The 2006 Annual Report

of the

United States Intelligence Community

Director of National Intelligence

February 2007

Foreword

On behalf of the President, it is my honor to present this report on the performance of the Intelligence Community (IC) in Fiscal Year (FY) 2006.

The IC underwent a great deal of change last year. The Office of the Director of National Intelligence embraced the reforms mandated by the Intelligence Reform and Terrorism Prevention Act of 2004 and guided the integration of the 16 elements that comprise the IC as outlined in the *National Intelligence Strategy*. This report details our efforts to meet the objectives articulated in that strategy. It is intended to complement my Annual Threat Assessment testimony to Congress and the analyses contained in my submission of the budget request for the National Intelligence Program for FY 2008.

The widest range of information has been included in this report to provide an accurate picture of what we have achieved and what we will achieve. Because this report is an unclassified document (per the statutory requirement), it cannot discuss all the details of our activities and plans. Nevertheless, I believe it provides the essential context for understanding the IC's achievements and intentions. It is important to remember that a large portion of our overall effort—both in the programs that I oversee and in the organic intelligence elements of the Department of Defense—helped to provide our service personnel on the front lines in Iraq and Afghanistan with unmatched intelligence support to protect them from harm and ensure the success of their operations.

Despite the many challenges the men and women in our Nation's intelligence services faced in FY 2006, their professionalism and dedication are unmatched, and our Nation owes them a great deal. Of course, none of our progress would be possible without the close and continuing support from our partners in Congress, whose continued support and encouragement are enduring sources of strength for the IC.

Sincerely,

John D. Negroponte

Contents

Congressional Tasking

This report is required under the following provisions of the National Security Act, as amended (50 USC 404d):

(a) 1(A) Not later each year than the date provided in Section 415b of this title [February 1] the President shall submit to the congressional intelligence committees a report on the requirements of the United States for intelligence and the activities of the intelligence community.

(B) Not later than January 31 each year, and included with the budget of the President for the next fiscal year under Section 1105(a) of Title 31, the President shall submit to the appropriate congressional committees the report described in subparagraph (A).

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.

(b) Matters covered

1 Each report under subsection (a) of this section shall—

(A) Specify the intelligence required to meet the national security interests of the United States, and set forth an order of priority for the collection and analysis of intelligence required to meet such interests, for the fiscal year beginning in the year in which the report is submitted; and

(B) Evaluate the performance of the intelligence community in collecting and analyzing intelligence required to meet such interests during the fiscal year ending in the year preceding the year in which the report is submitted, including a description of the significant successes and significant failures of the intelligence community in such collection and analysis during that fiscal year.

2 The report shall specify such matters under paragraph 1(A) in sufficient detail to assist Congress in making decisions with respect to the allocation of resources for the matters specified.

Executive Summary

In Fiscal Year (FY) 2006, the Intelligence Community (IC) contributed to the security of the United States and helped protect and advance national interests. Building on the important structural changes made just before FY 2006, the IC acted in a more integrated manner than ever before against our most important objectives, as expressed in our *National Intelligence Strategy*, assisting decisionmakers to understand the world around us and to act on behalf of the United States. Major accomplishments included work with military, diplomatic, and law enforcement officials in their efforts to

- Neutralize terrorists, their allies, and their plots, to include Abu Musab al Zarqawi in Iraq
- Identify and even disrupt the efforts of those seeking and spreading weapons of mass destruction
- Monitor and assist democratic reforms around the globe
- Understand the intentions and capabilities of hard-target regimes and their agents
- Watch the horizon for gathering threats and provide situational awareness during crises such as those in Lebanon and Darfur

Not all of our efforts in FY 2006 met with success, however, and significant challenges remain. In several areas, we have yet to achieve the transformation and integration of the IC called for in the Intelligence Reform and Terrorism Prevention Act of 2004. By its nature, this integration will be a long process, but its benefits in many areas are already evident, spurring increased support among the agencies and their customers for continuing the efforts at an accelerated pace. We are also seeing more clearly where the true challenges lie—and building the trust within the IC that will be necessary to address them.

In accordance with the statutory requirement to present this annual report, its text is divided into two sections. The first section states the requirements of the United States for intelligence in the next FY to come (FY 2008). The second section discusses the performance of the IC in the FY that just ended (FY 2006).

The requirements of the United States for intelligence remain large and likely to expand in the years ahead. The IC helps inform and implement decisions of our Nation's senior leaders while ensuring that the premises on which their strategic formulations rest remain valid in an ever-changing world. Doing so is all the more imperative today, with our Armed Forces engaged in Iraq, Afghanistan, and other battlefronts, and with our citizens and allies at risk of attacks from enemies bent on destruction. Our *National Intelligence Strategy* and an improved, dynamic process of identifying policymakers' priorities are helping to focus the IC's efforts on these requirements.

Requirements of the United States for Intelligence

The overarching purpose of the Intelligence Community (IC) has always been to help inform and implement decisions of our Nation's senior leaders, while ensuring that the premises on which their strategic formulations rest remain valid in an ever-changing world. The attacks of September 11, 2001 taught us that geography is no longer a bulwark against threats, and that an increasingly networked global economy can facilitate the acts of cunning adversaries who wish to harm America and its interests at home and abroad. Our service men and women on the battlefronts in Iraq and Afghanistan, moreover, face such adversaries face-to-face and supporting them in this struggle has and necessarily will continue to require a substantial share of the IC's efforts. As articulated in the first-ever *National Intelligence Strategy* (NIS) issued in October 2005, our national intelligence effort for the foreseeable future must perform five major missions to support the national security requirements of the United States:

- *Defeat terrorists at home and abroad by disarming their operational capabilities and seizing the initiative from them by promoting the growth of freedom and democracy.* The United States is fighting a war against terror in which our first priority is to identify, disrupt, and destroy terrorist organizations of global reach and attack their leadership; their command, control, and communications; and their material support and finances. Intelligence has to stay ahead of current and emerging dangers and, where possible, disrupt attacks before they materialize. No nation is safe from attack when ruthless enemies can build sanctuaries from which to spread their messages of hate and train operatives to hide in civilian populations.

