Intelligence Issues for Congress

Marshall Curtis Erwin
Analyst in Intelligence and National Security

April 23, 2013

Congressional Research Service
7-5700
www.crs.gov
RL33539

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

To address the challenges facing the U.S. intelligence community in the 21st century, congressional and executive branch initiatives have sought to improve coordination among the different agencies and to encourage better analysis. In December 2004, the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) was signed, providing for a Director of National Intelligence (DNI) with authorities to manage the national intelligence effort. The legislation also established a Director of the Central Intelligence Agency (CIA).

Making cooperation effective presents substantial leadership and managerial challenges. The needs of diverse intelligence "consumers" must all be met, using many of the same systems and personnel. The DNI has substantial statutory authorities to address these issues, but the organizational relationships remain complex, especially for intelligence agencies that are part of the Defense Department. Members of Congress in their oversight role may seek to observe the extent to which effective coordination is accomplished.

The intelligence community, which comprises 17 agencies, has experienced a decade of budgetary growth. That era was typified by (1) institution building with embryonic organization such as the Office of the DNI and other new or evolving intelligence components, (2) information sharing and collaboration across those institutions, and (3) a focus on counterterrorism.

While those issues will remain areas of congressional interest, Members will likely confronted by a new set of intelligence challenges resulting from budgetary realities and from second-order effects stemming from post-9/11 changes. These include:

- **Consolidation and redundancy**. Intelligence collection systems are expensive and some critics suggest there have been elements of waste and unneeded duplication of effort. The Administration is considering long-term reductions with an emphasis on potentially redundant information technology systems. There is great concern, however, that any reductions be carefully made to avoid curtailing capabilities that have become integral to military operations and to policymaking in many areas.
- **Information security and management**. The WikiLeaks disclosures that began in 2010 and other recent incidents of unauthorized disclosure of classified information have drawn considerable attention to the risks that widespread information sharing entails. Investigations into the 2009 Christmas day bombing attempt and the Fort Hood shooting also suggest analysts are now challenged to synthesize the large volumes of information being shared.
- **Intelligence support to counterterrorism and operations**. The Administration's targeting killing program raises legal, jurisdictional, and efficacy issues. Broader questions have also been raised about whether intelligence agencies have become too focused on counterterrorism to the detriment of other national security priorities and whether some of those functions should be transitioned to U.S. military control, allowing intelligence agencies to focus on traditional collection and analysis.

Contents

Appendixes

Contacts

Most Recent Developments

Intelligence officials and Members of Congress are addressing ways to reduce intelligence spending while protecting core capabilities. Director of National Intelligence (DNI) James R. Clapper Jr. recently stated that sequestration would require a 7% cut, or roughly $4 billion, to the National Intelligence Program (NIP) budget and warned of reduced global coverage and decreased human and technical intelligence collection. Mr. Clapper also warned of repercussions similar to those that occurred in the 1990s when the intelligence community saw a 23% cut in its budget, resulting in a "damaging downward spiral."[1] Those cuts allegedly distorted the intelligence workforce, resulting in what is sometimes referred to as a "bathtub" shaped employment curve, with large numbers of older employees and new hires but few mid-level professionals capable of steering the community through post-9/11 changes.

Congress completed action on the FY2013 intelligence authorization legislation (S. 3454) in December 2012. The Senate passed its version of the bill by voice vote on December 28. The House approved the Senate version by a 373-29-29 vote on December 31. The final bill was signed into law by the President on January 14, 2013 (P.L. 112-277). The bill reflected funding above the President's request but below the $53.9 billion appropriated for FY2012.

