized as one of the "Best Places to Work in the Federal Government" in an independent analysis sponsored by the Partnership for Public Service and the American University Institute for the Study of Public Policy Implementation (http://bestplacestowork.org/BPTW/rankings/).

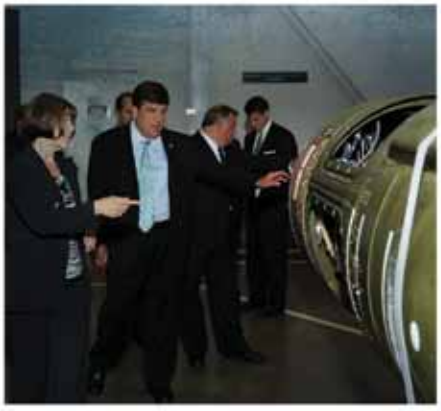
There are multiple pathways into the IC, as the following graphic indicates. Another key pathway is the Intelligence Community Centers of Academic Excellence (CAE) Program (www.dni.gov/cae).

A diverse workforce is critical to the IC's success. An essential component of intelligence is an understanding of people and cultures that differ from those of the United States and knowledge of other areas around the world. As such, the IC seeks individuals of all ages and ethnic backgrounds with diverse skills and educational experiences to fill positions across the IC. Hiring incentives and special pay scales are also available for those with certain foreign language skills, cultural expertise, and other critical skills and experience.

Another pathway to a career with the IC is the IC Wounded Warrior program. Wounded Warriors, many of whom already possess the skills and experience that the IC seeks, are recruited through IC-wide internship fairs and other IC Agency-based initiatives. Wounded Warriors may obtain internships across the IC that lead to full-time employment and an opportunity to serve Agencies that will benefit from their discipline and experience. See www.intelligence.gov/woundedwarrior for more information on the program.

The 17 agencies that form the IC include staffed offices in all 50 states and around the world. The men and women in these offices collect and analyze information, translate foreign-language documents, develop new intelligence technologies, design software and hardware, write reports for the President, manage the IC's people, programs, and processes, and perform many more important activities.

U.S. citizenship is required for employment with the IC. An extensive background investigation, which includes drug screening, must be successfully completed for all job applicants prior to their being hired into the IC. Some positions may also require medical and psychological examination and a polygraph interview. The IC is an Equal Opportunity Employer and is fully compliant with the Americans with Disabilities Act. To find out more about IC careers and employment opportunities, visit www.intelligence.gov.



References

On November 20, 1965, the Central Intelligence Agency completed flight testing on the A-12, the fastest and highest-flying jet aircraft yet to be built. It flew for 74 minutes at 90,000 feet at a sustained speed of Mach 3.2 and a peak speed of Mach 3.29.

The A-12 program (code named "Oxcart") was a successor to the U-2, the CIA's first high-altitude strategic reconnaissance aircraft. The U-2 was built to fly deep inside the Soviet Union, but it was soon vulnerable to Soviet air defenses—a problem demonstrated when the U-2 flown by Francis Gary Powers was downed by a surface-to-air missile. Lockheed Corporation's advanced design facility, nicknamed the "Skunk Works," submitted a design for a new reconnaissance aircraft that would fly too high and too fast to be intercepted by the Soviets.

But by the time the A-12 went into production, Soviet air defenses had advanced enough that even an aircraft flying faster than a bullet at the edge of space would be vulnerable. The CIA successfully deployed the A-12 to Asia, where it flew 29 missions in 1967 and 1968. Eight deactivated A-12s are on display at museums around the United States, and one is at CIA Headquarters.

Courtesy of CIA

CODE NAME "OXCART":
THE SUPERSONIC A-12

Glossary of Terms

A

Access: The means, ability, or permission to approach, enter, or use a resource.

Actionable: (1) Information that is directly useful to customers for immediate exploitation without requiring the full intelligence production process; actionable information may address strategic or tactical needs, support of U.S. negotiating teams, or actions dealing with such matters as international terrorism or narcotics. (2) Intelligence and information with sufficient specificity and detail that explicit responses based on that information can be implemented.