- *Prevent and counter the spread of weapons of mass destruction (WMD).* The comprehensive strategy of the US government to combat WMD includes proactive counterproliferation efforts, strengthened nonproliferation efforts to prevent rogue states and terrorists from acquiring these technologies, robust methods to interdict or minimize actual attacks, and effective consequence management to respond to the effects of their use—whether these threats are posed by terrorists or hostile states. Intelligence support is vital in all of these areas.

- *Bolster the growth of democracy and sustain peaceful democratic states.* We have learned to our peril that the lack of freedom in one state endangers the peace and freedom of others, since failed states can serve as a refuge and breeding ground for extremism. Self-sustaining democratic states are essential to world peace and development, and intelligence helps decisionmakers understand and act on challenges and opportunities in this field.

- *Develop innovative ways to penetrate and analyze the most difficult targets.* America's toughest adversaries know a great deal about our intelligence system and are becoming better at hiding their intentions and capabilities. Some adversaries are ruled by closed leadership cadres and protected by disciplined security and

intelligence services. Others are amorphous groups or networks that may share common goals, training, and methods, but operate independently.

- *Anticipate developments of strategic concern and identify opportunities as well as vulnerabilities for decisionmakers.* In a world in which developments in distant reaches of the globe can quickly affect American citizens and interests at home and abroad, the IC must alert policymakers to problems before they escalate and provide insights into their causes and effects. Analysis must do more than just describe what is happening and why; it must identify a range of opportunities for (and likely consequences of) diplomatic, military, law enforcement, economic, financial, or homeland security action. To support policymakers, the IC should develop, sustain, and maintain access to expertise on every region, every transnational security issue, and every threat to the American people.

Establishing an exact order of priorities among these missions can be difficult, as they are dynamic and interdependent. A key instrument for keeping the IC attentive to both policymaker concerns and potential shocks is the *National Intelligence Priorities Framework* (NIPF), managed by the Office of the Director of National Intelligence (ODNI). The NIPF process gathers the needs of senior decisionmakers across the US government on a semi-annual basis to support prudent allocation of both collection and analytical resources for the following 6-to-12 months. In contrast to earlier attempts to create such a tool, the NIPF has benefited from ongoing engagement by the National Security Council, with two Presidentially approved updates in 2006. Review of the *NIS* every six months, moreover, will enable consideration of larger and longer-range shifts in our priorities.

Activities of the Intelligence Community in Fiscal Year 2006

The IC contributed to the security of the United States and helped advance important national interests in Fiscal Year (FY) 2006. Implementation of reforms mandated in the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 and the President's Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the WMD Commission) enhanced the IC's ability to support policymakers, senior leaders, diplomats, commanders on the battlefield, officials, and law enforcement officers. The activities of the dedicated men and women of the IC, including those who bravely gave their lives while defending the United States, made all Americans safer.

Our efforts to integrate and transform the IC are important to meeting the needs and expectations of senior decisionmakers, the US government, and the American public. Several more years will be needed to fully achieve the goals of the IRTPA and other recommendations. We have made progress, but also face several obstacles. It is essential that the IC's activities be held to high standards of efficacy—and then adjusted if they fall short. The challenges to this transformation provide the context for understanding the developments—both the achievements and the shortcomings. The following is an account of the IC's performance of its missions on behalf of the United States and an assessment of that effort in light of the resources, authorities, and guidance given to the IC to perform its duties. Its sections describe the IC's progress in FY 2006 as well as shortfalls and unfinished business.

What We Have Achieved

The DNI's *NIS* helped to guide the efforts of the IC and to tie them to the larger goals of the President's *National Security Strategy*. Released just after the start of FY 2006, the NIS marked an innovation for the IC in identifying specific missions, naming the ODNI seniors responsible for the IC's progress toward attaining them, and tying program and budget decisions to an overall strategy. As a public document, moreover, it put the DNI and his deputies on record in a way that makes all IC officers aware of where they fit in the overall scheme, and will promote greater transparency in achieving NIS objectives.

The principle underlying the *NIS* is the transformation of the Community through the integration of its functions. Its five mission objectives and ten enterprise objectives are beginning to shape the Community as they are translated into strategic implementation plans (approved by the DNI in July 2006) and policy changes. The DNI-signed capstone IC Directive 1, Policy Directive for Intelligence Community Leadership, May 2006, articulated the roles and responsibilities of the DNI and the ODNI codified in the IRTPA. This document established the National Intelligence Policy System for the management of the IC, and it comprises a framework and process for the development and conveyance of overarching policy and guidance. Forty-eight DNI policies were approved and disseminated during 2006. Strategy and policy are implemented through program and budget decisions. The ODNI has revised the National Intelligence Program (NIP) budget structure, for instance, to improve transparency and

consistency across all NIP programs, to facilitate a "performance budget," and to facilitate analysis of how well the individual NIP programs are supporting the NIS. In addition, each head of an IC element signed a Personal Performance Agreement that the DNI is using to evaluate their contributions toward realizing the IC-wide objectives articulated in the NIS.

Given the importance of the *NIS*, the achievements of the IC in FY 2006 are keyed to the following mission objectives.

Mission Objective 1: *Defeat terrorists at home and abroad by disarming their operational capabilities and seizing the initiative from them by promoting the growth of freedom and democracy.*

The IC's first priority is to prevent attacks on the American people. The Community is bringing greater efficiency and effectiveness to this effort through the DNI's National Counterterrorism Center (NCTC), the mission manager for counterterrorism, where analysts can connect to more than 30 different US government networks to create a fuller picture of potential threats. This ability was employed recently at the 2006 Winter Games in Torino, Italy, for which NCTC established a multi-agency analytic fusion center to follow potential terrorist threats. When events mandate, NCTC can also become a hub for critical intelligence support to our Nation's leaders; the Center played an important role last summer when the British thwarted the transatlantic-airline bombing plot.