Background and Analysis

The attacks on the World Trade Center and the Pentagon on September 11, 2001, dramatically demonstrated the intelligence threats facing the United States in the new century. In response, Congress approved significantly larger intelligence budgets and, in December 2004, passed the most extensive reorganization of the intelligence community since the National Security Act of 1947. The Intelligence Reform and Terrorism Prevention Act of 2004 (hereinafter, the "Intelligence Reform Act") (P.L. 108-458) created a Director of National Intelligence (separate from a Director of the Central Intelligence Agency) who heads the intelligence community, serves as the principal intelligence adviser to the President, and oversees and directs the acquisition of major collections systems. As long urged by some outside observers, one individual is now charged with concentrating on the intelligence community as a whole and possesses statutory authorities for establishing priorities for budgets, for directing collection by the whole range of technical systems and human agents, and for the preparation of community-wide analytical products.

P.L. 108-458 was designed to address the findings of the National Commission on Terrorist Attacks Upon the United States, known as the 9/11 Commission, that there has been inadequate coordination of the national intelligence effort and that the intelligence community, as then organized, could not serve as an agile information gathering network in the struggle against international terrorists. The commission released its report in late July 2004, and Congress debated its recommendations through the following months. A key issue was the extent of the authorities of the DNI, especially with regard to management and budgeting for technical collection systems managed by Defense Department agencies. In the end, many of the recommendations of the 9/11 Commission regarding intelligence organization were adopted after

[1] See Senate Select Committee on Intelligence hearing on "Security Threats to the United States," March 12, 2013.

a compromise provision was included that called for implementing the act "in a manner that respects and does not abrogate" the statutory authorities of department heads.

For additional information about intelligence community reform, background on intelligence collection disciplines, and intelligence budgeting, please see **Appendix A** to this report. The text below provides a brief overview of the intelligence community and of enduring intelligence oversight issues and then discusses specific topics that may be addressed by the 113th Congress.

Intelligence Community

The intelligence community (defined at 50 U.S.C. 401a(4)) consists of the following:

The Office of the Director of National Intelligence
Central Intelligence Agency (CIA)
Bureau of Intelligence and Research, Department of State (INR)
Defense Intelligence Agency (DIA)
National Security Agency (NSA)
National Reconnaissance Office (NRO)
National Geospatial-Intelligence Agency (NGA)
The National Security Branch, Federal Bureau of Investigation (FBI)
Army Intelligence
Navy Intelligence
Air Force Intelligence
Marine Corps Intelligence
Coast Guard Intelligence
The Office of Intelligence and Analysis, Department of the Treasury
The Office of Intelligence, Department of Energy
The Office of National Security Intelligence, Drug Enforcement Administration (DEA)
The Office of Intelligence and Analysis, Department of Homeland Security

Except for the CIA, intelligence offices or agencies are components of Cabinet departments with other roles and missions. The intelligence offices/agencies, however, participate in intelligence community activities while supporting the other efforts of their departments.

The CIA remains the keystone of the analytic efforts of the intelligence community. It has all-source analytical capabilities that cover the whole world outside U.S. borders. It produces a range of studies that address virtually any topic of interest to national security policymakers. The CIA also collects intelligence with human sources and, on occasion, undertakes covert actions at the direction of the President. (A covert action is an activity or activities of the U.S. government to influence political, economic, or military conditions abroad, where it is intended that the U.S. role will not be apparent or acknowledged publicly.)

Three major national-level intelligence agencies in the Department of Defense (DOD)—the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the National Geospatial-Intelligence Agency (NGA)—absorb the larger part of the national intelligence budget. NSA is responsible for signals intelligence and has collection sites throughout the world. The NRO develops and operates reconnaissance satellites. The NGA prepares the geospatial data—ranging from maps and charts to sophisticated computerized databases—necessary for humanitarian operations and for targeting in an era in which military operations are dependent upon precision-guided weapons. In addition to these three agencies, the Defense Intelligence Agency (DIA) is responsible for defense attachés and for providing DOD with a variety of analytical products. It serves as the premier all-source analytic unit within DOD. Although the

Intelligence Reform Act provides extensive budgetary and management authorities over these agencies to the DNI, it does not revoke the responsibilities of the Secretary of Defense for these agencies.