All-Source Intelligence: Intelligence information derived from several or all of the intelligence disciplines, including SIGINT, HUMINT, MASINT, OSINT, and GEOINT.

Analysis: The process by which information is transformed into intelligence; a systematic examination of information to identify significant facts, make judgments, and draw conclusions.

C

Classification: The determination, in the interest of national security, that official information requires a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made; the designation is typically called a "security classification," which includes CONFIDENTIAL, SECRET, and TOP SECRET classification levels.

Collection: The identification, location, and recording and storing of information— typically from an original source and using both human and technological means—for input into the

Intelligence Cycle for the purpose of meeting a defined tactical or strategic intelligence goal.

Communications Intelligence (COMINT): The capture of information, either encrypted or in "plaintext," exchanged between intelligence targets or transmitted by a known or suspected intelligence target for the purpose of tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, or analysis of the substantive meaning of the communication. COMINT is a sub-discipline of SIGINT.

Confidential: A security classification designating information that, if made public, could be expected to cause damage to national security.

Consumer: An authorized person who uses intelligence or intelligence information directly in the decisionmaking process or to produce other intelligence.

Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or their agents, or international terrorist organizations or activities.

Counterterrorism: The practices, tactics, techniques, and strategies adopted to prevent or respond to terrorist threats or acts, both real and suspected.

Covert Action/Operation: Activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of teh United States Government will not be apparent or acknowledges publicly, but does not include activities the primary purpose of which is to aquire intelligence, traditional counterintelligence activities, traditional diplomatic or military activities, or traditional law enforcemnt activities.

D

Deployment: The short-term assignment of personnel to address specific problems or demands related to national security.

E

Electronic Intelligence (ELINT): (1) Information derived primarily from electronic signals that do not contain speech or text (which are considered to be COMINT). (2) Information obtained for intelligence purposes from the interception of electromagnetic non-communications transmissions by other than the intended recipient. The most common sources of this type of information are radar signals. ELINT is a sub-discipline of SIGINT.

Exploitation: The process of obtaining intelligence information from any source and taking advantage of it for intelligence purposes.

F

Foreign Instrumentation Signals Intelligence (FISINT): Information derived from the interception of foreign electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems including, but not limited to, telemetry, beaconry, electronic interrogators, and video data links. FISINT is a sub-discipline of SIGINT.

Freedom of Information Act (FOIA): The Freedom of Information Act, 5 U.S.C. 552, enacted in 1966, statutorily provides that any person has a right, enforceable in court, to access federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions or three exclusions.

Fusion Center: A collaborative effort of two or more agencies that provide resources, expertise, and information to a center with the goal of maximizing the ability to detect, prevent, investigate, and respond to criminal and terrorist activity. State and major urban area fusion centers are recognized as a valuable information-sharing resource. They are the focus, but not exclusive points, within the state and local environments for the receipt and sharing of terrorism information, homeland security information, and law enforcement information related to terrorism.

G

Geospatial Intelligence: Intelligence derived from the exploitation of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth.

H

Homeland Security Information: Any information possessed by an SLTT or federal agency that relates to (1) a threat of terrorist activity; (2) the ability to prevent, interdict, or disrupt terrorist activity; (3) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (4) a planned or actual response to a terrorist act.

I

Imagery Intelligence (IMINT): Intelligence that includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics.

Intelligence Analyst: A professional intelligence officer who is responsible for performing, coordinating, or supervising the collection, analysis, and dissemination of intelligence.

Intelligence Community: A federation of Executive Branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of U.S. national security. These organizations are (in alphabetical order): Air Force Intelligence, Army Intelligence, Central Intelligence Agency, Coast Guard, Defense Intelligence Agency, Department of Defense, Department of Energy, Department of Justice, Department of Homeland Security, Department of State, Department of the Treasury, Office of the Director of National Intelligence, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, and Navy Intelligence.

Intelligence Cycle: The steps through which information is converted into intelligence and made available to users. The cycle typically includes six steps: planning and direction, collection, processing and exploitation, analysis and production, dissemination, and evaluation.