The struggle against jihadi-inspired terror is a global one, without "fronts" in a conventional sense. It will necessarily be a long one, which cannot be won by military operations alone. Terrorists have grown more diverse in their inspirations, more sophisticated and adaptive in their tactics, and possibly more numerous. The difficulty of our mission to defeat them can hardly be overstated. The wars in Iraq and Afghanistan—and our intelligence efforts in support of coalition efforts in those countries—must be seen in this larger context. The IC in FY 2006 gave extensive support to national policymakers, commanders in the field, diplomats in capitals across the region, and coalition partners in both nations, as well as in other areas where jihadist terror cells are at work. Our efforts to defeat terrorists and diminish support for terrorism can be grouped in three main categories: collection, analysis and integration, and operational support.

Collection: Intelligence against the terrorism target rests on a large network of mutually dependent sensors and collectors at home and overseas. Technical collection provides vast amounts of data, and its capabilities are being modernized to keep pace with newer forms of communication and emerging opportunities. The National Security Agency's (NSA) Terrorist Surveillance Program, for instance, made critical contributions to protect American lives and interests. The IC also deployed formidable human collection assets. Several IC elements, most notably the Central Intelligence Agency (CIA), and the Defense Intelligence Agency (DIA) devised new ways to recruit assets and work with our allies to gather information in this struggle. The Federal Bureau of Investigation (FBI), with the Department of Justice, completed work to update guidelines on human source policy and validation to enhance the integrity of FBI human source collection. Other agencies, such as components of the Department of Homeland Security (DHS), monitored data to prevent suspected terrorist affiliates from entering the country or

gaining access to sensitive areas of ports and airports. Inappropriate disclosures of intelligence information, however, made it more difficult for US intelligence officers to gain the cooperation of foreign partners in this larger struggle.

Collection against terrorists in places like Iraq and Afghanistan took a substantial share of the IC's resources and efforts in FY 2006. From fielding new systems to monitor the placement of improvised explosive devices (IEDs), to exploiting documents and materials confiscated from suspects and terrorist sites, to deploying new sensors in unexpected places, the IC has worked hard to improve the volume and quality of the data it gathers. There have been notable successes, such as the elimination of al Qaeda-in-Iraq leader Abu Musab al Zarqawi, but we are under no illusions about the difficulty of the task. Indeed, we do not yet have the precision of counterintelligence and signals intelligence that we need.

Analysis and Integration. Improved collection is but one part of the intelligence campaign against terrorism. In FY 2006, the Director of NCTC built new Community processes to enhance analytic cooperation and integration. One example of this work is the *Analytic Framework for Counterterrorism*, which the DNI approved in July 2006. The *Framework* defines the roles and relationships for counterterrorism analysis and provides for planned competitive analysis on the most critical issues. It provides for a phased shift of resources—and mission—to NCTC over the next 18 months, to empower the Center to fulfill its legislative mandate and produce a range of strategic analyses. The *Framework*'s structure will help the IC use its analytic resources more efficiently, while ensuring that each agency continues to support its agency leadership and unique operational activities. It is the product of intense cross-community efforts under the collaborative leadership of the NCTC and represents an unprecedented cooperative achievement.

NCTC also supports integration and information sharing through managing the Terrorist Identities Datamart Environment (TIDE) database, which serves as the central repository for all-source information on international terrorist identities for use by the IC, law enforcement community, and others. TIDE also exports international watchlist recommendations to the Terrorist Screening Center (TSC) for use by federal agencies. TSC validates the recommendations and propagates them to federal agencies, as well as select foreign governments, who in turn, use this information to screen for terrorists. NCTC has instituted procedures to assist the TSC and other agencies charged with administering the watchlists, including support for quality control and redress mechanisms. This collective effort represents a major step forward from the pre-9/11 status of multiple, disconnected, and incomplete watchlists maintained throughout the government.

Similarly, other IC analysts are working on groundbreaking new methods for tracking and defeating terrorists abroad, while preventing the growth of radical Islam at home. For instance, the FBI expanded its analytic investment in NCTC. After completing successful pilots in 10 field offices across the country, the FBI has adopted a comprehensive "domain-management" methodology that will form the basis of its approach to analysis and integration. The Department of the Treasury has examined financial data to track money flows to groups like al Qaeda, Hamas, and Hizballah; and the DHS's Office of Intelligence and Analysis (I&A) is studying how radicalization may occur in the United States—with the ultimate objective of

finding ways of countering the message of hatred that leads to violence. In addition, DHS's Homeland Infrastructure Threat and Risk Analysis Center and its Office of Infrastructure Protection produced a steady stream of analyses for the IC and, importantly, for the private sector on potential threats to the Nation's critical infrastructure.

The Community needs to devote more analytic resources to understanding the insurgencies and the armed factions in Iraq and Afghanistan. The IC and the leaders whom it serves recognized the need for a deeper understanding of our opponents and worked throughout FY 2006 to improve that analysis. DIA and CIA both devoted large shares of their analytical efforts to this mission, developing intelligence that directly helped decisionmakers in the field and in Washington. Several IC elements are using innovative targeting methodologies to spot unknown insurgent networks and smuggling rings, uncover the financial underpinnings of the Iraq insurgency, mitigate the threat from IEDs, and understand the strengths and weaknesses of the governments in Baghdad and Kabul.

Operational Support. Since 2001, America's policymakers, diplomats, commanders, and law enforcement officials have required unprecedented intelligence support. The goal of the IC's collection and analysis is to provide support in ways that let decisionmakers take action in time to prevent attacks or catch their perpetrators. NCTC is the lead element of the US government for the "strategic operational planning" that unifies all instruments of national power to accomplish this goal. Although the Director of NCTC reports to the President regarding his responsibilities for the planning and progress of joint counterterrorism operations (other than intelligence operations), the work of the IC's collectors, analysts, and operators is still integral to accomplishing these efforts.

