Director of Central Intelligence

The 2002 Annual Report of the United States Intelligence Community

January 2003

DIRECTOR OF CENTRAL INTELLIGENCE

On behalf of the President, I am pleased to submit *The 2002 Annual Report of the United States Intelligence Community*. Throughout 2002, the US Intelligence Community has been at work in a dangerous and dynamic environment. From fighting terrorism to finding weapons of mass destruction, we have focused on converging threats and the social, economic, and political tensions that fuel them.

The Intelligence Community is meeting this convergence of threats with an essential mix of both urgency and longer-term vision. As we continue our relentless offensive effort to disrupt and destroy terrorist groups around the globe, we are working in close coordination with domestic agencies to protect Americans here at home. These efforts complement our Community's constant monitoring and analysis of events and trends throughout the world.

The past year has also reminded us of the vulnerabilities of our free and open society. Our continuing work to enhance security has a single aim: to protect the vital liberties our nation was founded to uphold. Consistent with that objective, new technology is being applied in creative and highly effective ways, and institutional and procedural barriers that impede communication and collaboration are being addressed aggressively.

Most importantly, we are building up our greatest resource: our people. The Intelligence Community is hiring talented, dedicated Americans to join an extraordinary work force with an extraordinary mission—tackling the challenges posed by the pressing intelligence problems of this new century. We will face many of those problems in partnership with the new Department of Homeland Security, as it builds bridges between the Law Enforcement and Intelligence Communities. We will fully support that department by sharing information and by providing connectivity and training.

The men and women of the Intelligence Community are making profound and lasting contributions to our national security. I appreciate this opportunity to share their efforts with Congress and the American people.

George J. Tenet

[CIA Homepage] [Publications Page] [DCI Annual Report Main Page] [Next]

Congressional Tasking

This report, along with its classified annex, fulfills the requirement for an annual report as stated in the Intelligence Authorization Act for Fiscal Year 1997, Sections 109(a) and 105(d) of the National Security Act of 1947, as amended.

Section 109(a):

> *(1) Not later than January 31 each year, the President shall submit to the appropriate congressional committees a report on the requirements of the United States for intelligence and the activities of the Intelligence Community.*
>
> *(2) The purpose of the report is to facilitate an assessment of the activities of the Intelligence Community during the preceding fiscal year and to assist in the development of a mission and a budget for the Intelligence Community for the fiscal year beginning in the year in which the report is submitted.*
>
> *(3) The report shall be submitted in unclassified form but may include a classified annex.*

Section 105(d):

> *The DCI, in consultation with SecDef and Chairman of Joint Chiefs of Staff, shall submit each year to the Committee of Foreign Intelligence of the National Security Council and to the appropriate congressional committees an evaluation of the performances and the responsiveness of the NSA, NRO, and NIMA in meeting their national missions.*

[CIA Homepage] [Publications Page] [DCI Annual Report Main Page] [Next]

Scope

The Director of Central Intelligence (DCI) *FY2002 Annual Report of the United States Intelligence Community* provides insight into the activities and accomplishments of the Intelligence Community (IC). The mission of the Intelligence Community is to provide policymakers, military commanders, and law enforcement officials with timely, accurate intelligence on a wide range of national security issues. Within this context, sources and methods must be protected. Therefore, this report acknowledges only a small fraction of the total contribution made by the men and women of the Intelligence Community.

This report, which is unclassified, addresses accomplishments of the Intelligence Community measured against the national security missions. A *Classified Annex* to the *Annual Report* provides additional detail and is provided to the Congressional Intelligence, Appropriations, and Armed Services Committees.

[CIA Homepage] [Publications Page] [DCI Annual Report Main Page] [Next]

Introduction

The past year, one of dynamic challenge throughout the world, has intensively focused the US Intelligence Community[1] on a dramatically increased threat environment. While Americans recovered from the dramatic terrorist attacks on 11 September, the Intelligence Community responded to changing priorities with speed, skill, and strength.

This year's annual report to Congress first highlights the contribution of the Intelligence Community in responding to the violent acts of terror perpetrated against the United States by al-Qa'ida and those who would follow in its footsteps. The IC played a critical role in supporting Operation ENDURING FREEDOM and is actively contributing to the homeland security mission. Our number one priority is clear: win the global war against terrorism. Reflecting this priority, this year's report opens with a new section: "Support to the War on Terrorism and Homeland Security."

Terrorism, however, represented only one of many complex threats to our national security last year. Strategic issues, including those involving weapons of mass destruction and the increasing capability of states of concern to deliver them, continued to require our most sophisticated collection and analysis. Support to military operations demanded increasing IC attention as we prosecuted a new type of warfare. In addition, support to law enforcement and to countering foreign intelligence gained even greater importance than heretofore and required maximum cooperation and coordination among the several agencies and activities of the Community.

We must be clear about these threats, building upon our past efforts to prepare for the future. The concluding section of this year's report outlines several imperatives for the IC. They give direction to the IC's mandate to serve our country with resolve in time of war or uncertainty and to protect our dominance in worldwide intelligence collection and analysis. The topics addressed by these imperatives are all discussed in this report.

The accomplishments described in the following pages represent only a small sampling of the achievements of the men and women of the IC, but are representative of the many classified successes over the past year. They clearly demonstrate the extraordinary courage, commitment, and creativity of our intelligence professionals, and reflect the high standards and finest traditions of the US Intelligence Community.

[1] The Intelligence Community (IC) is composed of the Central Intelligence Agency (CIA), the National Security Agency (NSA), the National Reconnaissance Office (NRO), the Defense Intelligence Agency (DIA), the National Imagery and Mapping Agency (NIMA), The Department of State Bureau of Intelligence and Research (INR), as well as the intelligence units of the Departments of Treasury, Justice, and Energy and the intelligence elements of the Army, Navy, Air Force, Marine Corps, and Coast Guard.

[CIA Homepage] [Publications Page] [DCI Annual Report Main Page] [Next]

Support to the War on Terrorism and Homeland Security

Make no mistake: despite the battles we have won in Afghanistan, we remain a nation at war.

George J. Tenet
Director of Central Intelligence
Testimony Before the Senate Select
Committee on Intelligence
February 6, 2002

The Intelligence Community provided critical support to the Global War on Terrorism, Operation ENDURING FREEDOM, and Homeland Security. New lines of communication and collaboration were opened between the IC and the Law Enforcement and Counterintelligence Communities. The IC built upon longstanding foreign partnerships and established new partnerships to aid in the War on Terrorism. All elements of the IC brought greater emphasis to issues of counterterrorism and homeland security, focusing on producing actionable intelligence and timely warning in support of military forces and law enforcement.

Countering al-Qa'ida and the Worldwide Terrorist Threat

- Central Intelligence Agency (CIA) officers worked with foreign intelligence services to detain more than 2,900 al-Qa'ida operatives and associates in over 90 countries. A CIA recruit provided intelligence on an al-Qa'ida operative who was planning an impending terrorist operation using shoes to conceal weapons. This report resulted in the issuance of an FAA warning prior to the incident on Flight AA63 and the arrest of alleged "shoe-bomber" Richard Reid.

- CIA officers and Federal Bureau of Investigation (FBI) agents supported the Greek National Police arrest of Alexandros Yiotopoulos, the founder of the 17 November terrorist organization. Following that arrest, the Air Force Office of Special Investigations (AFOSI), FBI, Greek National Police, and New Scotland Yard initiated a joint investigation. The investigation focused on determining the identities of the group's members and why they carried out assassinations and other terrorist attacks against US Air Force and Army personnel. Safehouses used by 17

November contained weapons, rockets, grenades, communications equipment, and other evidentiary items. To date, the Greek National Police have arrested fourteen individuals and trial preparations are underway in Athens. FBI, CIA, AFOSI and Greek Police are collaborating to close out one murder and three attempted murder investigations.

- CIA supported the Greek Government in preparations to provide security at the 2004 Olympic Games by training government officials and analyzing the terrorist challenge in the region.

- CIA, with FBI and the Department of Defense (DoD), devised a campaign of coordinated raids on several al-Qa'ida-affiliated nongovernmental organizations (NGOs) that led to the indictment and arrest of at least one group leader.

- The Treasury Department played a major role in targeting and dismantling terrorist financial networks through such mechanisms as the inter-agency Foreign Terrorist Asset Tracking group, the international Financial Action Task Force, and others. Treasury's Operation GREEN QUEST, which drew upon the expertise of the US Customs Service (USCS), the Internal Revenue Service, the Secret Service, the FBI, and other agencies including the CIA, investigated terrorist financing. Treasury's Office of International Affairs worked with other countries to maintain and expand international efforts to choke off terrorist funds. The Office of Foreign Assets Control worked with other federal, state, local and international entities to implement a strong regime of blocking actions, fund freezes, and other initiatives to derail terrorist financing structures.

- Treasury's Financial Crimes Enforcement Network (FinCEN) operated as an information conduit between law enforcement and financial institutions to disseminate information relating to suspected terrorists and money launderers. FinCEN established a secure network to permit, among other things, the filing of Bank Secrecy Act reports over the Internet, and to put this information into law enforcement databases.

- The FBI's Terrorist Financing Operations Section, created during FY 2002, participated in the effort to target NGOs believed to provide financial support to known foreign terrorist organizations and affiliated terrorist cells. The joint efforts targeting al Barakaat, the Holy Land Foundation for Relief and Development, the Global Relief Foundation, and the Benevolence International Foundation resulted in the execution of numerous search warrants and the disruption of the fund-raising and money remittance operations of these organizations. Financial investigations of these entities have revealed that approximately $200 million in contributions passed through these organizations each year.