Intelligence Mission: The role that the intelligence function of an agency fulfills in support of the overall mission of the agency; the intelligence mission specifies in general language what the intelligence function is intended to accomplish.

Intelligence Officer: A professional employee of an intelligence organization engaged in intelligence activities.

Intelligence Products: Reports or documents that contain assessments, forecasts, associations, links, and other outputs from the analytic process.

Intelligence Requirement: The need to collect intelligence information or to produce intelligence, either general or specific, on a particular subject.

J

Joint Terrorism Task Force (JTTF): A JTTF is a coordinated "action arm" for federal, state, and local government response to terrorist threats in specific U.S. geographic regions. The FBI is the lead agency that oversees the JTTFs.

M

Measurement and Signature Intelligence (MASINT): Technically derived intelligence data other than imagery and SIGINT. The data results in intelligence that locates, identifies, or describes distinctive characteristics of targets. It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences.

N

National Intelligence: National Intelligence and the term "intelligence related to national security" refer to all intelligence, regardless of the source from which it is derived and including information gathered within or outside the United States that pertains, as determined to be consistent with any guidance issued by the President, to (1) more than one U.S. Government agency and that involves threats to the United States, its people, property, or interests; (2) the development, proliferation, or use of weapons of mass destruction; or (3) any other matter bearing on U.S. national or homeland security. Source: Intelligence Reform and Terrorism Prevention Act of 2004, Section 1012, Public Law 108-458, December 17, 2004.

National Intelligence Council (NIC): The NIC is the IC's council for midterm and long-term strategic thinking. Its primary functions are to support the Director of National Intelligence, provide a focal point for policymakers to task the IC to answer their questions, reach out to nongovernment experts in academia and the private sector to broaden the IC's perspective, contribute to the IC's effort to allocate its resources to policymakers' changing needs, and lead the IC's efforts to produce National Intelligence Estimates and other NIC products.

National Intelligence Estimate (NIE): NIEs are produced by the National Intelligence Council. NIEs express the coordinated assessment of the IC and, thus, represent the most authoritative assessment of the DNI with respect to a particular national security issue. NIEs contain the coordinated judgment the IC regarding the probable course of future events.

O

Open-Source Intelligence (OSINT): Publicly available information appearing in print or electronic form, including information from radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings used to enhance intelligence analysis and reporting.

P

Privacy Act: The Privacy Act of 1974, 5 U.S.C. 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by an individual's name or by some other identifier assigned to the individual. The Privacy Act requires that agencies provide public notice of their systems of records through publication in the Federal Register. The Privacy Act prohibits the disclosure of information from a system of records

absent the written consent of the individual who is the subject of the information search, unless the disclosure is pursuant to one of 12 statutory exceptions. The Privacy Act also provides individuals with a means by which to seek access to and amend their records and sets forth various agency record-keeping requirements.

R

Raw Data: Bits of collected data that individually convey little or no useful information and must be collated, aggregated, or interpreted to provide meaningful information.

Raw Intelligence: A colloquial term meaning collected intelligence information that has not yet been converted into finished intelligence.

S

Secret: Information that, if it is made public, could be expected to cause serious damage to national security.

Signals Intelligence (SIGINT): Intelligence derived from signals intercepts comprising, individually or in combination, all communications intelligence (COMINT), electronic intelligence (ELINT), and/or FISINT.

Source: A document, interview, or other means by which information has been obtained. From an intelligence perspective, sources are individuals (or HUMINT) who collect or possess critical information needed for intelligence analysis.

T

Threat: (1) A source of unacceptable risk. (2) The capability of an adversary coupled with the adversary's intention to undertake actions that would be detrimental to the success of certain activities or operations.

Top Secret: Information that, if it is made public, could be expected to cause exceptionally grave damage to national security.

U

Unauthorized Disclosure: A communication or physical transfer, usually of sensitive but unclassified information or classified information, to an unauthorized recipient.

Unclassified: Information not subject to a security classification; that is, information not classified CONFIDENTIAL, SECRET, or TOP SECRET. Although unclassified information is not subject to a security classification, there may still be limits on its disclosure.