The efforts of the IC substantially helped other elements of the US government and foreign partners in this fight to remove terrorists from the battlefield, to disrupt their operations, and to eliminate their sources of support. Several hundred terrorists and their allies no longer pose a threat to our forces or our friends because of the work of the IC. Intelligence analysts in the Departments of State and Treasury, for example, identified the enablers of terror in the United States and abroad and helped to guide asset seizures and the imposition of sanctions. The FBI, moreover, matured and sustained an effective partnership with operational forces in a number of theaters of operation. The Bureau's expertise is part of an integrated team supporting targeting and the rapid exploitation of operational results to assess opportunities and possible threats to the homeland.

Several civilian and military agencies worked closely with the special activities of the US military in combating terrorists. In Iraq and Afghanistan, for example, the goal of the IC has been to deploy intelligence officers, analysts, and resources as far forward as possible to assist tactical operations, while enabling commanders and even small units to reach back to national resources and databases to improve their planning and situational awareness. The Joint Intelligence Operations Center (JIOC) in Iraq is beginning to benefit operations down to the battalion level via the elements of a "flat network" to pass information to the warfighter and tactical reports back to the theater and national levels.

Mission Objective 2: *Prevent and counter the spread of WMD.*

WMD in the possession of hostile states and terrorists represent one of the greatest security challenges facing the United States. Success in this mission requires the IC to collect information that addresses critical information gaps on WMD proliferation, development, and delivery. The Community also must develop information and insights to help policymakers shape counterproliferation options, strategies, approaches, and actions. In addition, the IC must effectively deal with the rapid change in science and technology worldwide, the options created by global markets, and other factors that influence WMD programs and capabilities.

The DNI established the National Counterproliferation Center (NCPC) to focus the IC toward meeting these objectives. Working in partnership with the IC's counterproliferation leadership, NCPC began implementing a three-year program designed to strengthen, integrate, and focus IC efforts. As a first step, NCPC and its Community partners began work to identify and implement integrated strategies to address critical gaps on high-priority problems: countries of concern, fissile material security, proliferation, biological and chemical threats; Strategic Interdiction, and over-the-horizon proliferation threats from state and non-state actors. NCPC also developed an Innovation Fund to promote multi-agency solutions to technical and other counterproliferation problems and initiated a campaign to help collection and analysis stay current with evolving technology. These and other initiatives are designed to help the Community work together to use innovation and technology to expand its capabilities in support of the counterproliferation mission.

The Community monitored the status of nuclear and WMD activities in many states of concern in FY 2006, using all available means and paying particular attention to events in North Korea and Iran. NSA, the National Reconnaissance Office (NRO), and the National Geospatial-Intelligence Agency (NGA) have been indispensable in this sustained effort. More broadly, the IC agencies worked to forge a closer integration between the elements, disciplines, and capabilities of the Community. CIA has been a leader in IC efforts to create new sources, collection platforms, and sensors, while DIA initiated a program to integrate expertise in developing focused human sources. Finally, significant information on WMD programs of concern can be assembled from open sources (particularly the Internet). This effort, in turn, is complemented by insights gained from outside experts. The DNI Open Source Center, based in and administered by CIA, has the lead for the IC here.

Analysis is key to making sense of the data and finding opportunities to take timely action. Elements of the IC that historically have been focused on domestic topics significantly improved their analytical capabilities in this area. The FBI, for instance, created a WMD directorate and partnered with the Department of Energy (DOE) to improve forensic analysis. DHS/I&A began a special assessment of the WMD threat to the homeland. Several IC elements worked to identify personnel and funds involved in WMD programs, in addition to monitoring materiel and shipments. Finally, DOE is implementing an August 2006 Presidential directive to create a government-wide database on international nuclear material holdings and security.

Countering WMD is a priority for officials and commanders across the US government, and enhanced intelligence support helped them formulate policies and interventions ranging from demarches to interdictions. The IC provided thousands of reports on these issues and devoted

many man-hours to assist policymakers, diplomats, commanders, and officials in gaining situational awareness and in spotting opportunities, especially with regard to Iran and North Korea. The Office of Intelligence and Analysis of the Department of the Treasury played an integral role in identifying networks supporting WMD proliferators and in taking action to disrupt their activities. DIA, moreover, provided analytical and technical support to coalition forces in Iraq in locating and removing hundreds of pre-1991 chemical weapons. Finally, the multi-agency effort at the National Maritime Intelligence Center (NMIC), led by the US Navy and US Coast Guard, provided analytical expertise dedicated to identifying and monitoring threats in the maritime domain, including the movement of WMD and related materials, as well as the tracking of sea-borne, terrorist-related activity, illicit narcotics, and other high-interest cargo.

Mission Objective 3: *Bolster the growth of democracy and sustain peaceful democratic states.*

The President's *National Security Strategy* emphasizes the opportunity that our Nation has to encourage democracy's growth in many regions. IC officers work on a daily basis with intelligence and security counterparts around the world. Their contacts help to build understanding of the United States and its policies, and to reassure friends and win new allies, and to bolster their capabilities against common enemies. By statute, the CIA plays the lead role in coordinating such exchanges, but vital contacts are also maintained by other components of the IC, particularly the military attachés and intelligence elements of the Department of Defense. In addition, intelligence collectors and analysts provide a great deal of information to help policymakers understand the spread of free institutions and the perils they often face. A groundbreaking National Intelligence Assessment on global prospects for democratization, for example, provided policymakers with a framework for prioritizing the importance of individual countries where democratization is a challenge. In addition, the Department of State's Bureau of Intelligence and Research (INR) oversees opinion polling that helped the United States understand attitudes toward democratic transitions in Latin American, Eastern Europe, the Middle East, and Central Asia, as well as the integration of Muslim populations in Europe. CIA and INR have also connected with outside experts to help understand how to build democracy in weak states and to stabilize transitioning ones.