- In the aftermath of the 11 September terrorist attacks, every Department of State Bureau of Intelligence and Research (State/INR) office added terrorism to their regular portfolios in ways that enabled State/INR to continue to provide global coverage while uncovering and examining terrorist-related developments in every country and region. State/INR continued to manage and maintain the TIPOFF database of known and suspected terrorists. Efforts were made to increase the information available in the database and make this information available to other agencies. This has contributed to improved interagency information sharing.

- US Central Command (USCENTCOM) implemented a collaborative capability through the Joint Worldwide Intelligence Communications System (JWICS) to support the Global War on Terrorism by:
    - Establishing over 1,600 information work space accounts to increase information sharing.
    - Enabling the coordination of time-sensitive targeting and collection requirements.
    - Providing greater situational awareness to USCENTCOM Headquarters, components, supported Combatant Commands, other intelligence organizations, and 43 coalition partners.
- The Office of Naval Intelligence (ONI) conducted all-source analysis on al-Qa'ida maritime logistics networks in the Middle East, East Africa, and the Mediterranean and developed extensive intelligence on the companies, ships, individuals, organizations, and infrastructure involved in legitimate and illicit maritime activities. A wide range of products was published on terrorist-related shipping, including the daily locations of ships suspected of supporting terrorist groups.
- In the aftermath of the attacks on New York and Washington, the National Intelligence Council (NIC) brought together outside experts and members of the US Intelligence Community for a series of sessions aimed at mitigating surprise in the wake of the 11 September attacks and identifying potential new or emerging terrorist threats.
- Following the overthrow of the Taliban and the convening of an international conference on the political reconstruction of Afghanistan, the NIC coordinated analysis from across the Intelligence Community on the prospects for the country during its transitional administration.
- The NIC sponsored a conference that examined the impact of events in Afghanistan since 11 September on a variety of regional actors, including Russia, Iran, Turkey, India, Europe, Pakistan, and Central Asian states. The conference brought together government and outside experts to exchange views on this issue. The NIC produced an unclassified report, *Afghanistan and Regional Dynamics after 11 September*, summarizing the discussions.
- In response to the 11 September attacks, the Department of Energy (DOE) Office of Counter Intelligence (OCI) and Office of Defense Nuclear Counter Intelligence (ODNCI) formed the Headquarters Counterterrorism Team to evaluate and respond to potential threats of terrorism against DOE facilities, personnel, and information. The CT Team regularly disseminated to field personnel intelligence reporting that detailed any terrorist threats to, or interest in, DOE facilities and personnel.
- The National Security Agency (NSA) increased hiring to maintain a heightened operations tempo, accelerated development and implementation of advanced analytic tools and systems, and bought and built better processing systems—all of which enable NSA to "hunt" for the Nation's adversaries. After the 11 September attacks, NSA received approximately 83,000 resumes and

hired 820 new full-time employees in FY2002. NSA also utilized the largest number of retired NSA civilians in its history, bringing thousands of years of experience across a wide range of technical and analytical areas to bear in the war on terrorism.

Operation ENDURING FREEDOM

- The Joint Captured Materiel Exploitation Center (JCMEC) supported the theater commander in Afghanistan by providing technical intelligence for force protection issues raised by the soldiers in the field. The JCMEC also satisfied national intelligence requirements by collecting foreign materiel from the theater and transporting the materiel back to the United States for detailed exploitation. The JCMEC recovered foreign materiel estimated to be worth $40M, and the in-theater teams have helped recover additional materiel to satisfy IC and explosive ordnance disposal requirements.

- DIA, as the Intelligence Community lead for document exploitation, in collaboration with CIA, NSA, and FBI, established an Intelligence Community Document Exploitation Center as the primary exploitation node outside the Afghan theater of operations for all captured documents related to the Global War on Terrorism. The center has the capability to scan, screen, and process high volumes of original documents as well as those copied from magnetic media.

- As Afghan detainees were moved to Guantanamo Bay, the Defense HUMINT Service (DHS) deployed the first interrogation team to support the activities of US Southern Command's Joint Task Force-170 at Camp X-Ray. A six-person team reported within 48 hours and assessed the first 158 detainees. The team produced over 1,000 intelligence reports.

- DIA printed more than 75,000 copies of country handbooks on Afghanistan for deployed forces engaged in Operation ENDURING FREEDOM; received, processed, and posted 68,570 HUMINT intelligence information reports, with 25,000 digitized linked enclosures; and, in 72 hours, rapidly reformatted and disseminatedgeospatial operational supportpackages for tactical operations. These packageswere used to track and monitorpotential escape routesof al-Qa'ida troops and leaders.

- National Imagery and Mapping Agency (NIMA) analysts have been deployed throughout the USCENTCOM area of responsibility for Operation ENDURING FREEDOM. NIMA provided environmental assessments on troop deployment areas and addressed such humanitarian issues as the location and movement of refugees and displaced persons within Afghanistan and surrounding countries.

- USCENTCOM and DIA developed and provided precise targeting information on al-Qa'ida and Taliban facilities and forces. This information was used by combined military strike assets during Operations ANACONDA and ENDURING FREEDOM.

- NIMA provided extensive targeting support and conducted battle damage assessments in support of Operation ENDURING FREEDOM. NIMA analysts created critical geospatial intelligence databases for key areas affected by the war on terrorism. They analyzed the activities of al-Qa'ida

and the Taliban and provided assessments of installations and equipment associated with key Taliban ground force units.

- CIA worked with the military services throughout Operation ENDURING FREEDOM to deny Usama Bin Laden and al-Qa'ida the use of Afghanistan as a terrorist sanctuary. CIA provided force-protection support and intelligence that was used in planning for military counterterrorism operations, transported US and NATO forces into combat areas during Operation ANACONDA, deployed modified Global Positioning Systems to identify al-Qa'ida and Taliban locations, supported rescue operations, and established a supply pipeline and coordinated the delivery of weapons and ammunition into Afghanistan.

- CIA's assessments of the military strength of Taliban and Northern Alliance forces was used to plan battles and assess enemy strength, as well as to plan the successive phases of the military campaign.

- The Joint Staff Director for Intelligence, the DIA J2, established the Global War on Terrorism/Operation ENDURING FREEDOM Intelligence Task Force to provide actionable intelligence for combat operations in Afghanistan.

- In response to Operations NOBLE EAGLE and ENDURING FREEDOM, DIA initiated the largest reserve mobilization in the history of the agency. DIA mobilized over 500 intelligence officers and enlisted specialists to locations across the country and around the world to take part in the Global War on Terrorism.

- NSA deployed civilian and military analysts worldwide in support of Operation ENDURING FREEDOM.

- The Defensive Information Operations Group at NSA provided round-the-clock monitoring of USCENTCOM unencrypted (and, therefore, vulnerable to intercept by unauthorized persons) communications, strengthening operational security for ENDURING FREEDOM activities. Using feedback and recommendations from NSA's monitoring, USCENTCOM reduced its sensitive information disclosure rate 90 percent in three months.

Mustering for Homeland Security

- The DCI created the Office of Associate DCI for Homeland Security to serve as the IC focal point on issues of intelligence support to homeland security.

- On October 30, 2001, the President directed the creation of the Foreign Terrorism Tracking Task Force (FTTTF) within the Department of Justice under the administrative control of the FBI Counterterrorism Division. The mission of the FTTTF is to keep foreign terrorists and their supporters out of the United States by providing critical and timely information related to entry denial and removal as well as the identification and location of known and suspected terrorists. During FY2002, the FTTTF was involved in a number of specific projects to fill gaps in existing

efforts relating to foreign terrorists and their supporters. The FTTTF engaged in projects to:

- Maintain a unified, unclassified Consolidated Tracking List.
- Identify foreign terrorists and their supporters who have entered undetected or seek to enter the United States or its territories.
- Detect indications of violations of criminal or immigration law which would permit exclusion, detention, or deportation of such individuals.
- Co-locate critical law enforcement, intelligence, and open source data for analysis and decisionmaking support.

- Following the terrorist attacks of 11 September, FBI compiled what became known as the Project Lookout Watch List. Subsequently, FBI established a permanent Terrorism Watch List (TWL) to serve as the single, integrated listing of individuals of investigative interest that will be accessible throughout the Law Enforcement and Intelligence Communities. The TWL is a compendium of names based on information identified through FBI investigations, IC and DoD reporting, as well as information provided by cooperating foreign governments. The TWL will assist both the intelligence and the law enforcement communities in their investigations of terrorist groups and individuals and alert IC officers and law enforcement agents should a person of interest in a terrorism matter be encountered by another agency.

- DIA analysts exploited documents found in Afghanistan and developed additional insight into the infrastructure of al-Qa'ida's biological warfare (BW) efforts. These analysts worked with counterproliferation, counterterrorism and special investigative elements of the FBI to support the monitoring and neutralization of potential scientific contributors to that al-Qa'ida BW infrastructure. Additionally, DIA's *Biological and Chemical On-line Repository of Technical Holdings* (BACWORTH) database has assisted FBI and other law enforcement personnel in understanding BW and CW threats. For example, BACWORTH has provided FBI with data related to anthrax lethal doses and has served as the foundation of law enforcement's own BW and CW databases.

- DIA addressed chemical, biological, radiological, nuclear and missile (CBRN&M) threats through multi-layered analysis of national-level proliferation networks. The multi-layered analysis approach has been expanded to include sub-national and terrorist entities, and is involved in identifying vulnerabilities plus points-of-leverage-and-influence in foreign CBRN&M programs. Assessments helped identify attempts by non-state groups to obtain CBRN&M equipment and their associated technologies, and helped to identify linkages that could be exploited to stop those transactions.