W

Warning: To issue an advance notification of possible harm or victimization following the receipt of information or intelligence concerning the possibility of a crime or terrorist attack.

Acronyms and Abbreviations

A

A2: Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (Air Force)

ADNI/SRA: Assistant Director of National Intelligence for Systems and Resource Analyses

C

CAE: Center of Academic Excellence

CD: Counterintelligence Division

CFO: Chief Financial Officer

CI: Counterintelligence

CIA: Central Intelligence Agency

CIKR: Clinical Infrastructure and Key Resources

CIO: Chief Information Officer

CLPO: Civil Liberties and Privacy Office

COM: Collection Operations Management

CNO: Chief of Naval Operations

CNO: Computer Network Operations

COMINT: Communications Intelligence

CSS: Central Security Service

CR: Collection Request

CRM: Collection Requirements Management

CRWG: Capability Requirements Working Group

CTD: Counterterrorism Division

D

DA: Directorate for Analysis

D/CIA: Director Central Intelligence Agency (formerly DCI)

DCHC: Defense Counterintelligence and Human Intelligence Center

DDII: Deputy Director Intelligence Integration

DDNI: Deputy DNI Director for Intelligence Integration

DDNI/A&T: Deputy DNI for Acquisition and Technology

DEA: Drug Enforcement Administration

DEXCOM: Deputy Executive Committee

DHS: Department of Homeland Security

DI: Directorate of Intelligence

DIA: Defense Intelligence Agency

DIAC: Defense Intelligence Analysis Center

DIRINT: Director of Intelligence

DNI: Director of National Intelligence

DoD: Department of Defense

DoDIIS: Department of Defense Intelligence Information System

DOE: Department of Energy

DS: Directorate for Information Management and Chief Information Officer

DS&T: Directorate of Science and Technology

DT: Directorate for MASINT and Technical Collection

DT: Domestic Terrorism

DTRA: Defense Threat Reduction Agency

E

ELINT: Electronic Intelligence

EO: Executive Order

EXCOM: Executive Committee

F

FBI: Federal Bureau of Investigation

FIG: Field Intelligence Group

FISA: Foreign Intelligence Surveillance Act

FISINT: Foreign Instrumentation Signals Intelligence

FOIA: Freedom of Information Act

FOUO: For Official Use Only

G

GDIP: General Defense Intelligence Program

GEOINT: Geospatial Intelligence

GMII: Global Maritime Intelligence Integration

H

HPSCI: House Permanent Select Committee on Intelligence

HUMINT: Human Intelligence

I

I&A: Office of Intelligence and Analysis (DHS)

IC: Intelligence Community

ICCR: Intelligence Community Capability Requirements

ICD: Intelligence Community Directive (replaces Director of Central Intelligence Directives)

IED: Improvised Explosive Device

IMINT: Imagery Intelligence

IN: Office of Intelligence and Counterintelligence

INR: Bureau of Intelligence and Research (DOS)

INSCOM: Intelligence and Security Command (Army)

IOB: Intelligence Oversight Board

IPPBE: Intelligence Planning, Programming, Budgeting, and Evaluation

IRB: Intelligence Resources Board

IRTPA: Intelligence Reform and Terrorism Prevention Act of 2004

ISR: Intelligence, Surveillance, and Reconnaissance

IT: Information Technology

ITACG: Interagency Threat Assessment and Coordination Group, NCTC

J

J-2: Directorate for Intelligence, Joint Staff Intelligence

JICC: Joint Intelligence Community Council

JTTF: Joint Terrorism Task Force

JWICS: Joint Worldwide Intelligence Communication System

M

MASINT: Measurement and Signatures Intelligence

MCIA: Marine Corps Intelligence Activity

MIP: Military Intelligence Program

MSA: Major System Acquisition

MSIC: Missile and Space Intelligence Center

N

NCIX: National Counterintelligence Executive

NCMI: National Center for Medical Intelligence

NCPC: National Counterproliferation Center

NCS: National Clandestine Service

NCTC: National Counterterrorism Center

NDIC: National Defense Intelligence College

NGA: National Geospatial-Intelligence Agency (formerly NIMA)