Mission Objective 4: *Develop innovative ways to penetrate and analyze the most difficult targets.*

America's intelligence capabilities were originally created in no small part to deal with the threats posed by the emergence and persistence of closed, ideological regimes and their destabilizing effects on their neighbors. The IC in FY 2006 devoted significant resources to this problem. It made progress in some areas while lagging in others—particularly in divining the near-term intentions of certain foreign leaders and in spotting activities that they wished to conceal. Of greatest concern are the WMD programs and the improvement of ballistic and cruise missile arsenals of these states, but several nations and even non-state actors demonstrated their ability to deploy conventional weapons systems in surprising and dangerous ways. As in the proliferation field, our expert analysts and collectors working foreign space, missile, intelligence, and cyber capabilities are pressed by demands for urgent support to senior decisionmakers and may not have ample opportunities to think strategically about their accounts.

IC leaders believe the solution to the "hard-targets" problem lies in close partnership between collection and analysis and intensified collaboration among all intelligence agencies and disciplines. Directorates of the ODNI surveyed intelligence customers for their needs with regard to several hard-target countries in response to a National Security Council request to evaluate the IC's posture and capabilities, and gave collectors a listing of the significant gaps in analysts' understanding of the most difficult targets for collection emphasis. DNI-appointed Mission Managers are leading efforts to close gaps against several countries, and the ODNI's Multi-Intelligence Working Group seeks to make it easier for the IC to identify and promote cross-agency innovations for solving problems of national significance.

The Community mounted innovative efforts to close these and other gaps. The intelligence agencies of the US Air Force and the US Navy are paying particular attention to foreign long-range strike, sea-denial, and anti-satellite capabilities. One significant innovation in this regard has been the modeling of foreign naval capabilities to improve our own tactics and net assessments. The FBI is working with the CIA to develop approaches to align their focus and integrate their respective capabilities in a coordinated effort to have the greatest impact on the Nation's most difficult targets. This effort will engage both operational and analytic capacity. The CIA, in addition, provided its case officers with better analytical support (in part through task forces to coordinate work on hard targets), and developed and shared new tools to enable technical collection and operations. In enhancing its collection and analysis, moreover, the DNI Open Source Center is complementing technical collection in a cost-effective manner.

Countering the intelligence activities of hard-target states is a *NIS* priority. Their efficient intelligence and security services are partly what make their intentions and capabilities so difficult to ascertain in the first place. The Office of the National Counterintelligence Executive (ONCIX) in FY 2006 undertook to re-write the Nation's counterintelligence strategy to align it with NIS objectives. ONCIX fostered exchanges on activities of foreign intelligence services between analysts and collectors around the Community to improve collection requirements. The ONCIX also led a year-long Community effort against one hard target that set common goals, unified US collection and counterintelligence activities, and increased information sharing. This effort resulted in new operations and a better sense of the collection gaps and is now an ongoing program managed by the CIA. In addition, the US Coast Guard, with the assistance of several IC elements, monitored suspicious ships and sailors in US territorial waters and spotted strong indications that some were being used for intelligence collection against the US military.

Mission Objective 5: *Anticipate developments of strategic concern and identify opportunities as well as vulnerabilities for decisionmakers.*

American intelligence has always been expected to watch the horizon for gathering threats and to warn decisonmakers in time for them to act. On a daily basis, the IC provides truly remarkable support and depth of insight.

The ODNI in FY 2006 continued its campaign to improve the President's Daily Brief (PDB), integrating all the analytical agencies into the PDB process to ensure that the President and his senior advisers receive the best available intelligence judgments, including alternative viewpoints. The IC in FY 2006 worked to maintain the high level of support it provides to national decisionmaking, while working to correct issues identified in earlier inquiries. In addition, the National Intelligence Council (NIC) now serves as the primary mechanism for providing intelligence support to the discussions of the principals and their deputies represented on the National Security Council and the Homeland Security Council.

With so many IC resources dedicated to the War on Terror and WMD programs in closed regimes, the Community's collection efforts still have to devote significant attention to potential or emerging threats of strategic consequence. The Open Source Center plays a large role here; its officers are monitoring an expanding range of sources and are making their analyses more relevant to the concerns of senior policymakers.

NGA, moreover, revamped its broad-area search program and used it to discover several previously unknown sites of interest to US intelligence. The FBI's National Security Branch (NSB) is striving to achieve and sustain an appropriate operational balance between strategic and tactical analysis to understand homeland threats in a strategic context. The FBI created 16 senior-level positions in its intelligence directorate to provide a dedicated cadre of senior analysts. One challenge to improving the coverage of emerging and strategic issues across the IC has been the diversion of resources to current crisis support in places like Lebanon and Darfur (although a new model to rapidly "lift-and-shift" IC collection resources against these and other crises proved very effective in focusing Community efforts and delivering important new intelligence).

The IC is shifting to address the NIS's emphasis on strategic analysis and reaching out to outside expertise. The NIC's new Long-Range Analysis Unit served as the lead unit for interagency projects involving integrated, in-depth and multidisciplinary assessments of many strategic issues. It also partnered with INR to create government-private working groups on several topics. CIA remains an IC leader in conducting strategic analysis; it has devoted particular attention to studying issues of concern in the Muslim world such as Sharia, Islamic economic ideas, and financial support for terrorist groups.

Analysis and collection helped diplomatic and military operations abroad and protected the United States against a range of conventional and unconventional threats. As an example of the latter, IC agencies cooperated extensively with each other, and with public and private organizations and experts, in FY 2006 to monitor the threat of avian influenza. The IC brought together expertise from across US government to build and share understanding of the avian flu virus and related issues such as migratory bird patterns, poultry production, and other key data that the IC simply would not have had otherwise. Several agencies, from the CIA to DHS to DIA's Armed Forces Medical Intelligence Center, contributed substantially to the larger effort.