The State Department's Bureau of Intelligence and Research (INR) is one of the smaller components of the intelligence community but is widely recognized for the high quality of its analysis. INR is strictly an analytical agency; diplomatic reporting from embassies, though highly useful to intelligence analysts, is not considered an intelligence function (nor is it budgeted as one).

The key intelligence functions of the FBI relate to counterterrorism and counterintelligence. The former mission has grown enormously in importance since September 2001, many new analysts have been hired, and the FBI has been reorganized in an attempt to ensure that intelligence functions are not subordinated to traditional law enforcement efforts. Most importantly, law enforcement information, including counterterrorism and counterintelligence information, is now expected to be forwarded to other intelligence agencies for use in all-source products.

The intelligence organizations of the four military services concentrate largely on concerns related to their specific missions. Their analytical products, along with those of DIA, supplement the work of CIA analysts and provide greater depth on key military and technical issues.

The Homeland Security Act (P.L. 107-296) provided the new Department of Homeland Security (DHS) responsibilities for fusing law enforcement and intelligence information relating to terrorist threats to the homeland. The Office of Intelligence and Analysis in DHS participates in the inter-agency counterterrorism efforts and, along with the FBI, has focused on ensuring that state and local law enforcement officials receive information on terrorist threats from national-level intelligence agencies.

The Coast Guard, now part of the DHS, deals with information relating to maritime security and homeland defense. The Energy Department analyzes foreign nuclear weapons programs as well as nuclear nonproliferation and energy-security issues. It also has a robust counterintelligence effort. The Treasury Department collects and processes information that may affect U.S. fiscal and monetary policies. Treasury also covers the terrorist financing issue.

Authorization Legislation

Annual intelligence authorization bills were enacted from FY1979 through FY2005, providing congressional authorization for intelligence programs and guidance to the several intelligence agencies in specific provisions and report language. No intelligence authorization legislation was enacted between December 2004 and October 2010.

Annual intelligence authorization acts were first passed in 1978 after the establishment of the two congressional intelligence committees. These acts provided specific authorizations of intelligence activities and were accompanied by reports that provided detailed guidance to the nation's intelligence agencies. The absence of intelligence authorization acts meant that key intelligence issues were addressed in defense authorization acts and defense appropriations acts that focused primarily on the activities of the Department of Defense. Several Members have maintained that this procedure resulted in misplaced priorities and wasteful spending estimates that could run into billions.

However, over the last two years, Congress has met its statutory requirement by passing three Intelligence Authorization bills (for FY2011, FY2012, and FY2013) that included classified schedules of authorizations and that were signed into law. Most recently, in December 2012, both the House and Senate passed S. 3454, the Intelligence Authorization for FY2013, which was signed into law by the President on January 14, 2013 (P.L. 112-277). Key issues debated during the passage of these bills included the adequacy of Director of National Intelligence (DNI) authorities, Government Accountability Office (GAO) audit authority over the Intelligence Community, and measures to combat national security leaks. These three bills appear to reflect a determination to underscore the continuing need for specific annual intelligence authorization legislation.

For a complete treatment of intelligence authorization issues, see CRS Report R40240, *Intelligence Authorization Legislation: Status and Challenges*, by Marshall Curtis Erwin.

Enduring Oversight Issues

Duplication of Effort

The Intelligence Reform and Terrorism Prevention Act of 2004 tasks the DNI with ensuring the elimination of waste and unnecessary duplication within the intelligence community. Some observers believe the DNI has focused more on other statutory requirements—specifically its mandate to facilitate information sharing—while neglecting this responsibility to eliminate waste, resulting in the proliferation of intelligence organizations, particularly in the areas of counterterrorism and analysis, that fulfill many of the same functions.