NFIP: National Foreign Intelligence Program

NGIC: National Ground Intelligence Center

NIC: National Intelligence Council

NIE: National Intelligence Estimate

NIP: National Intelligence Program

NIS: National Intelligence Strategy

NJTTF: National Joint Terrorism Task Force

NMEC: National Media Exploitation Center

NMIC: National Maritime Intelligence Center

NRO: National Reconnaissance Office

NSA: National Security Agency

NSB: National Security Branch

NSC: National Security Council

NSOC: National Security Operations Center

NSPD: National Security Presidential Directives

NTOC: NSA/CSS Threat Operations Center

NVTC: National Virtual Translation Center

O

ODNI: Office of the Director of National Intelligence

OIG: Office of the Inspector General

ONCIX: Office of the National Counterintelligence Executive

ONI: Office of Naval Intelligence

ONSI: Office of National Security Intelligence

OPNAV N2/N6: Deputy Chief of Naval Operations for Information Dominance

OSC: Open-Source Center

OSINT: Open-Source Intelligence

P

PFIAB: President's Foreign Intelligence Advisory Board

PIAB: President's Intelligence Advisory Board

R

RFI: Request for Information

S

S&T: Science and Technology

SCI: Sensitive Compartmented Information

SIGINT: Signals Intelligence

SLTT: State, Local, Tribal, and Territorial

SSCI: Senate Select Committee on Intelligence

S&T: Science and Technology

T

TIDE: Terrorist Identities Datamart Environment

TSC: Terrorist Screening Center

U

UFAC: Underground Facilities Analysis Center

UGF: Underground Facility

UIS: Unifying Intelligence Strategies

USCG: U.S. Coast Guard

USCG-ICC: U.S. Coast Guard Intelligence Coordination Center

USD(I): Undersecretary of Defense for Intelligence

U/SIA: Under Secretary for I&A

USMC: U.S. Marine Corps

W

WMD: Weapons of Mass Destruction

WMDD: Weapons of Mass Destruction Directorate

Resources

ORGANIZATION	URL	DESCRIPTION
IC Agency Web Sites		
Air Force ISR (Intelligence, Surveillance, and Reconnaissance) Agency	http://www.afisr.af.mil	■ General office information ■ News, press releases, and videos ■ Links to career and internship opportunities
Central Intelligence Agency	http://www.cia.gov	■ General office information and information on CIA mission ■ Policy and appointment updates ■ Congressional testimony–related links ■ News, press releases, videos, and CIA World Fact Book ■ Links to career and internship opportunities and descriptions of the CIA organizational culture
Defense Intelligence Agency	http://www.dia.mil	■ General office information and information on the DIA mission and Defense Intelligence Enterprise strategy ■ Policy and appointment updates ■ Congressional testimony–related links ■ News, press releases, and videos ■ Links to career and internship opportunities (within dia.mil site) and descriptions of the DIA organizational culture
Federal Bureau of Investigation	http://www.fbi.gov	■ General office information, FBI overview, and overview of Directorate of Intelligence ■ Policy and appointment updates ■ Congressional testimony–related links ■ News, press releases, and videos ■ Links to career and internship opportunities