- As an outgrowth of its leadership in the intelligence community in the forecasting of future technology impacts related to global security trends, DIA created the Disruptive Technology Innovative Partnership (DTIP) with participation from the UK, Canada and Australia as well as all elements of the US Intelligence Community. DTIP will provide integrated forecasts of foreign

state and non-state capabilities stemming from innovative applications of both mature and emerging technologies. DTIP's focused on terrorism-related issues and it is working with officials at DoD, Homeland Security (Critical Infrastructures), Law Enforcement, Finance/Banking, and Transportation to focus on potential targets, attack modes, and attack means. Additionally, DTIP works with the primary intelligence producers to broaden and sharpen collection requirements.

- DIA prepared a special assessment of the cyber threat to National Airspace System networks at the request of the Federal Aviation Administration (FAA). DIA also participated in the Network Security Information Exchange, a partnership of government, industry and network security professionals that promotes exchanges of information to enhance computer network and public telephone switched network security and improve critical infrastructure protection. This is a key security issue because much of the DoD information infrastructure rides on the public switched network.

- The Air Force Eagle Eyes program, introduced in FY2002, represents a new awareness methodology, where AFOSI draws upon the entire Air Force military and civilian community to detect and deter terrorism. Eagle Eyes conveys raw information that does not meet formal reporting standards but is deemed to be of interest. As an outgrowth of the Eagle Eyes program, the AFOSI Homeland Security Analysis Office published a weekly product entitled Eagle Vision, a compilation of articles analyzing Homeland Security threat information which also served as a liaison tool to help bridge the gap between the DoD Counterintelligence (CI) community and local law enforcement.

- ONI began assessing the probability of terrorists using ships as a means of delivering WMD that could be detonated or designed to release toxic chemicals or biological agents. ONI evaluated over 40 hazardous chemicals identified by the US Coast Guard (USCG) to determine their potential for explosion, fire, or toxic release. Based on a model developed by ONI, the Coast Guard can quickly evaluate the threat posed by these chemicals and has taken increased precautions prior to permitting ships containing hazardous materials to enter US ports.

- Over 1,000 Navy Reserve intelligence personnel were mobilized for active participation in the war on terrorism. Mobilized Navy Reserve Intelligence personnel who are skilled in analysis of merchant marine shipping activities provided valuable support to US port and harbor security operations. Additionally, many analysts provided direct intelligence support to border patrol efforts, counterdrug operations, and counterterrorism activities.

- The USCG Intelligence Program provided the Joint Interagency Task Force—Counterterrorism (JITF-CT) a dedicated maritime threat analysis cell that supports Homeland Security. As the JITF-CT maritime security element, this cell researched, analyzed, and produced finished intelligence products addressing maritime-related threats of concern to US intelligence and law enforcement officials.

- The USCG Intelligence Program, DIA, and NIMA are enhancing situational awareness of the Captains of the Port (the senior Coast Guard officers assigned to US ports) with commercial high-

resolution satellite imagery of maritime areas of interest.

- CIA initiated collaboration with medical officers from the White House, the Capitol, NSA, FBI, Department of State (DoS) and the Department of Health and Human Services Office of Emergency Preparedness to coordinate a US Government response to the potential threat of chemical and biological warfare. On the local level, in Virginia CIA also initiated information sharing meetings with the Arlington County-based National Medical Response Team and Fairfax County emergency medical personnel.

- CIA provided information to interagency teams responsible for security at the 2002 Salt Lake City Winter Olympics.

- CIA briefed the President and his Cabinet on the worldwide smallpox threat, providing analysis that is helping to drive the US Government smallpox vaccination policy. A series of technical assessments on smallpox provided to senior policymakers helped determine the USposition on worldwide destruction of smallpox virus.

- CIA officers, in collaboration with the National Science Foundation, formed an intragovernmental committee to formalize cooperation in the genetic sequencing of pathogens that could be used as biological weapons. A National Interagency Genomics Sciences Coordinating Committee was established to guide the interagency sequencing work.

- The NIC provided extensive briefings on the development of biological weapons capabilities by potential adversaries—particularly important after the anthrax attacks in the United States—and also briefed on cyber threats to the United States. The NIC coordinated an Intelligence Community assessment that focused on the threats and individual capabilities posed by terrorist use of cyber space.

- NSA established a Homeland Security Support Office to develop and coordinate NSA's Homeland Security Strategy and to identify SIGINT and information assurance capabilities, products and services for supporting the National Homeland Security Strategy. The new support office immediately detailed people to the Office of Homeland Security (OHS), the staff of the newly created Associate DCI for Homeland Security, and the FTTTF. NSA also provided secure communications connectivity for these organizations.

- NSA responded to standing requirements for reporting threat and warning information to the Office of Homeland Security. NSA not only disseminated end product reporting to Homeland Security elements, but also implemented procedures to telephonically tip-off high-priority information before formal publication. This tip-off mechanism ensured that senior officials received perishable information as quickly as possible.

- NSA's Interagency Operations Security (OPSEC) Support Staff (IOSS) provided OPSEC training and information to federal, state, and local first responders. In support of the Salt Lake City Olympics, NSA OPSEC personnel trained officials on operations security and developed an OPSEC video for the public, which was played at the Olympic venues and on inbound commercial

aircraft. The IOSS returned to Utah in May 2002 to host the largest ever (over 600 attendees) National OPSEC Conference and Exhibition. For the first time, a public safety track was added to reach out to first responders who were attending their first OPSEC conference.

- NSA completed a study of threats to information systems, including several focused directly on Homeland Security issues. For example, a specific threat assessment was completed for the FAA on the National Airspace System.

NIMA applied its traditional foreign analysis capabilities to the domestic challenge. In addition, NIMA has tailored its processes and products to respond to the unique needs of the responder community and domestic federal agencies.

- NIMA researched and verified the 25 most dangerous chemical facilities in the United States for the OHS and produced a graphic depicting their locations. This graphic was briefed to the members of the Cabinet, including the Environmental Protection Agency Administrator.

- NIMA produced force protection graphics for 50 airports in the United States at the request of the OHS. These graphics identified the locations of water treatment plants, ordnance storage, fuel storage, control towers, water towers, communications towers, perimeter fences, overrun areas, entry control points, and guard towers, including vulnerable points of entry. NIMA also provided aeronautical graphics and imagery reviews for over 5,000 airfields in the United States at the request of the White House Situation Room for Presidential visits, the National Security Council, and the OHS.

- NIMA supported the FBI and US Secret Service for the 2002 Winter Olympics in Salt Lake City, Utah, by providing security graphics for all event locations, images of the event locations, different line of sight analysis, elevation terrain analysis, and three-dimensional (3D) modeling. NIMA provided similar support at Milwaukee, Wisconsin, for the 2002 Major League Baseball All-Star Game; Boise, Idaho, at the National Governors' Conference; and New Orleans, Louisiana, for the National Football League Super Bowl XXXVI.

- NIMA, in partnership with CIA, developed the Blast Modeling Prototype system to provide photo-realistic 3D visualization and structural blast analysis for vulnerability assessment and threat analysis used in predicting structural collapse and other damage levels when a catastrophic event occurs. The success of the prototype ensured structural damage could be translated and animated in the context of photo-recognizable 3D site models to support analysis and decisionmaking.

- The DOE Information and Special Technologies Support Program (ISTP) supported multiple nation-wide counterterrorism investigations under the authority of the FBI. The ISTP contributed materially to these investigations using a combination of expert personnel in the field and advanced analysis of network-based indicators gathered through the Inquiry Management and Analytical Capability program—which indicates potentially hostile cyber activity against selected DOE and National Nuclear Security Administration (NNSA).

- The Bureau of Alcohol, Tobacco and Firearms (BATF) within the Treasury Department initiated an inspection program for explosives licensees and permittees located within a 50-mile radius of all major metropolitan areas. This effort determines whether there have been any recent thefts or losses of explosives, any unusual activities, or suspicious purchases that may be related to any events that may have occurred or, more importantly, any future acts that are planned.

- The FBI's Joint Terrorism Task Force (JTTF) Program broadened interagency liaison and communications, eliminating duplication of effort, and combined federal, state, and local law enforcement resources in the fight against terrorism. During FY2002, the FBI established JTTFs in 21 field offices and now has a JTTF in each of its 56 field offices. In addition, the FBI established a new National JTTF (NJTTF) at FBI Headquarters to improve collaboration and information sharing with other agencies. The NJTTF currently has representation from 26 federal agencies and two state and local law enforcement officials. IC representatives in the NJTTF include CIA, DIA, DOE, State/INR, and US Coast Guard. BATF also participates.

- BATF expanded its electronic links to the IC and initiated protocols for transmitting classified terrorism-related intelligence from BATF Headquarters to field investigative elements. This link includes access to DoS and DoD classified data processing systems. NSA established a permanent detail position within the BATF Intelligence Division to provide BATF with real-time access to classified intelligence coverage and national security information relevant to BATF's counterterrorism.

- The National Reconnaissance Office, under the direction of the DCI, sponsored the IC-based Law Enforcement Working Group (LEWG). LEWG brings together representatives from federal law enforcement and IC organizations to focus on the appropriate and legal uses of technologies and data collected by the IC and DoD in support of law enforcement operations. This initiative forms a bridge between the Law Enforcement and the Intelligence Communities while protecting the equities of each in relation to sources, methods, and potential grand jury information.

- The US Secret Service (USSS) Intelligence Division continued to work with the Intelligence Community and law enforcement entities to investigate and evaluate all intelligence issues relative to executive protection. The USSS has agents assigned to the FBI's National Joint Terrorism Task Force office, as well as to the CIA. The USSS has representatives on the Counterterrorism Security Group of the National Security Council, the NSC-CSG Counter-Terrorism International training Focus Group, and working groups for the OHS. The USSS also has detailees on its staff from a number of IC agencies, including NSA and NIMA.