What We Will Achieve

The IC in FY 2006 can claim many successes, but we cannot rest on prior accomplishments as we still face serious challenges. Our capacity to maintain competitive advantages over forces inimical to America's security and interests depends in part on our ability to transform our capabilities faster than threats emerge, protect what needs to be protected, and perform our duties according to the law. Doing these things more effectively will ensure America possesses an IC that is able to shift rapidly and effectively to the new missions that will inevitably arise in the future. Improvements to the intelligence enterprise in the following areas should help make it better able to perform all the missions that fall to it.

We need to integrate intelligence capabilities to address threats to the homeland, consistent with US laws and the protection of privacy and civil liberties. Before 2001, the elements of the IC rarely acted as a system in conjunction with one another and with state, local, and tribal authorities. Building such a system from new and legacy elements has to be a methodical process. The FBI is forging broader alliances with the IC and leveraging its longstanding law enforcement partnership with state, local, tribal, and private sector entities to build a network of intelligence partnerships to optimize our capacity to understand and act on threats. DHS's I&A is posting liaison officers to state-level and other select fusion centers being formed across the country to enhance intelligence and information collaboration, in partnership with the FBI to codify expectations for their roles in these centers and to put at least one special agent and one intelligence analyst in the leading fusion center in each state. I&A is also promoting corporate governance to the Department's diverse intelligence activities, assessing where gaps and overlaps may exist. DHS elements (including the US Coast Guard) are better integrated with the IC to guard America's borders and ports; indeed, I&A has developed an Intelligence Campaign Plan focused on transnational threats to our borders. In response to the President's new National Strategy for Maritime Security, the ODNI, with support from the US Navy and US Coast Guard, created the Global Maritime Intelligence Integration initiative to be responsible for the effective government-wide access to maritime information and data critical to intelligence production. Finally, the DNI's Civil Liberties and Privacy Office has taken a lead role in ensuring that civil liberties and privacy concerns are appropriately incorporated into all these efforts through its participation with other IC components and in its review of intelligence initiatives that potentially raise such concerns.

We must build analytic expertise, methods, and practices; and help IC professionals to tap expertise wherever it resides and to explore alternative analytic views. Roughly half of the workforce has fewer than five years experience, and the newer analytical elements at Treasury and Homeland Security have an especially difficult challenge. Training, tasking, connectivity and even physical space are all issues for them and for analysts at the FBI's new NSB. Helping analysts at all agencies work more efficiently and collaboratively is another challenge, though analysts from the new elements are already contributing to the IC's work and gaining the respect of their peers in the older intelligence agencies. Several agencies are exploring new software solutions to help analysts be more productive, and the advent of Intellipedia—which has been well reported on in the news media—may presage a true cultural shift in the way that analysts and all IC officers do their work. Finally, the IC is working to raise the standards and expectations for analytic practices and integrity, and to benefit from expertise wherever it can be

found. ODNI has responded to the challenge with several initiatives launched by its Office of Analytic Integrity and Standards, including "Analysis 101," a joint course in critical thinking and intelligence-cycle skills; an evaluation program for finished intelligence products, the results of which are fed back into the agencies and schoolhouses; and a research program on analytic methodologies which encompasses workshops and conferences, as well as research projects being conducted by a group of ten outside experts. Moreover, CIA, INR, and the NIC sponsored dozens of conferences and workshops with academic and private experts in FY 2006, with the initiatives of CIA's Global Futures Forum and the ODNI's Private Sector Initiative being two good examples.

We still need to re-balance, integrate, and optimize collection capabilities to meet current and future customer and analytic priorities. Collection is by far the most expensive activity undertaken by the IC, but it is also what gives the IC its "competitive advantage" in protecting the United States and its interests. The Nation's intelligence satellite constellations, managed by the NRO, provide the indispensable foundation that enables many of the IC's capabilities. The DNI has approved the Integrated Collection Architecture (ICA) to balance the resources and needs of all the Community's systems, and the managers of the ICA, in conjunction with the Mission Requirements Board, are now validating needs for national intelligence capabilities and using that knowledge to fill gaps. Human intelligence, moreover, remains a concern. In coordination with the CIA's National Clandestine Service, FBI, DIA, and the military Services are improving the training, tradecraft, and integration of their case officers and operations.

We are working to attract, engage, and unify an innovative and results-focused IC workforce. The IC was losing the "war for talent," finding it difficult to recruit, motivate, and retain the best candidates for its positions. In recent years, IC agencies have increased their applicant pool of motivated entry-level applicants, but recruiting and retaining high-level skills in critical languages and scientific and technical fields remains difficult, and competition with contractors for top skills presents a new challenge. The ODNI's Chief Human Capital Officer is leading efforts to address these problems, gathering statistics on the workforce's (both contract and civilian) qualifications and attitudes, rationalizing recruiting plans and training programs (especially in foreign languages, a chronic weak point), and ensuring high-quality benefits programs for IC officers. Yearly changes in hiring allocations have compounded difficulties in ensuring that there will be open billets for qualified personnel in advanced training programs when they graduate and are seeking employment. To counter this trend, efforts to promote and lead IC-wide education and training efforts have been initiated, in part to build a common Community *ethos*, and promote networking across the IC. These specialized training initiatives include a requirements-driven training planning system that addresses current and projected mission-critical skill requirements; joint IC training; increasing training opportunities open to IC personnel outside the IC training provider organizations; and advanced educational technology (to include an on-line searchable training catalog, E-learning resources, and modeling/simulation in both classroom and online courses).

IC senior leaders believe strongly that diversity is a mission-critical imperative, essential to ensuring our Nation's security and success in the war on terror. To combat new, global, and increasingly complex national security threats, the IC must employ, develop, and retain a dynamic, agile workforce that reflects diversity in its broadest context—cultural backgrounds,

ethnicity, race, gender, language proficiency, perspectives, experience, and expertise. While the IC continues to move forward in achieving these goals, much more needs to be done to accelerate our progress and focus on results in diversity.