Redundancy can serve important functions in intelligence. In the more tactical venues like counterterrorism, having multiple foreign and domestic intelligence organizations working to identify and disrupt terror plots ensures due diligence on the large amount of threat reporting flowing into the intelligence community each day. For example, in the wake of the 2009 Christmas day attack, a White House review noted that, "As with intentional analytic redundancy, the counterterrorism community also has multiple and overlapping warning systems to ensure that departments and agencies are kept fully aware of ongoing threat streams."[2] In the area of strategic analysis, redundancy might more effectively check the biases of individual organizations. The DNI commented on this issue in July 2010, noting, "'Competitive analysis' avoids single points of failure and unchallenged analytic judgments. The lack of competing analytic judgments was a criticism by several post-9/11 commissions."[3] Notionally, such competition might have improved the pre-war analysis of Iraq's weapons of mass destruction capacity.

Striking a balance that eliminates unnecessary redundancy while maintaining the competitive environment that has proven effective over the last decade at preventing at least large-scale, 9/11-type attacks will likely be the greatest challenge facing the 113th Congress in the area of intelligence.

[2] White House Review Summery Regarding 12/25/2009 Attempted Terrorist Attack, January 7, 2010.

[3] Questions & Answers on the Intelligence Community Post 9/11, Office of the Director of National Intelligence, July 19, 2010

Information Sharing vs. Information Overload

Investigations of the 9/11 attacks concluded that both technical and policy barriers had limited sharing of information collected by different agencies that, if viewed together, could have provided forewarning into the unfolding plot. This insight led to a series of reforms. The USA Patriot Act eliminated statutory barriers to information sharing, primarily in the domestic intelligence arena, and the Intelligence Reform and Terrorism Prevention Act of 2004 created the broader institutional framework for sharing across the intelligence community. That 2004 act gave the DNI the authority to "ensure maximum availability of and access to intelligence information within the intelligence community."

Intelligence successes and failures in recent years suggest significant improvement has been made in the area of information sharing. A White House review of the 2009 Christmas day bombing attempt, for example, found that "Information sharing does not appear to have contributed to this intelligence failure," and that information about a pending attack had been shared with those in a position to disrupt the plot.[4] A Senate investigation into the 2012 attack on the diplomatic mission in Benghazi, Libya, similarly concluded that intelligence was effectively shared between the Department of State and other intelligence agencies prior to the incident. John Brennan, in a prehearing question for his confirmation hearing as CIA Director, stated his view that sharing between the intelligence community, DOD, and other intelligence and law enforcement partners was at an all-time high.[5]

While the intelligence community is not entirely without its legacy "stovepipes,"[6] the challenge more than a decade after 9/11 is largely one of information overload, not information sharing. Analysts now face the task of connecting disparate, minute data points buried within large volumes of intelligence traffic shared between different intelligence agencies. According to a DNI statement from July 2010, "Terabytes of foreign intelligence information come in each day, vastly exceeding the entire text holdings of the Library of Congress, which is estimated at 10 terabytes." In the additional views section of the Senate report on the Christmas day bombing attempt, Senators Saxby Chambliss and Richard Burr noted that analysts who could have connected the dots prior to the incident struggled to search the large volume of terrorism-related intelligence available to them.[7] The same problem was identified at the FBI in the aftermath of the 2009 Foot Hood shooting.[8]

While not a new problem for the intelligence community, the challenge of "separating the wheat from the chaff" may have been exacerbated over the last decade by a number of factors, including the fusion of domestic and foreign intelligence and the use of new information technologies that generate large amounts of data accessible to the federal government. Congress may wish to revisit

[4] White House Review Summery Regarding 12/25/2009 Attempted Terrorist Attack, January 7, 2010.

[5] Senate Select Committee on Intelligence, Additional Prehearing Questions for. Mr. John O. Brennan upon his nominiation to be the Director of the Central Intelligence Agency.

[6] See for example, the Webster Commission and Senate Homeland Security and Government Affairs Committee reports on the 2009 Fort Hood shooting.