- Immediately following the 11 September terrorist attacks, the DCI initiated daily intelligence briefings for the Commissioner of the US Customs Service. These briefings focus on threats to homeland security and threats to US interests abroad. The briefings provide the Commissioner with current threat information giving a clear understanding of the terrorist threat facing the USCS at the border of the United States. Customs used this information to determine the response to counter specific threats.

- The USCS began posting its Daily Border Security Incident Reports to CT-LINK, an all-source interagency database containing intelligence on terrorists and extremist groups maintained by the Intelligence Community.

- The DCI hosted several US Customs Intelligence analysts and special agents on-site as full-time representatives to several interagency centers, including the Counterterrorism Center. This facilitated the rapid exchange of intelligence critical to the Customs law enforcement mission, and provided the IC valuable feedback to augment and refine its intelligence collection and analysis. NSA had an on-site representative at the USCS to facilitate the rapid movement and sharing of information between agencies. This daily support proved to be extremely valuable, especially in coordinating time-sensitive information.

- The IC Chief Information Officer Executive Council endorsed an integrated secure architecture plan to support Homeland Security. The architecture will interconnect organizations operating at the Top Secret, Secret, and Sensitive but Unclassified levels seamlessly as the appropriate secure guard technologies become available. Procedures were adopted to provide direct access to sensitive intelligence information by non-intelligence federal offices involved in the effort. To date, the Environmental Protection Agency, the Department of Interior, the OHS, and the Transportation Security Agency have been connected to the Community Top Secret networks. In addition, the Intelink Management Office established secure connectivity among DoD, Intelligence Community, DoS, and Justice Department and other law enforcement networks to improve information sharing and collaboration among those communities.

[CIA Homepage] [Publications Page] [DCI Annual Report Main Page] [Next]

Support to National Policy

> ***Today the United States enjoys a position of unparalleled military strength and great economic and political influence. In keeping with our heritage and principles, we do not use our strength to press for unilateral advantage. We seek instead to create a balance of power that favors human freedom: conditions in which all nations and all societies can choose for themselves the rewards and challenges of political and economic liberty.***
>
> President George W. Bush
> *The National Security Strategy of the United States of America*
> September 2002

The Intelligence Community routinely gives national policymakers intelligence regarding the intentions of foreign states in many arenas including strategic warning, diplomacy and treaty monitoring, proliferation of WMD, and promoting economic security. Each intelligence discipline provides a valuable piece of the puzzle, and in many cases, a single intelligence discipline may provide the only information available on a given topic. The IC has placed great emphasis on methodologies of alternative analysis and outreach to new and non-traditional sources of expertise, including nongovernmental experts.

Through the Intelink program, significant gains were made in moving classified information from IC Top Secret networks to the Secret-level environment where the majority of the intelligence consumers involved in diplomacy, treaty monitoring, and support to military field operations operate. In addition, information portals tailored to individual site needs are being built so that mission-essential information will be presented directly to the user as it is received.

Strategic Warning

- CIA analysts conducted research on trends that transcend current issues and could pose major policy challenges in the future. Major studies in support of this role included "Russia's Defense Industries and Military Forces in 2020," "Russian Goals for Arms Sales and Technology Exports

in 2010," and "Ethnic Russians in the Former Empire: The Potential for Trouble in the Next Decade." CIA also engaged with a broad range of outside experts on such matters as alternative European Security and Defense Policy futures, war games on a Libyan WMD crisis, and a simulation focused on European reactions to a new Balkan crisis.

- CIA established an energetic program to ensure that analysts keep abreast of outside views on issues of interest to the policy community, including an Alternative Analysis panel of prestigious outsiders and academic specialists to promote "out of the box thinking" on key trends.

- The National Intelligence Warning System continued to provide strategic warning to senior policymakers to enable them to either avert crises or prepare to effectively deal with them. The National Intelligence Officer (NIO) for Warning manages the National Warning Process, along with the DCI Strategic Warning Committee, composed of representatives from CIA, DIA, NSA, State/INR, and NIMA. The NIO also oversees training on warning analysis.

- As tensions between nuclear powers India and Pakistan rose and the threat of war between them increased in late 2001 and early 2002, the NIC produced a series of assessments, as part of its warning function, alerting policymakers to the situation on both sides and the prospects for the standoff escalating or cooling down.

- DIA, in collaboration with the Joint Intelligence Center-Pacific and other elements of the Intelligence Community, produced both the classified and unclassified versions of the Secretary of Defense's *Annual Report on the Military Capabilities of the People's Republic of China*. This Congressionally-directed report is a comprehensive assessment of China's current and future military trends and capabilities and their potential impact on US national security policy.

- During and immediately following the Afghan campaign, State/INR provided a variety of assessments, tools, and intelligence support to policymakers, including a humanitarian map and integrated situation report for Secretary Powell. This information was provided to the Secretary on a daily basis prior to his morning meetings at the White House.

- The DCI Warning Committee monitored and developed an early warning system for near-term crises in which complex contingency planning might be needed and humanitarian situations in which early international intervention would avert massive human suffering and reduce the demand for direct US military involvement.

- The USCG Intelligence Program produced its annual Worldwide Maritime Threat Assessment that covers maritime terrorism, crimes, and piracy. It is distributed to government and commercial entities and fosters information sharing.

Diplomacy, Treaty Monitoring, and Arms Control

The Deputy DCI for Community Management, on behalf of the DCI, signed the *IC Support to Diplomacy and Diplomatic Operations Implementation Plan* specifying actions the IC will pursue in

support of diplomacy. Our response to the 11 September attacks required rapid coalition building to support the deployment of US forces in Afghanistan, which in turn required close support from Intelligence and the crafting of delicate diplomatic arrangements. The Intelligence Community and the Diplomatic Community worked together to maximize the contribution of Intelligence to achieving America's foreign policy goals.

- After the military campaign in Afghanistan, State/INR and World Bank officials presented the Afghanistan Reconstruction Information Management Strategy (ARIMS) concept in Tokyo at the International Conference for Reconstruction Assistance in Afghanistan in January 2002. This information strategy for Afghanistan's reconstruction was established to assist the Afghan Interim Authority and the international donor community with a means to organize data collection related to living conditions throughout the country and donor-funded relief and reconstruction projects. ARIMS promoted standardized data collection and sharing among various UN agencies, the World Bank, and Afghan ministries. It contributed geospatial and imagery data provided by NIMA.

- NIMA responded to a DoS request to delineate the common border of the Federal Republic of Yugoslavia and Former Yugoslav Republic of Macedonia in support of negotiations of a boundary treaty. Sixty-six areas of dispute were identified along the border. The DoS used this product in negotiations with delegates from both countries.

- NIMA produced a Zimbabwe reference map that was disseminated to IC customers, in a collaborative effort with the DoS and CIA. The reference map was produced to aid in the evacuation of foreign nationals, based on the increased violence in Zimbabwe prior to the presidential elections. It portrayed towns, roads, railroads, elevation, airfields, ferries, dams, population density, administrative boundaries, and the mileage between cities.

- State/INR sponsored and organized (frequently with other agencies) 113 conferences—often at the specific request of a policymaker. These conferences facilitated the interchange of expertise and ideas between outside experts and government officials. These events contributed to a more informed foreign policy process. Notable conferences held during FY2002 included:

    - *Conference on Global Infectious Disease and U .S. Foreign Policy*. This conference was organized to heighten awareness of the economic and political impacts of disease. Speakers stressed the linkages among poverty, conflict, and disease.

    - *Conference on Counterterrorism*. Participants discussed defeating and eradicating terrorism, noting that failed and lawless states and zones have become the most useful for

terrorists.

- *Conference on China's Strategic Vision*. Presenters gave insights into China's priorities for the future.

- *Conference on Anti-Americanism*. This conference explored the various manifestations and roots of anti-Americanism around the world, what it means for the United States, and how the United States may address it.

- *Conference on Islamic Extremism in Sub-Saharan Africa*. Conference participants examined new lines of Islamic and radical thought in Africa.

- State/INR is the official pollster for the US Government abroad. Insights gained from the polls conducted in FY2002 were used to advise the President, the Secretary of State and other senior policymakers on the implications of foreign public opinion.

- CIA analysts produced a landmark intelligence assessment on the crisis between India and Pakistan. That assessment has served as the basis for policy meetings and papers looking at next steps in managing the India-Pakistan relationship and for points of US leverage to facilitate a more peaceful coexistence.

- CIA analysts provided extensive support for meetings, summits, and official visits, including the G8 Summit in Canada and a US-European Union Summit. CIA also supported the May 2002 US-Russia Summit.

- CIA analysts provided extensive support to policymakers on trade, human rights and other issues affecting US-China relations. They also reported on North Korean foreign policy and security and economic issues, drawing extensively on outside expertise to broaden CIA's analytic perspective and build substantive expertise.

- The Army's National Ground Intelligence Center identified at least 15 contracts related to Iraqi tank procurement that appeared to be in violation of international sanctions. As a result, these contracts were flagged for termination.

- In anticipation of ratification hearings, the NIC produced a National Intelligence Estimate (NIE), *Monitoring the Moscow Treaty on Strategic Offensive Reductions*.

Combating Proliferation

- DIA's Operation ENDURING FREEDOM Intelligence Task Force also contributed counterproliferation planning data that played a role in the successful mediation of tensions between India and Pakistan. The Secretary of Defense personally credited task force members with providing the information and advice that made his mission to South Asia a success and helped to avoid a possible war between those two nuclear powers.

- The NIC published the unclassified paper, *Iraq's Weapons of Mass Destruction Programs*. The paper warned that Iraq had continued its WMD programs in defiance of UN resolutions and restrictions. Baghdad has chemical and biological weapons as well as missiles with ranges in excess of UN restrictions; if left unchecked, it probably will have a nuclear weapon during this decade. In addition, the NIC produced several NIEs on WMD programs in Iraq and several other countries of concern, including North Korea.