ORGANIZATION	URL	DESCRIPTION
IC Agency Web Sites		
National Geospatial-Intelligence Agency	http://www.nga.mil	■ General office information and information on NGA mission and strategic intent ■ Policy and appointment updates ■ Congressional testimony–related links ■ News, press releases, and videos ■ Links to career and internship opportunities
National Reconnaissance Office	http://www.nro.gov	■ General office information and information on NRO mission ■ News, press releases, and videos
National Security Agency/ Central Security Service	http://www.nsa.gov	■ General office information and information on NSA/CSS mission and strategic plan ■ Policy and appointment updates ■ Congressional testimony–related links ■ News, press releases, and video transcripts ■ Links to career and internship opportunities
Office of the Director of National Intelligence	http://www.dni.gov	■ General ODNI information, ODNI mission information, and U.S. National Intelligence Strategy ■ Policy and appointment updates ■ Congressional testimony–related links ■ News, press releases, and speeches ■ Links to information on ODNI careers, internships, scholarships, and other such opportunities
U.S. Army Intelligence and Security Command	http://www.inscom.army.mil	■ General office information ■ News, press releases, and videos ■ Links to career and internship opportunities
U.S. Coast Guard, U.S. Department of Homeland Security	http://www.uscg.mil	■ General office information ■ News, press releases, and videos ■ Links to career and internship opportunities
U.S. Department of Energy	http://www.energy.gov	■ General office information and DOE Directives ■ Policy and appointment updates ■ Congressional testimony–related links ■ News, press releases, and videos ■ Links to career and internship opportunities

ORGANIZATION	URL	DESCRIPTION
IC Agency Web Sites		
U.S. Department of Homeland Security	http://www.dhs.gov	■ General office information and information on DHS mission and DHS strategic plan ■ Policy and appointment updates ■ Congressional testimony–related links ■ News, press releases, and videos ■ Links to career and internship opportunities
U.S. Department of State	http://www.state.gov	■ General office information and information on the State Department mission ■ Policy and appointment updates ■ Congressional testimony–related links ■ News, press releases, and videos ■ Links to career and internship opportunities
U.S. Department of the Treasury	http://www.treasury.gov	■ General information and information on the Department of the Treasury mission and U.S. economic strategy ■ Policy and appointment updates ■ Congressional testimony–related links ■ News, press releases, and other information resources ■ Links to career opportunities
U.S. Drug Enforcement Administration	http://www.justice.gov/dea	■ General office information and information on DEA mission ■ Policy and appointment updates ■ Congressional testimony–related links ■ News, press releases, videos, and news and information on the Drug Enforcement Administration Museum and Visitors Center ■ Links to career and internship opportunities and descriptions of the DEA organizational culture
U.S. Marine Corps, U.S. Marine Corps Forces Special Operations Command, Marine Special Operations Intelligence Battalion	http://www.usmc.mil/unit/marsoc/msoib	■ General office information ■ News, press releases, and videos ■ Links to career and internship opportunities
U.S. Navy, Office of Naval Intelligence	http://www.oni.navy.mil	■ General office information ■ News, press releases, and videos ■ Links to career and internship opportunities

ORGANIZATION	URL	DESCRIPTION
IC Employment Websites		
Central Intelligence Agency	https://www.cia.gov/careers	Identifies career opportunities and career paths within the CIA
Defense Intelligence Agency	http://www.dia.mil/careers	The DIA's "Employment Headquarters" website
Federal Bureau of Investigation	http://www.fbijobs.gov	Highlights the FBI's featured opportunities and other news as well as links to information on FBI career paths
FBI Language Services: Contract Linguists	http://fbijobs.gov/ling/	Contains postings specifically on FBI contract linguist opportunities
National Geospatial-Intelligence Agency	http://erecruit.nga.mil	Identifies current career opportunities at the NGA
National Security Agency/ Central Security Service	http://www.nsa.gov/careers	Identifies current NSA career opportunities and the benefits of working at the NSA/CSS
National Virtual Translation Center	http://www.nvtc.gov	Provides answers to pertinent FAQs related to employment at the NVTC
Office of the Director of National Intelligence (Intelligence.gov)	http://intelligence.gov/careers-in-intelligence/	Highlight the diverse careers that the IC offers and the type of talent needed across the IC
U.S. Air Force	http://www.airforce.com/joining-the-air-force/officer-overview/	Provides an overview of the requirements to become an Air Force officer
U.S. Army Intelligence and Security Command	http://www.inscom.army.mil/Employment/Defaultjobs.aspx	Provides links to USAJobs.gov and Army-specific sites for current employment opportunities
U.S. Coast Guard, U.S. Department of Homeland Security	http://www.uscg.mil/top/careers.asp	Identifies current career opportunities and the benefits of working for the Coast Guard as officer, enlisted, reserve, civilian, or auxiliary personnel
U.S. Department of Energy	http://jobs.energy.gov/	A career information portal that enables users to search for DOE opportunities through the USAJobs website.
U.S. Department of Homeland Security	http://www.dhs.gov/xabout/careers	Identifies current DHS career opportunities and the benefits of working at the DHS
U.S. Department of State	http://careers.state.gov	Identifies the career opportunities within the State Department
U.S. Department of the Treasury	http://www.treasury.gov/careers	Identifies career opportunities at the Department of the Treasury headquarters and at the individual Treasury bureaus
U.S. Drug Enforcement Administration	http://www.justice.gov/dea/resources/job_applicants.html	Identifies career opportunities within the DEA