[7] "Unclassified Executive Summary of teh Committee Report on the Attempted Terrorist Attack on Northwest Airlines Flight 253," Senate Select Committee on Intelligence, May 18, 2010.

[8] FINAL REPORT of the WILLIAM H. WEBSTER COMMISSION on The Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009

the technical and institutional changes implemented by the intelligence community since this problem came into focus in 2009.[9]

Counterterrorism and Intelligence Support to Military Forces

In 1997, the House Intelligence Committee noted that "intelligence is now incorporated into the very fiber of tactical military operational activities, whether forces are being utilized to conduct humanitarian missions or are engaged in full-scale combat." The Persian Gulf War demonstrated the importance of intelligence from both tactical and national systems, including satellites that had been previously directed almost entirely at Soviet facilities. There were, nonetheless, numerous technical difficulties, especially in transmitting data in usable formats and in a timely manner. Many of these issues have since been addressed with congressional support and in Operation Iraqi Freedom intelligence was an integral part of the operational campaign and remained so in both Iraq and Afghanistan.

A classified report prepared by the President's Intelligence Advisory Board (PIAB) in 2012 allegedly found that, after a decade of counterterrorism and intelligence support to the wars in Iraq and Afghanistan, the CIA specifically and the intelligence community more generally has now become too focused on tactical operation and military.[10] Some observers believe the community has neglected its traditional functions of gathering and analyzing intelligence on more strategic topics. Members expressed similar concerns during recent confirmation hearings for CIA Director Brennan, who signaled his intent to examine allocation of mission within the CIA.[11]

The DNI is responsible for establishing intelligence community priorities and has a staff dedicated to ensuring collection and analytic resources are properly allocated to meet those priorities. In light of these mechanisms, the findings of the PIAB might be overstated. Some argue that an alleged focus on counterterrorism and operational support may reflect public perception of intelligence community activity rather than an actual allocation of intelligence resources.[12]

Collection Capabilities

Intelligence agencies collect vast quantities of information on a daily, even an hourly, basis. The ability to locate fixed installations and moving targets has become an integral component of U.S. military capabilities. On almost any subject, the intelligence community can provide a wealth of knowledge within short time frames. Inevitably, there are "mysteries" that remain unknowable—the effects of unforeseeable developments and the intentions of foreign leaders. The emergence of the international terrorist threat has posed major challenges to intelligence agencies largely

[9] For example, the National Counterterrorism Center established "pursuit teams"—groups of analyst who are not responsible for producing finished intelligence for policymakers and whose responsibility is it follow-up terrorism leads.

[10] Greg Miller, "Secret Report Raises Alarms on Intelligence Blind Spots bcause of AQ focus," *The Washington Post*, March 20, 2013

[11] Senate Select Intelligence Committee, Confirmation Hearing on the Nomination of John O. Brennan to be CIA Director, February 7, 2013

[12] Paul Pillar, "Intelligence and Public Perceptions of It," *The National Interest*, March 27, 2013, available at http://nationalinterest.org/blog/paul-pillar/intelligence-public-perceptions-it-8283

designed to gather information about nation states and their armed forces. Sophisticated terrorist groups in some cases relay information only via agents in order to avoid having their communications intercepted. Human collection has been widely perceived as inadequate, especially in regard to terrorism; the Intelligence Reform Act stated the sense of Congress that, while human intelligence (humint) officers have performed admirably and honorably, there must be an increased emphasis on and greater resources applied to enhancing the depth and breadth of human intelligence capabilities. In October 2005 the National Clandestine Service was established at CIA to manage humint operations by CIA and coordinate humint efforts by other intelligence agencies.

There are also congressional concerns regarding major technical systems—especially reconnaissance satellites. These programs have substantial budgetary implications. Whereas the intelligence community was a major technological innovator during the Cold War, today both intelligence agencies and their potential targets make extensive use of commercial technologies, including sophisticated encryption systems. Consensus has yet to be reached on acquisition programs for a new generation of satellites.