Results show that we continue to make steady, though very modest, gains in the representation of minorities and women in the major IC components. We are also making gains in hiring, developing, recognizing, promoting, and retaining minorities and women in the IC overall, in core occupations, and in the higher pay grades. Improvement is needed, particularly in hiring and retaining persons with disabilities, and our results continue to lag significantly behind other Federal government and Civilian Labor Force external benchmarks.

We must ensure that IC members and customers can access the intelligence they need when they need it. Sharing information is an issue much bigger than the information technology (IT) field. Each agency and department runs legacy systems that were planned and in many cases deployed long before the Internet age. They were not built to talk to one another, and the technical challenges involved with making them communicate (to create a common IC identification badge, for example) have proved daunting. Fixing them demands vast resources to harmonize various systems and to keep them secure while also modernizing agency IT facilities and infrastructures at the speed of the Information Revolution. Another considerable part of the problem is the dearth of secure physical space to hold the equipment and the people to run it, especially in cramped headquarters buildings in Washington, DC, and even in agencies like NSA or CIA that are already struggling to seat all their new analysts, officers, and administrative personnel. Solutions in the information-sharing field will involve policy changes as well, including sharing information with non-Federal partners and the private sector. The DNI Chief Information Officer (CIO) is gradually getting control of these issues in part by insisting that all significant IT deployments in the Community be consistent with a common IC enterprise architecture and with the Federal enterprise architecture. As part of this, the DNI CIO has inventoried the IC architecture with an eye to pointing the way for IC members to modernize in compatible ways. In addition, the DNI CIO established a joint office with the Department of Defense CIO for managing the development and provision of cross-domain solutions that enable the national security systems to move information between networks operating at different security classifications, thereby improving collaboration and sharing.

We are still building the foreign intelligence relationships to help us meet global security challenges. The IC cannot win against our adversaries on its own, but its necessary work with foreign intelligence and security services must proceed on a planned and prudent basis. Progress has been made. In fact, the IC partnered with the Department of Defense to provide Commonwealth partners access to information on a classified US system to improve our combined ability to fight the wars in Iraq and Afghanistan. The ODNI also completed the first-ever inventory of all US intelligence liaison relationships, and is using the knowledge gained to maximize our reach and minimize the real and potential costs of working with foreign partners. Its Foreign Relations Coordination Council (which includes members from around the IC) will help in this task. Two issues are of particular concern: how to set policies to expand and govern sharing of information and secure network access with foreign partners, and how to find the resources and access to assess the strengths and weaknesses of current and potential partners.

We need clear, uniform security practices and rules that allow us to work together, protect our Nation's secrets, and enable aggressive counterintelligence activities. The challenges in this field are significant, but a methodical and measurable approach is yielding some early success. The goal is easy to state—to share what needs to be shared, while defending what needs to be defended—but is not so easily achieved. Reform of security clearance procedures remains incomplete (and with it our ability to hire critical skill sets). Many of the means for reform in the personnel field lie outside the DNI's purview (the Office of Personnel Management conducts most clearance investigations for the US government). ODNI is working with the Office of Management and Budget, which has the national mandate for security clearance reform, and with the agencies most directly concerned, contributing to several national-level working groups on this issue. In the areas it can control (i.e., the elements funded under the NIP), the ODNI has assumed an aggressive oversight role and imposed reporting requirements on the IC agencies that conduct their own security clearance investigations and adjudications. This has allowed us to gauge the scope of the problem and to measure the progress made towards achieving an IC-wide solution. Finally, agencies are still reluctant to share counterintelligence information. In some cases this reluctance stems from concern about protecting sources and methods.

We need path-breaking scientific and research advances that will enable us to maintain and extend intelligence advantages against emerging threats. Our technical intelligence advantages are under siege. The rapid pace of technological change is forcing the Community to sprint just to stay even, and forcing wholesale policy and resource shifts on all IC elements. In addition, the IC is learning new ways to analyze foreign plans and activities in emerging technologies, particularly their intentions and abilities to illegally acquire American scientific and technological achievements, and to mount cyber attacks against us or our allies. The latter issue is particularly difficult, despite innovative work by the IC in simulating foreign capabilities. Solutions will have to come from our own spirit and tradition of innovation. The new Intelligence Advanced Research Projects Activity, for instance, will nurture good ideas for sharing and growing science and technology expertise. IC elements are particularly creative at devising and fielding advanced sensors to spot adversary personnel, equipment, and processes, and the National Signatures Program run by DIA supports both the IC and the Department of Defense by building and sharing a very large database of "signatures" acquired by our technical means. In keeping with its statutory mandate to ensure that the use of technologies sustain, and do not erode, privacy protections, the DNI's Civil Liberties and Privacy Office works closely with scientific and technological officers to identify and address privacy and civil liberties issues as they arise.

We should learn from our successes and mistakes to anticipate and be ready for new challenges. The IC has rarely reflected on its experiences with the goal of serving the Nation's interests with greater proficiency and ensuring that it can continue that service even in a crisis. The ODNI is leading efforts to redress this deficit, encouraging historical activities throughout the IC, using lessons-learned to help train a new generation of analysts, and promoting enterprise-wide after-action reviews, such as that conducted following the North Korean missile launches last July. The IC is also sharing more representatives among interagency exercises, and preparing in advance to handle both deployments and emergencies.

We are still eliminating redundancy and programs that add little or no value and re-directing savings to existing and emerging national security priorities. The ODNI is making frequent use of the new budgetary powers granted by the Intelligence Reform Act to manage and shape the Community. The FY 2008 NIP is critical; it marks the first one that the DNI led all steps of the process. In other areas, the ODNI worked with the office of the Undersecretary of Defense for Intelligence to deconflict the NIP and the Military Intelligence Program (MIP), ensuring they are not duplicative and do not create gaps, and that the guidance they give their respective programs is harmonized. When IC programs or personnel are to be shifted across NIP programs, moreover, ODNI has worked with the departments and agencies involved to ensure that the moves can be done with minimal disruption to operations and capabilities. The ODNI implementation of the new acquisition powers is still a work in progress; its Milestone Decision Authority, for instance, pertains only to "major" programs funded in whole in the NIP. Nevertheless, the tying together of budgets, programs, plans, and strategy has created a powerful demonstration effect on the IC elements, several of which are now starting to model their own internal governance processes on the ODNI model. Crucial to this, also, has been the development of the aforementioned Integrated Collection Architecture inter-agency review process for all NIP- and MIP-funded technical collection programs.