ORGANIZATION	URL	DESCRIPTION
IC Employment Websites		
U.S. Office of Personnel Management (USAJobs.gov)	http://usajobs.gov/	Highlight the diverse careers that the IC offers and the type of talent needed across the IC
U.S. Marine Corps	http://www.marines.com http://officer.marines.com	Provides an overview of opportunities as enlisted or officer personnel
U.S. Navy Department of the Navy Civilian Human Resources Office of Naval Intelligence "Hot Vacancies" Office of Naval Intelligence "Military Duty at ONI"	http://www.donhr.navy.mil/ http://www.oni.navy.mil/Join_Us/hot_jobs.htm http://www.oni.navy.mil/Join_Us/Military_duty.htm	Naval civilian HR and ONI job-search sites

Laws and Policies Governing the IC

Office of the Director of National Intelligence
Office of General Counsel
Legal Reference Book

The Constitution Of The United States Of America

National Security Act Of 1947

Intelligence Reform And Terrorism Prevention Act Of 2004*

Central Intelligence Agency Act Of 1949

National Security Agency Act Of 1959

Department Of Defense Title 10 Authorities

National Imagery And Mapping Agency Act Of 1996

Homeland Security Act Of 2002*

Counterintelligence And Security Enhancements Act Of 1994

Counterintelligence Enhancement Act Of 2002

Classified Information Procedures Act

Foreign Intelligence Surveillance Act Of 1978

Protect America Act Of 2007

Usa Patriot Act Of 2001*

Usa Patriot Improvement And Reauthorization Act Of 2005*

Detainee Treatment Act Of 2005

Military Commissions Act Of 2006

Freedom Of Information Act

Privacy Act

Federal Information Security Management Act

Inspector General Act Of 1978

War Crimes Act Of 1996

Interception Of Wire, Electronic, And Oral Communications

Implementing Recommendations Of The 9/11 Commission Act Of 2007*

Executive Order 12139

Executive Order 12333

Executive Order 12949

Executive Order 12951

Executive Order 12958

Executive Order 12968

Executive Order 13354

Executive Order 13355

Executive Order 13388

Executive Order 13462

Executive Order 13467

Executive Order 13491

Executive Order 13492

Executive Order 13493

Intelligence Sharing Procedures For Foreign Intelligence And Foreign Counterintelligence Investigations Conducted By The Fbi

Guidelines For Disclosure Of Grand Jury And Electronic, Wire, And Oral Interception Information Identifying United States Persons

Guidelines Regarding Disclosure To The Director Of Central Intelligence And Homeland Security Officials Of Foreign Intelligence Acquired In The Course Of A Criminal Investigation

Guidelines Regarding Prompt Handling Of Reports Of Possible Criminal Activity Involving Foreign Intelligence Sources

The Attorney General's Guidelines For Domestic Fbi Operations

Strengthening Information Sharing, Access, And Integration B Organizational, Management, And Policy Development Structures For Creating The Terrorism Information Sharing Environment