- CIA analysts prepared DCI testimony to Congress on Iraqi WMD and military capabilities. CIA provided new information on three of Iraq's primary missile systems to policymakers and worked with foreign intelligence services to track Iraqi illicit weapons and dual-use technology procurement activity.

- The NIC's *Annual Report to Congress on the Safety and Security of Russian Nuclear Facilities and Military Forces* was quoted widely in the national and international press and academic journals. The report noted that Russia employs physical, procedural, and technical measures to secure its weapons against an external threat, but many of these measures are not designed to counter the pre-eminent threat faced today—an insider who might attempt unauthorized actions. The report also expressed the IC's concern that weapons-grade nuclear materials have been diverted from Russia in the last 10 years, although the Community does not know the extent or magnitude of such thefts.

- The NIC published an unclassified summary of its NIE on *Foreign Missile Developments and the Ballistic Missile Threat Through 2015*. The summary noted that most intelligence agencies project that before 2015 the United States most likely will face ballistic missile threats from North Korea and Iran, and possibly from Iraq—barring significant changes in their political orientations—in addition to the longstanding missile forces of Russian and China.

- During FY2002, State/INR provided senior officials with all-source analyses on nonproliferation issues, especially the development of WMD and their deployment, transfers of advanced

conventional weapons and technologies, and bilateral and multilateral arms control agreements.

- State/INR supported the policy community's effort to prepare demarche language based on intelligence to combat the proliferation of WMD, sensitive technologies, and arms to countries such as Iraq, and ensured appropriate vetting of this language within the Intelligence Community.

- CIA analysts continue to assess proliferation issues relevant to states of the former Soviet Union, including questions of Ukraine's role in a possible sale of an air defense detection system to Iraq.

- CIA analysis on North Korea's uranium enrichment program has been key to US efforts to engage Pyongyang.

Promoting Economic Security and Civil and Environmental Stability

- The USCG Intelligence Program supported the interdiction of illegal fishing in a US Exclusive Economic Zone that escalated into a force protection and US sovereignty issue.

- NIMA analysts traveled to La Plata, Maryland, at the request of the Federal Emergency Management Agency (FEMA), as an integral responder in the aftermath of the La Plata tornado that devastated the area. NIMA analysts created four imagery-derived base maps showing the locations and levels of the damage. The resulting products were released to FEMA and the emergency management community.

- NIMA provided crucial imagery-based information to prosecutors of the International Criminal Tribunal for the Former Yugoslavia in the case against former Yugoslav President Milosovic.

- NIMA produced a Nyiragongo Volcano reference map at the request of the DoS and United Nations Human Rights Commission to aid relief efforts precipitated by the volcanic eruption in Sub-Saharan Africa. The map encompassed portions of the countries of Burundi, Democratic Republic of the Congo, Rwanda, and Uganda. Data layers portrayed towns, roads, drainage, airfields, lava flow paths, and existing refugee camps.

- After more than a year of consultations with partners in both US Government civilian agencies and military commands, State/INR in September 2002 inaugurated its new interagency Humanitarian Information Unit (HIU). Unique within the US Government, the HIU's complement of interagency humanitarian affairs specialists—with a broad range of expertise—to

address both extensive complex emergencies and the more specific aspects of humanitarian assistance such as food security, infectious diseases, climatology, and demining.

- The HIU has been established to provide a nucleus for a better information management system focused on developing reliable, unclassified data needed for humanitarian planning and disaster response.

- The HIU also will produce value-added analysis, coordinate with IC components to facilitate better use of their unclassified information, enhance interagency assessments of conditions affecting US involvement in humanitarian and peace operations, and provide a coordinating mechanism for data sharing with the UN, NGOs, and foreign governments.

- The HIU currently is spearheading new technical initiatives and customized software to both improve analytical capabilities and expedite information exchange.

- The NIC provided policymakers with analyses on continuing security, political, and economic challenges affecting many countries in Latin America. The NIC published papers on the continuing economic turmoil in the Southern Cone of Latin America, with a particular emphasis on the crisis in Argentina and prospects for contagion throughout the region and its impact on US policy. The NIC, through consultations and workshops with outside experts, assisted policymakers in gaining a better understanding of the complex and serious challenges in the Andean Ridge, particularly Colombia and Venezuela.

- The NIC published a special unclassified report, *The Next Wave of HIV/AIDS: Nigeria, Ethiopia, Russian, India and China (ICA 2002-04D, September 2002)*. The report drew on extensive consultations with outside experts to assess prospects for the spread of HIV/AIDS through 2010 in five countries of importance to the United States. This paper and others are part of the NIC's ongoing effort to improve the public discourse on critical national security issues and engage outside experts in a dialogue about global trends, looking out to the year 2015.

- The NIC and the DoS cosponsored a conference that examined the prospects for resolving regional conflicts involving four states of the former Soviet Union: Armenia, Azerbaijan, Georgia, and Moldova. The conference brought together outside scholars and regional experts to deepen understanding of the complex geopolitical dynamics at work in the region. The NIC summarized the views of the participants in a conference report, *Resolving Conflicts in the Caucasus and Moldova: Perspectives on Next Steps*.

-

CIA analysts prepared a multimedia presentation on Caspian energy, looking both at the energy-producing potential of the region and the geostrategic visions of the Caspian states and key outside players. These analysts also met the heavy demand for information on Russia's energy sector, including work on Russia's contentious relations with OPEC, the effects of privatization on Russia's seven major oil companies, and Moscow's energy investment strategy. CIA also gathered information on the energy infrastructure of the world's other key oil and gas producers and used the data to produce analyses of their capabilities and vulnerabilities.

- The NIC supported policymakers with analyses on environmental issues, including dynamics and developments regarding the United Nations World Summit on Sustainable Development.

- CIA provided policymakers with analysis on the humanitarian situation in and around Afghanistan; identified actions needed to stabilize it; and provided medical aid to Afghan civilians, delivering enough medical supplies, equipment, and medication to enable local hospitals and clinics to function.

[CIA Homepage] [Publications Page] [DCI Annual Report Main Page] [Next]

Support to Military Operations

> ***Fusing the ability to see and strike through interconnected systems, while at the same time reducing the vulnerability of operators, portends momentous changes in the nature of warfare. On the other hand, the complex task of extracting the Taliban and al-Qa'ida forces from difficult terrain and cave hideouts illustrates how much farther we need to progress in our ability to fuse knowledge, decisions, and action into a seamless combat process.***
>
> General Richard B. Myers
> Chairman of the Joint Chiefs of Staff
> Joint Forces Quarterly
> Autumn/Winter 2001-02

The US Intelligence Community supported military operations in the areas of Indications and Warning, Force Protection, Force Modernization, Operational Planning and Execution, and Training and Readiness. The IC alerted national and theater combatant commanders in a timely manner about threats to US and allied interests; provided senior defense decisionmakers with strategic warning; provided information on, and monitored the readiness and disposition of foreign military forces; assisted in force protection; and worked directly with individual military units, ships, and bases to provide mission-enhancing tactical intelligence capabilities. IC officers have integrated directly with military forces, and greater attention is being paid to defensive communications security and operations security measures.

Indications and Warning

- NIMA placed personnel at each of the service components of the theater combatant commands to improve timeliness and tailored products in satisfaction of geospatial intelligence requirements. NIMA established the Spatial Analysis Branch after the 11 September attacks to focus analytic support on covert and clandestine military and paramilitary operations and counterterrorism analysis.

- NSA developed and deployed a computer network defense intrusion detection system that significantly enhances protection of the Defense Information Infrastructure (DII). The system consists of a network of sensors that are strategically placed within the DoD infrastructure, providing analysts the capability to identify anomalous cyber activities traversing the network.

The system complements local DoD intrusion detection systems by providing a layered cyber-defense system.

- NSA managed and improved the capabilities of the Intelligence Community Incident Response Center and the process for dissemination of cyber threat information. NSA also provided frequent, often time-urgent support to military operations, describing the threats to information systems and networks faced by such operations.

- CIA analysis of guerrilla and mujahidin operations and weaponry in Chechnya provided clear threat warnings to US and Coalition troops in Afghanistan.

Force Protection

- Based on the findings of an Advanced Concept Technology Demonstration, DIA established and equipped a deployable Chemical and Biological Intelligence Support Team (CBIST) staffed by technically qualified, all-source analysts. CBIST operations provided direct support to combatant commanders through overt collection of chemical, biological, radiological, and nuclear (CBRN) samples at suspected CBRN sites. The combination of team capabilities in technical, clinical and on-site analysis, coupled to Washington-based analysts through real-time video and on-line coordination, resulted in early confirmation of al-Qa'ida's pursuit of a sophisticated biological warfare capability. DIA analysts also worked directly with USCENTCOM warfighters to deal with potential radiological hazards of materials and objects encountered during operations in Afghanistan.

- DIA formed the Joint Information Operations Threat Working Group with broad participation from the intelligence, acquisition, and test communities to develop a *Capstone Information Operations Threat Assessment*. This capstone assessment provides validated threat details to meet Congressional direction to conduct regular information assurance testing of all DoD information technology. It will result in an assessment of the most current threats to the entire DoD system and support efforts to conduct realistic information assurance testing to ensure the warfighter has survivable capabilities in combat. DIA also hosted a series of briefings on information warfare threats to senior DoD policymakers to ensure their development and acquisition programs are mitigating future information warfare threats.