Analytical Quality

The ultimate goal of intelligence is to provide accurate analysis in a timely manner. Analysis is not, however, an exact science and there have been, and undoubtedly will continue to be, failures by analysts to prepare accurate and timely assessments and estimates. The performance of the intelligence community's analytical offices during the past decade is a matter of debate; some argue that overall the quality of analysis has been high while others point to the failure to provide advance warning of the 9/11 attacks and a flawed estimate of Iraqi weapons of mass destruction as reflecting systemic problems. Congressional intelligence committees have for some time noted weaknesses in analysis, a lack of language skills, and a predominant focus on current intelligence at the expense of strategic analysis.

Analytical shortcomings are not readily addressed by legislation, but Congress has increased funding for analytical offices since 9/11 and the Intelligence Reform Act of 2004 contains a number of provisions designed to improve analysis—an institutionalized mechanism for alternate or "red team" analyses to be undertaken (§1017), the designation of an individual or entity to ensure that intelligence products are timely, objective, and independent of political considerations (§1019), and the designation of an official in the office of the DNI to whom analysts can turn for counsel, arbitration on "real or perceived problems of analytical tradecraft or politicization, biased reporting, or lack of objectivity" (§1020).

These efforts, however, are affected by the long lead times needed to prepare and train analysts, especially in such fields as counterterrorism and counterproliferation. Initiatives undertaken after the passage of the 2004 act should now have produced a mature cadre of analysts. At the same time, sensitivity to intelligence tradecraft and to the pitfalls of groupthink may have dulled in the years since the intelligence failure associated with Iraq's WMD program. The quality of intelligence community analysis may be tested by emerging national security challenges, such as those associated with Iran's nuclear program.

Issues in the 113th Congress

In addition to government-wide budgetary issues that have the potential for significant effects on intelligence activities, observers expect that oversight of the implementation of the Intelligence Reform Act will continue to be a concern for the 113th Congress. Congress continues to monitor the evolving relationship between the DNI and the CIA Director. The role and effectiveness of new or reformed post-9/11 intelligence elements—for example, the FBI, DHS Intelligence & Analysis, and the Under Secretary of Defense for Intelligence—will likely continue to be areas of congressional interest. Future satellite procurement programs likely continue to be an important issue given the multi-billion dollar costs involved, though many of the details remain classified.

Unauthorized disclosures of classified information will likely continue to be a concern, despite recent executive branch efforts to address this problem. The committee comments in S.Rept. 112-192 state their "grave concern" with "both the quantity and substance" of the disclosures, influencing the introduction of new provisions to prevent and detect future unauthorized disclosures. While no one agency or branch of government was believed to be more responsible than others, the committee called upon the executive branch to be vigilant and aggressively investigate and prosecute those found to be responsible.

The CIA's role in targeted killings may come under closer scrutiny, as the Administration and Members seek to balance a desire for increased transparency and accountability with the need to safeguard what many argue is an effective tool against al-Qaeda.

Benghazi

The attack in Benghazi on September 11, 2012, that claimed the lives of four Americans, including U.S. Ambassador to Libya John C. Stevens, raised a number of intelligence issues. As it pertained to Administration and intelligence community actions after the attack, public debate focused on two related but separate questions regarding whether the incident was a terrorist attack and whether there was a protest prior to the incident. The second question is more directly related to the analytic judgments of the intelligence community. According to public accounts provided by the news media, the intelligence community assessed incorrectly on September 12 that a protest had occurred. The community changed its assessment, based on new information, around September 20.[13] The DNI more than a week later publically acknowledged this change, stating, "As we learned more about the attack, we revised our initial assessment to reflect new information indicating that it was a deliberate and organized terrorist attack carried out by extremists."[14]

Defenders of the IC performance point out that analysts are often called on soon after an incident such as the one that occurred in Benghazi to make difficult judgments based on incomplete information. Those judgments can and should change as information becomes available that provides a more complete picture.[15] This is the nature of intelligence work. They also argue that

[13] Adam Entous and Siobhan Gorman, "Intelligence Stressed Libya Protest Scenario," *The Wall Street Journal*, October 22, 2012.