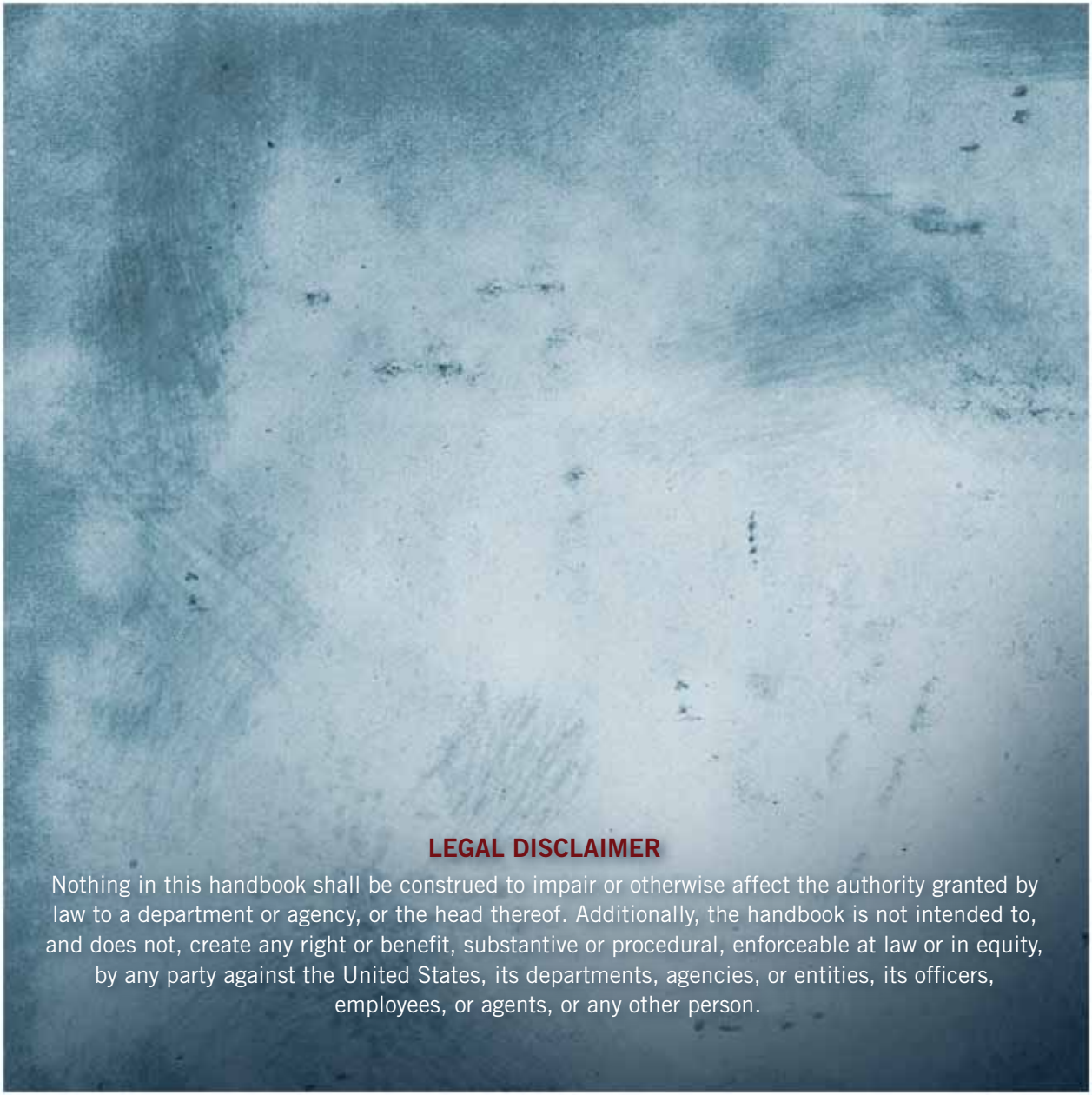
Guidelines To Ensure That The Information Privacy And Other Legal Rights Of Americans Are Protected In The Development And Use Of The Information Sharing Environment

Criteria On Thresholds For Reporting Intelligence Oversight Matters

Mou: Reporting Of Information Concerning Federal Crimes

Intelligence Community And Government Websites

Subject Index



LEGAL DISCLAIMER

Nothing in this handbook shall be construed to impair or otherwise affect the authority granted by law to a department or agency, or the head thereof. Additionally, the handbook is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.


WWW.DNI.GOV