- The Air Force provided CI analytical capability to its Network Operations Security Centers. This initiative included capabilities aimed at identification and analysis of probes to critical networks, protecting networks where critical program information is resident, supporting the INFOCON process, detecting insider threats, conducting awareness briefings, and supporting information flow. This continued capability is aimed at providing predictive analysis through collection of all-source intelligence to prevent attacks against Air Force information systems. AFOSI gleaned viable raw intelligence through CI collection methods and promptly reported it to local customers and the IC. In-garrison commanders relied heavily upon AFOSI's CI support as their basis for force protection and other CI decisions.

- CIA led an interagency effort to acquire information on minefield locations in Afghanistan. The effort identified minefield locations and the information was reported directly to USCENTCOM, US Special Operations Command (USSOCOM), and the Marine Corps Intelligence Activity.

- NIMA provided extensive monitoring and targeting support, identifying and locating threat systems, to Operation NORTHERN WATCH and SOUTHERN WATCH, US military operations to patrol the northern and southern no-fly zones of Iraq.

- NSA deployed to 39 locations worldwide and performed Communications Systems Security (COMSEC) and Force Protection monitoring of virtually every communications suite in the US military inventory in support of the Global War on Terrorism, Homeland Security (Operations ENDURING FREEDOM and NOBLE EAGLE), Operations NORTHERN WATCH and SOUTHERN WATCH, and Operations JOINT FORGE and JOINT GUARDIAN. NSA reported on both classified and sensitive but unclassified information that was revealed.

- NIMA analysts used a wide variety of high-resolution commercial imagery types to respond to US Transportation Command (USTRANSCOM) requirements for terrorist threat information at airfields worldwide. In response to this request, NIMA produced and posted over 900 new and revised Force Protection Airfield Graphics on the Imagery Product Library Server. These graphics were used at the USTRANSCOM Threat Working Group, in conjunction with HUMINT and other sources, to determine whether a mission was a "Go or No-Go." These graphics were also used by other commands and agencies in support of non-combatant evacuation operations, humanitarian relief, and Presidential visits.

- NIMA provided high-resolution commercial imagery of Force Protection Port Graphics for 13 US ports to USTRANSCOM. These ports had high-volume shipments of munitions, tanks, and other weapons. This product was a force protection vector overlay on imagery, which included major road and railroad networks, walls and fences, entry control points, and floodlights.

Force Modernization

- NIMA achieved full operating capability of the Target Management System Network in January 2002. This system provided NIMA customers direct access to targeting support and navigation data from the NIMA precise point database. The new capability was demonstrated as part of a NIMA-Navy technical exchange meeting on targeting accuracy.

- The NIO for Conventional Military Issues led comprehensive studies on China and Iraq that included strategy and doctrine, campaign planning, weapons development, and military professionalization. These studies play a major role in US forces strategy formulation and are an important input to new weapons development programs.

Operational Campaign Planning and Execution

- DHS forward-deployed to Afghanistan with USSOCOM elements. DHS collectors obtained valuable targeting information and other actionable intelligence that directly supported US combat operations. DHS consolidated its Detachment Afghanistan at Bagram Air Base and deployed collectors with combat forces throughout the country. In addition, DHS formed new field exploitation teams that accompanied USSOCOM forces in the field.

- NSA built upon the considerable efforts already made prior to FY2002 to more fully integrate the role of intelligence information with the missions of deployed military forces, senior military planners, and military intelligence analysts at every level. This integration is best seen in the multifaceted support to Operation ENDURING FREEDOM, where NSA personnel have been integrated with the combatant commander staffs. NSA officers identified and located terrorist threats to disrupt military operations; ensured field commanders and others had access to NSA operations and crisis action centers; developed a collection system that supports military forces abroad; and coordinated the development of supporting intelligence plans with USCENTCOM, US European Command, US Pacific command (USPACOM), and USSOCOM.

- NIMA analysts teamed with US Strategic Command (USSTRATCOM) analysts to enhance the analytical capabilities in a special program dedicated to long-term trend analysis of mobile strategic rocket forces. This joint team put in place the analytical skills to provide comprehensive, three-dimensional views of strategic mobile missile areas, and increase the command's ability to test missile vulnerabilities.

- CIA established a platform to provide support to USPACOM Joint Task Force-510. Using HUMINT reporting and a variety of technical operations, this platform proved instrumental in the June rescue of US hostages from the Abu Sayyaf Group in the Philippines.

- The NIO for Conventional Military Issues served as a conduit between USCENTCOM military planners and IC analysts for regular intelligence assessments on developments in the Middle East.

- CIA deployed 45 officers to support combatant commander staffs at USCENTCOM, US Space Command, USSTRATCOM, and USPACOM.

Training and Readiness

- Activated within days of 11 September, the Intelligence Community POW/MIA Analytic Cell leveraged national intelligence analysis and collection to support emerging POW/MIA intelligence requirements in Afghanistan, Somalia, Yemen, Philippines, Iraq, Pakistan, and other regions around the world where US forces were or may be deployed. The POW/MIA Cell, managed by DIA, published a comprehensive POW/MIA study for Afghanistan that was used extensively by deploying US forces. The POW/MIA Cell produced nine more POW/MIA studies supporting the Office of the Secretary of Defense, the Joint Chiefs of Staff, combatant commanders, and allied foreign partners. Its efforts resulted in the location and eventual rescue of

the Shelter Now International detainees. The POW/MIA Cell also has been directly involved in determining the fate of Lieutenant Commander Michael Speicher, a US Navy pilot downed in Iraq during the Gulf War; supporting US forces deployed to the Philippines; and spearheading a comprehensive POW/MIA study on the probable treatment of Coalition prisoners captured by Iraq or al-Qa'ida.

- As Executive Agent for OPSEC Training, the Director of NSA used the IOSS to provide "Train the Trainer" OPSEC skills to seven major DoD and federal components that train approximately 2,000 students annually. The IOSS also presented 86 OPSEC courses to 2,885 students at the National Cryptologic School and at customer sites worldwide.

- The Joint Military Intelligence Training Center supported the Global War on Terrorism by offering increased training opportunities on its home campus and providing more mobile training teams. Increased emphasis was placed on counterterrorism, intelligence analysis, collection management, indications and warning, intelligence production, and intelligence mission systems applications.

- The DIA Joint Intelligence Virtual University provided cost-efficient training for the Intelligence Community and introduced new training opportunities with the inclusion of the NSA National Cryptologic School, the NIMA National Geospatial Intelligence College, and the USPACOM Joint Intelligence Training Activity-Pacific. Web–based training saves money, time, and manpower with more than 200 courses offered on-line. More than 6,000 students enrolled in FY2002.

[CIA Homepage] [Publications Page] [DCI Annual Report Main Page] [Next]

Support to Law Enforcement

> ***The relationship between the FBI and the CIA has never been stronger or more productive. While we concede that there were isolated failings in the information flow between the two agencies prior to 9/11, we must not overlook the fact that a successful, systematic effort has been underway for years to develop and build upon our agencies' relationship.***
>
> Robert S. Mueller, III Director,
> Federal Bureau of Investigation
> Testimony to the Joint Intelligence
> Committee Inquiry, October 17, 2002

The Intelligence Community provided the law enforcement community, especially the Department of Justice, FBI, and the Immigration and Naturalization Service, with actionable intelligence on terrorist groups, transnational organized crime groups, and their activities, such as narco-trafficking. Policymakers expressed increasing need to be knowledgeable of the actions of these criminal figures as their influence on foreign governments grows. IC agencies collaborate via unclassified e-mail systems and database sharing in supplying foreign intelligence to US policymakers and, within established guidelines, in a robust exchange of lead information with law enforcement agencies. The IC has made valuable contributions, particularly in identifying and tracking terrorist funds, and has taken advantage of existing and new relationships with foreign governments.

Recognizing the need for a more formalized strategy to support law enforcement customers, the DCI had initiated the development of a *Strategic Plan for IC Support to Law Enforcement* prior to the attacks of 11 September. The plan was developed as a collaborative effort among IC representatives and with full participation from law enforcement agencies. The plan sets forth a coordinated IC strategy to address future federal law enforcement needs by specifying goals and specific IC actions to fulfill the strategy, while protecting those elements of existing support that are already working well.

The FBI's Security Division supports state and local law enforcement by ensuring that those who require access to classified information have the proper security clearance and need-to-know. It makes accurate and timely judgments of the trustworthiness of state and local officials who require access to classified information to support their counterterrorism efforts. Over 1,000 clearances were granted to state and local law enforcement officers during FY2002, a substantial increase over previous years.

Counternarcotics

DIA focused intelligence support on Drug Enforcement Administration (DEA) efforts in Mexico. A special study on the Quintana Roo region played a major role in positioning operational forces to interdict the movement of illegal drugs into the US and directly contributed to the arrests of two major drug traffickers.

- CIA supported a reevaluation of US antidrug priorities by the President's Office of National Drug Control Policy by publishing a paper that addressed the strategic vulnerabilities of the global drug trade. The paper addressed the exploitable operational, logistical, financial, and geographic weakness of the many criminal enterprises that supply narcotics to the United States and other markets. The paper was well received by the Director of the Office of National Drug Control Policy, and he instructed the law enforcement community to use it as a template to craft a companion product addressing the vulnerabilities of the US domestic drug trade.

- NSA provided US policymakers and law enforcement agencies, including the Office of National Drug Control Policy, Counter Drug Executive Secretariat, Coast Guard, FBI, Customs, and DEA, with foreign intelligence that contributed to the disruption or dismantlement of major foreign narco-trafficking organizations. This was accomplished by full integration into the counternarcotics community under the leadership of the DCI's Crime and Narcotics Center and was based on the robust exchange of lead information between the Intelligence Community and law enforcement agencies.

- NSA also provided tailored briefings describing the threat to information systems and networks, focusing on issues of interest to the FBI. NSA provided COMSEC monitoring for the Joint Interagency Task Force-East and the Joint Interagency Task Force-West.