Conclusion

The IC has embraced the reforms of the past two years and is implementing them, resulting in improvements to all aspects of its work. Integration is not just a process between agencies; it is also a process within the agencies as we try to coordinate the insights and work of the various intelligence disciplines and processes. By its nature, this integration will be a long process, but its benefits are already being realized and creating increased support among the agencies and their customers for continuing the efforts at an accelerated pace. We are also seeing more clearly where the true challenges lie—and building the trust within the IC that will be necessary to address them.

Appendix: Organizational Change in the Intelligence Community

The Intelligence Community (IC) in Fiscal Year (FY) 2006 saw significant growth of its central management capabilities. The task of the Office of the Director of National Intelligence (ODNI) is to enable all IC elements to do what they do best while integrating them into a more cohesive, collaborative, and effective Community. This vital organization-building work continued at a rapid pace over the last year, and it is worth recounting in some detail as it provides the backdrop for the successes and shortcomings discussed in the body of this report.

The progress made in FY 2006 built upon the achievements of the watershed events of the year before. Led by the Office of the Director of National Intelligence, the IC in FY 2005 implemented the broad changes mandated by the Intelligence Reform and Terrorism Prevention Act. We worked to better collect the right intelligence in the best ways possible with the establishment of the FBI's National Security Branch (NSB) and the creation of the CIA's National Clandestine Service. We strengthened our analytic work with a renewed focus on quality, objectivity, and timeliness. We began dismantling stovepipes through the creation of "mission managers" focusing on our hardest targets and most looming threats. And we developed a science and technology agenda that identified major unmet needs for the Community and focused our work against them. In short, we laid the groundwork for significant progress and reform.

In FY 2006 the ODNI grew from a fledgling staff overseeing several legacy offices into a functioning and integrated organization. It co-located most of its components in temporary quarters at Bolling Air Force Base in Washington, DC, and recruited staff to achieve the congressionally directed missions and functions of the ODNI. In so doing, it became more independent of the direct administrative support from the CIA that was essential to the initial establishment of the ODNI.

Several IC agencies experienced significant changes as well. The CIA revised its management structures to reflect the adjustments to its responsibilities mandated by the Intelligence Reform Act. CIA grew rapidly, hiring a record number of new employees. Indeed, 40 percent of its workforce has been hired since September 11, 2001. The quality of its new hires is high, but ensuring they receive the appropriate training and develop expertise will be a challenge for several years to come.

The Department of Defense (DoD) also undertook a major change to its intelligence effort, creating Joint Intelligence-Operations Centers (JIOCs) in each combatant command (and a complementary Defense JIOC in the DIA—which also operates as the US Strategic Command's JIOC). The JIOC system is intended to provide combatant commanders with the full spectrum of intelligence support from organic DoD and national systems and expertise, while providing access to national and tactical-level data and reports as broadly as possible among customers in the field, in theater, and in Washington. When North Korea launched a series of missiles in July 2006, the JIOC system demonstrated the value of an IC enterprise capable of integrating and

synchronizing planning and execution for intelligence operations. The ODNI is maintaining a close relationship with DoD to ensure the JIOC concept succeeds.

The FBI built up its new NSB. The NSB combines the missions, capabilities, and resources of the counterterrorism, counterintelligence, intelligence activities of the FBI, along with a newly established weapons of mass destruction element, into an integrated capability to address national security intelligence requirements through the collection of intelligence in the United States. These actions marked not just an organizational change, but changes in doctrine, policy, procedures, partnerships, and training.

Other elements of the IC also saw important changes. The Drug Enforcement Administration (DEA) returned to the IC in FY 2006. Through its new Office of National Security Intelligence, DEA will enjoy better access to valuable intelligence, and give IC elements greater insight into important law enforcement issues and activities. The Office has been given space and connectivity, and is busy hiring required staff. The Department of Energy (DOE) merged its intelligence and counterintelligence offices, and is also incorporating the National Nuclear Security Administration under the combined Office of Intelligence and Counterintelligence. Both of these moves in DEA and DOE were facilitated by budgetary actions undertaken by the ODNI. The departmental IC elements in general are much more engaged with the rest of the IC, sharing products and viewpoints more easily, and benefiting from better access to products from the larger agencies.

Acronyms

CIA	Central Intelligence Agency
CIO	Chief Information Officer
DEA	Drug Enforcement Administration, Department of Justice
DIA	Defense Intelligence Agency, Department of Defense
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOE	Department of Energy
FBI	Federal Bureau of Investigation
FY	Fiscal Year
I&A	Office of Intelligence and Analysis, Department of Homeland Security
IC	Intelligence Community
ICA	Integrated Collection Architecture
IED	Improvised explosive device
INR	Bureau of Intelligence and Research, Department of State
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
IT	Information Technology
JIOC	Joint Intelligence Operations Center
MIP	Military Intelligence Program, Department of Defense
NCIX	National Counterintelligence Executive
NCPC	National Counterproliferation Center
NCTC	National Counterterrorism Center

NGA	National Geospatial-Intelligence Agency
NIC	National Intelligence Council
NIP	National Intelligence Program
NIS	*National Intelligence Strategy*
NIPF	*National Intelligence Priorities Framework*
NRO	National Reconnaissance Office
NSA	National Security Agency
NSB	National Security Branch, Federal Bureau of Investigation
ODNI	Office of the Director of National Intelligence
ONCIX	Office of the National Counterintelligence Executive
PDB	President's Daily Brief
TIDE	Terrorist Identities Datamart Environment
TSC	Terrorist Screening Center
WMD	Weapons of Mass Destruction