- NIMA provided focused intelligence support to USCS, FBI, and DEA on narcotics trafficking along the US/Mexico border port of entries. NIMA also provided extensive information and analysis of suspected drug cartel facilities and airfields believed to be used for narcotics trafficking in Colombia.

- CIA analysts wrote the first-ever analysis of drug flows and consumption in Brazil, the world's second-largest consumer of cocaine after the United States. The study entailed open-source field collection and an innovative methodology for calculating the prevalence of drug use.

- The NIC provided policymakers with analysis on the damaging and corrupting influence that the illicit narcotics trafficking industry continues to exert on several of the young democracies in Latin America.

Countering International Organized Crime

- A joint investigation with the AFOSI, the USCS, the DoS, the Department of Commerce, and the Naval Criminal Investigative Service led to the discovery and arrest of a subject who brokered sales of military aircraft parts from US companies and had them shipped to companies in Iran. The subject was found guilty and was sentenced to 30 months in jail, 36 months probation, and $10,000 fine.

- CIA, working with foreign governments, collected and reported intelligence to US law enforcement agencies conducting operations against members of Latin American and Middle Eastern terrorist groups and against smugglers of aliens into the United States. CIA also provided the DoS with an expert on human smuggling and trafficking who oversaw the assessment, drafting, and coordination of the 2002 Trafficking in Persons report.

- USCG Pacific Area Intelligence worked with Law Enforcement and Intelligence Community members to identify human smuggling activities. Their analytical efforts allowed USCG forces to preposition scarce interdiction assets and interdict illegal migrants in the Eastern Pacific and off the coasts of California, Hawaii, and Guam.

- The Financial Crimes Enforcement Network actively participated in these joint Law Enforcement-Intelligence Community committees: Countering Organized Crime, Counter-Narcotics, and Counterterrorism. Intelligence Community reporting was routinely used as lead information in tracking suspects.

- CIA provided key research results to the Treasury Department in its efforts to apply the Patriot Act to a foreign bank involved in money laundering. CIA analysts identified key players in the bank, their relationship to international organized crime, and the bank's efforts to hide its accounts from US law enforcement.

[CIA Homepage] [Publications Page] [DCI Annual Report Main Page] [Next]

Support to Countering Foreign Intelligence

> ***I have nothing but contempt and anger for those who betray the trust by exposing the names of our sources. They are, in my view, the most insidious of traitors.***
>
> President George H. W. Bush
> Dedication ceremony for the George Bush
> Center for Intelligence, April 26, 1999

During FY2002 the President affirmed Presidential Decision Directive 75 (PDD-75) committing the US Government to creating a national-level counterintelligence system that would be positioned to deal with the asymmetric threat environment and other realities of the global, interconnected information age of the 21st century. The Intelligence Community as a whole supported the counterintelligence mission through focused analysis and reporting of espionage threats, improved information management and sharing, and by providing more and better training to at-risk groups. A major focus has been on protecting sensitive nuclear weapons-related information within the Department of Energy.

- The Office of the National Counter Intelligence Executive (NCIX) initiated development of the National Counter Intelligence Strategy mandated by PDD-75 and developed a risk assessment methodology for identifying critical national assets. The NCIX completed two damage assessments and continued work on seven others, including those of former FBI Agent Hanssen and former DIA analyst Montes. CIA, in cooperation with foreign governments, collected and reported intelligence that assisted US law enforcement agencies in conducting operations against the Cuban intelligence apparatus.

- The DCI Foreign Denial and Deception Committee (FDDC) published a landmark study of damage caused by unauthorized disclosures of classified intelligence, in support of the Attorney General's report to Congress (per Section 310 of the FY2002 Intelligence Authorization Act). Per DCI direction, FDDC began an Intelligence Community-wide initiative to provide denial and deception (D&D) briefings to Senior Intelligence Service-level managers. FDDC also launched a major training initiative in partnership with the Joint Military Intelligence College for senior IC analysts to better counter foreign D&D.

- The FBI's Security Division protected FBI facilities, personnel, and information systems against compromise by foreign intelligence services. Using a layered "defense-in-depth" strategy, the Security Division improved the FBI's ability to make accurate and timely judgments of the trustworthiness of applicants, employees, contractors, and task force members who have access to the FBI. A pilot financial disclosure program and an expanded personnel security polygraph program were developed to support this effort, as was a comprehensive security policy, education, and training function. The Security Division also created a comprehensive, centrally managed Information Assurance (IA) program to safeguard the integrity and confidentiality of FBI information systems while providing them with full lifecycle security. This IA capability strengthens the FBI's ability to guard against the compromise or misuse of its information systems by a trusted insider, defends against external attacks, and addresses the potential for inadvertent compromise through ignorance or carelessness.

- DIA implemented a major information assurance initiative, the Public Key Infrastructure (PKI) system, which enables intelligence analysts to create subject-specific or case-specific sites on a shared network and enforce a "need-to-know" security policy by limiting on-line access. In FY 2002, the DoD Intelligence Information Systems (DoDIIS) community installed the PKI program at more than 50 sites and enrolled over 800 users. The system is expected to encompass all of the DoDIIS community's 25,000 users.

- The AFOSI created a revolutionary information management system that acts as a warehouse, consolidating investigative, operational, and intelligence information. The Investigative Information Management System was adopted by the Defense Computer Intelligence Information System (DCIIS), now known as PORTICO. AFOSI's concept, structure and code allowed DCIIS/PORTICO to hit the ground running with a functional tool, adapting it to service all customers: Army, Air Force, Navy, Marine, NSA, DIA, NIMA, and CIA. Once operational, PORTICO will standardize the collection, storage, and dissemination of intelligence information reports, as well as source information, analysis, and production, thereby creating a seamless system in which all items and agencies interact to support the national CI structure.

- NSA presented over 175 Defensive Information for Counter Intelligence Espionage (DICE) briefings to over 40,000 attendees. A companion video "DICE 2002, Now It's Personal" was produced and distributed to reach customers who could not attend the briefings.

- NSA, DIA, CIA and the NIC analyzed and reported on the threat to information systems and networks posed by intelligence operations of foreign governments and a multitude of transnational groups. The purpose of this mission is to identify the threats faced by IC customers, enabling them to implement information assurance security measures to counter the foreign intelligence threat by protecting information systems and networks.

- NSA assessed and reported on the principal intelligence threats confronting US military operations around the globe. NSA also provided US policymakers and law enforcement agencies with foreign intelligence information that contributed to the conduct of sensitive activities by the CI community. The CI community used NSA products to help build defensive security programs

and activities designed to protect against both foreign intelligence collection efforts and unauthorized access to, or disclosure of, protected facilities, information, and material.

- Through an improved sharing of information between NSA and both the CI and Law Enforcement Communities, NSA was able to turn lead information into actionable intelligence for those who are responsible for deterring, detecting, and neutralizing foreign intelligence service activities against the United States and its interests.

- The DOE OCI/ODNCI Investigations Program supported FBI counterintelligence investigations involving DOE and NNSA personnel, facilities, programs, or information. The program provided technical experts to evaluate information developed by the FBI relating to WMD and other areas within the technical domain of DOE/NNSA.

- The DOE OCI/ODNCI Investigations Program also provided CI coverage for nuclear facilities under the joint control of the US Navy and DOE. The Investigations Program continued liaison with federal, state, and local law enforcement and CI agencies.

- The DOE OCI/ODNCI Analysis Program produced country threat summaries and in-depth country threat assessments evaluating the threat of foreign intelligence collection against DOE/NNSA laboratories, personnel, and information. These products served as the basis for CI-awareness briefings for laboratory personnel who interact with foreign nationals within the United States and overseas. CI analysis provided focused assessments to support specific treaty-related overseas deployments of DOE personnel.

- During FY2002 there were significant increases in the numbers of the DOE/NNSA population reached through CI course and seminar offerings; 1,760 individuals attended 104 mobile training courses provided by the CI Training Academy based in Albuquerque. In concert with the Office of Security, OCI/ODNCI provided CI material via a web-based module that is included in DOE security refresher briefings.

- The OCI/ODNCI Counter Intelligence Evaluation Program (CIEP) completed more than 5,700 evaluations on individuals with required access to DOE's high risk programs. The CIEP has continued to conduct liaison with other federal agencies maintaining access to sensitive source information.

- DIA expanded the scope of its anomalies recognition and reporting program, introducing it to new organizations including USTRANSCOM. This program complements the office's parallel focus on insider threats and is an active tool to connect the DIA work force and other organizations to an interagency CI enterprise. The anomalies briefing brought new levels of CI awareness to well over 2,500 people and responds to earlier guidance by the DCI and the Foreign Denial and Deception Committee.

- The Defense Security Service (DSS) received 1,715 suspicious contact reports (an 85 percent rise over FY2001) from defense industry, of which 975 warranted in-depth analysis. One of these

reports resulted in the January 2002 arrest of Klaus Buhler, a German national who was attempting to illegally purchase and export military aircraft engines to Libya. The DSS experienced a 116 percent rise in reports received regarding potential foreign collection activities.

[CIA Homepage] [Publications Page] [DCI Annual Report Main Page] [Next]

Looking Ahead

The threats we face are growing in complexity and they are in fact, converging. The convergence of these threats, combined with a resurgence in regional ethnic strife, provides a breeding ground for instability that can be exploited by our enemies.

We are more likely to achieve success against these threats if we partner with our strategic allies. Strategic partnerships are critical if we are to maintain our decisive intelligence advantage and stay ahead of the threats and dangers they pose. Internally, this new and evolving environment demands seamless interagency cooperation because our adversaries continually will seek to counter or minimize our strengths and exploit our weaknesses.

Our customers expect us to provide knowledge and insight on foreign leadership plans and intentions, warning of global crises or threats to our homeland, and they expect us to provide actionable intelligence around-the-clock while maintaining global coverage. While balancing our customers' needs for actionable intelligence, with the recent substantial increase in IC funding, we will continue to be responsible stewards of the funds provided by the Congress and the American people. This means we must be clear on our strategic imperatives—both near- and long-term—to provide a decisive information advantage to our customers,to safeguard our country's intelligence advantage, and to overcome the growing convergence of threats.

Intelligence Imperatives

The DCI has established the following imperatives, or goals, for the Intelligence Community to build on our pledge to serve our country with resolve in time of war or uncertainty, and in ways that protect our dominance in worldwide intelligence collection and analysis. As we move forward to achieving these imperatives, the DCI is constructing a performance-planning framework to establish performance goals with measures. This framework will enable IC leaders to guide Community activities and their progress against IC objectives.

Win the War on Terrorism

The Intelligence Community's war on terrorism began prior to 11 September and will not end soon. We have been warning of the threat posed by international terrorism for at least two decades, however, we must do better. Now that our country has been attacked, we are determined to serve the American people by doing whatever is necessary to avoid future attacks. In the months following the September tragedy, the pace of our activities has quickened and the scope has broadened to a truly global scale. Still, the day-to-day war we wage on terrorism, for the most part, is a silent one. Our unrelenting focus is on providing

precision intelligence to successfully win the war onterrorism. Our intelligence will serve all types of customers—from the decisionmakers at the national level, to forward deployed US forces executing the war, to "first responders" in Homeland Security. We must strengthen our capabilities and resolve to achieve our objectives.

Warn of Impending Global Threats

Given the shifting global landscape and the emergence of a new array of threats to Americans, the Intelligence Community has greater responsibilities to inform our leaders and supply them with actionable intelligence. Our ability to provide insights into the intentions of state and non-state actors across the globe is a central role for Intelligence and is a key reason for our past success. To continue being successful, we must address intelligence gaps in non-traditional ways and offer alternative scenarios as we piece together the intelligence puzzle. Our intelligence capabilities cannot be ubiquitous, but we must have broad abilities to access the threats to our nation's safety.

Protect America

Foreign intelligence remains the first line of defense for Americans at home and abroad. In the past, intelligence served primarily one group of national policy and military customers to provide for the nation's security. Today, we face a greatly expanded group of customers with responsibility to provide for the nation's internal security, and we must quickly identify legal, policy, technical, and cultural impediments to working with that expanded customer set. Further, we must adapt IC processes to receive law enforcement information for the purpose of linking it with foreign intelligence. Thus we will be better postured to gain insights into terrorist plans and intentions to enable the government to prevent terrorist attacks.

Succeed Against Enduring Strategic Challenges

While we are focused on defeating terrorism and protecting our homeland, we must not lose sight of the enduring strategic challenges that we face. These enduring strategic challenges require that we focus our resources beyond the next crisis by investing our time, talent, and energy in the long term, in-depth activities and research we need to address these challenges. Recently, the DCI established several key programs that will build the capabilities required to make significant progress against these key challenges.

Protect Our Intelligence Capabilities

Protecting our intelligence capabilities will be increasingly difficult because our adversaries have access to many of the same technical advances and breakthroughs that we are attempting to leverage. Our challenge is to further our competitive advantage by protecting our sources and methods, reducing our vulnerability to denial and deception tactics, defending against insider threats, ensuring continuity of operations in the event of natural or man-made disaster, and by operating effectively in the event of a

crisis. Our efforts to protect intelligence sources and methods cannot unduly inhibit the delivery of intelligence to the people who need it, when they need it.

Leverage Technology to Transform Intelligence

Recent advances in science and technology provide us with a unique opportunity to transform intelligence. New resources are being applied to develop our analytic, collection, and processing capabilities, and to improve cross-component collaboration through the Intelligence Community System for Information Sharing. We are increasing our investments in capabilities that will give US intelligence the edge it needs, and we must ensure that these technologies reach fruition. Innovative programs such as In-Q-Tel provide CIA and the Intelligence Community with effective reach into the cutting edge creativity of America's private sector. We will continue to deploy novel commercial technologies to meet critical mission requirements. The successes of In-Q-Tel suggest a positive trend in this direction.

Needed Capabilities

As we work to achieve the results expected of us by our customers, we need a commitment to develop the human and technological capabilities critical to meet Community imperatives. We must optimize our existing suite of capabilities, while making continuous improvements to our intelligence portfolio.

Our People

The intelligence business is a people business. We cannot forget that all the hardware, technology, and tools we employ are useless without the innovation, commitment, and creativity of our work force. We must emphasize recruitment and retention of the best and brightest from diverse cultural and educational backgrounds. We need to mentor our work force, train them to be prepared for the challenges that they will face in the future, and ensure that our seasoned professionals invest time in sharing their knowledge with our new recruits.

Multi-Intelligence Operations

While we have made great progress harnessing the collective capabilities of the Intelligence Community, we still have a way to go. We must continue our evolution and more effectively integrate all intelligence disciplines because the fusion of multiple intelligence sources is efficient, provides the most complete picture, increases the confidence that we have in our reporting, enhances our situational awareness, and provides more viable options for policymakers, diplomats, and warfighters.

Analysis

We must train and reward our analysts to gain the depth necessary to provide customers a long-term perspective and implications of fast-moving events. We must encourage analysts to increase cooperation and communication with the private, commercial, and academic sectors. These partnerships will offer us

new insights, broader access to information, and greater understanding in many areas of intelligence.

Clandestine Collection

We face growing demands for information, and our collectors face growing defenses, including denial and deception. Because foreign denial and deception depends on increasingly available information about our collection systems, we need to put much greater emphasis on innovative techniques that are much less vulnerable to foreign countermeasures. Our ability to draw on a global collection network is critical to develop an effective worldwide warning capability.

Remote Sensing

A new class of remote sensing capabilities is needed to maintain global awareness and support the military's battle space awareness plan. We will also need to develop innovative sensing technologies to address hard targets.

Research & Development

We must research and develop promising areas to help develop smaller, smart sensors, and advanced computing. We must expand development of next-generation sensors and explore how we might apply these sensors to detect and characterize chemical, biological, radiological, and nuclear threats.

Our Leadership Challenge

The success of the Intelligence Community in accomplishing these objectives is contingent upon our ability to integrate our capabilities into a cohesive whole, focused with common purpose on the same goals. To succeed, senior Intelligence Community management must be responsible to ensure that our people have:

- **Leadership** that enables them to take prudent risks to advance the mission.
- **Support** they need to continuously improve their skills.
- **Environment** that supports and rewards innovation.
- **Opportunity** to develop an IC perspective and a shared set of values.

[CIA Homepage] [Publications Page] [DCI Annual Report Main Page] [Next]

Appendix B: Glossary

3D	Three Dimensional
AFOSI	Air Force Office of Special Investigations
ARIMS	Afghanistan Reconstruction Information Management Strategy
BACWORTH	Biological and Chemical On-line Repository of Technical Holdings (DIA)
BATF	Bureau of Alcohol, Tobacco and Firearms
BW	Biological Warfare
CBIST	Chemical and Biological Intelligence Support Team
CBRN&M	Chemical, Biological, Radiological, Nuclear and Missile
CI	Counterintelligence
CIA	Central Intelligence Agency
CIEP	Counter Intelligence Evaluation Program
CIO	Chief Information Officer

COMSEC	Communications Systems Security
CTC	Counterterrorism Center
CW	Chemical Warfare
D&D	Denial and Deception
DCI	Director of Central Intelligence
DCIIS	Defense Computer Intelligence Information System
DEA	Drug Enforcement Agency
DHS	Defense HUMINT Service
DIA	Defense Intelligence Agency
DICE	Defensive Information for Counterintelligence Espionage
DII	Defense Information Infrastructure
DoD	Department of Defense
DoDIIS	Department of Defense Intelligence Information Systems
DOE	Department of Energy
DoS	Department of State
DSS	Defense Security Service

DTIP	Disruptive Technology Innovative Partnership
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FBI/CTC	FBI Counterterrorism Center
FDDC	Foreign Denial and Deception Committee
FinCEN	Financial Crimes Enforcement Network
FY	Fiscal Year
G8	An informal group of eight countries: Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States
HIU	Humanitarian Information Unit
IC	Intelligence Community
INFOCON	Information [threat] Condition
INR	Department of State Bureau of Intelligence and Research
IOSS	Interagency Operations Security (OPSEC) Support Staff
ISTP	Information and Special Technologies Program

J2	Joint Staff Director for Intelligence
JCMEC	Joint Captured Materiel Exploitation Center
JITF-CT	Joint Interagency Task Force – Counter Terrorism
JTTF	Joint Terrorism Task Force
LEWG	Law Enforcement Working Group
MIA	Missing in Action
NATO	North Atlantic Treaty Organization
NCIX	National Counterintelligence Executive
NGO	Nongovernmental Organization
NIC	National Intelligence Council
NIMA	National Imagery and Mapping Agency
NIO	National Intelligence Officer
NJTTF	National Joint Terrorism Task Force
NNSA	National Nuclear Security Administration

NRO	National Reconnaissance Office
NSA	National Security Agency
OCI	Office of Counter Intelligence
ODNCI	Office of Defense Nuclear Counter Intelligence
ONI	Office of Naval Intelligence
OPSEC	Operations Security
PKI	Public Key Infrastructure
POW	Prisoner of War
USCENTCOM	United States Central Command
USCG	United States Coast Guard
USCS	United States Customs Service
USJFCOM	United States Joint Forces Command
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
USSS	United States Secret Service

USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command
WMD	Weapons of Mass Destruction

[CIA Homepage] [Publications Page] [DCI Annual Report Main Page]