[14] Statement by the Director of Public Affairs for ODNI, Shawn Turner, on the intelligence related to the terrorist attack on the U.S. Consulate in Benghazi, Libya, September 28, 2012.

[15] See for example Aki Pertiz, "How Critics of Obama's Libya Response Profoundly Misunderstand Intelligence," *The* (continued...)

the possible presence of a protest in Benghazi was just one of many challenging questions presented to analysts about the responsibility and implications of the attack.

As noted above, the performance of the intelligence community's analytical offices came into focus after the failure to provide advance warning of the 9/11 attacks and a flawed estimate of Iraqi weapons of mass destruction. Assessments of Benghazi offer an oversight opportunity for Congress to determine to what extent the intelligence community has improved its analytic tradecraft. Congressional oversight thus far has focused primarily on the Department of State's actions prior to the attack and on the Administration's public statements.

Britt Snider, in his book about intelligence oversight, argues that looking behind intelligence analysis has historically proven difficult for the intelligence committees. He notes, however, that "This is not to say the select committees cannot do independent evaluations of intelligence analysis or do them well. The HPSCI's 1979 report on the fall of the Shah in Iran and the SSCI's 2004 evaluation of the prewar assessments on Iraq are cases in point."[16] With respect to Benghazi, oversight questions that could be addressed include: Was the initial judgment that a protest had occurred valid given the information that was available as of September 12? Why was information about a protest considered credible at the time? Based on new information, should analysts have corrected their assessment earlier than September 20? Did analysts display "anchoring bias"—the tendency to give greater weight to early information and assessments?

Intelligence Agencies and Drone Warfare

U.S. counterterrorism efforts in Iraq, Afghanistan, Pakistan, and in other areas have been heavily dependent upon the use of unmanned aerial vehicles (UAVs) or unmanned aerial systems (UAS), referred to as "drones" in the media, for intelligence collection, often in real time. They provide important substitutes for, or supplements to, other intelligence platforms such as satellites and manned aircraft. In addition, some UAVs have been modified to launch weapons at designated targets. Operated remotely from ground stations in the region or even from the United States, armed UAVs can avoid the need to introduce U.S. personnel into direct combat, a significant advantage. Their use can also avoid the diplomatic complications of a ground-based U.S. military presence. UAVs are operated both by the military services and intelligence agencies depending on a number of operational and statutory considerations. Use by the military forces would be undertaken consistent with Title 10 authorities. 50 U.S.C. 413b provides statutory authorities for the DNI to undertake covert actions at presidential direction.

Many have expressed concern about reports of expanded use of UAVs in targeted attacks. Some observers suggest that some individuals may not be legitimate targets as envisioned by the 2001 Authorization for the Use of Force (P.L. 107-40), or believe that targeted attacks in countries where the United States is not otherwise engaged in armed conflict might violate international law. Since the September 2011 targeted killing of Anwar al-Awlaki, an American who fled to Yemen and became a senior leader within al-Qaeda in the Arabian Peninsula, many have questioned the legal basis of such a strike against a U.S. citizen. Still others question the

(...continued)

Atlantic, October 2, 2012.

[16] Britt Snyder, The Agency and the Hill: The CIA's Relationhip with Congress, 1946 – 2004, The Center for the Study of Intelligence, p. 221

effectiveness of the program over the long term and warn that drone attacks inside foreign countries such as Pakistan will encourage opposition to overall U.S. policy goals by engendering negative perceptions that ultimately bolster al-Qaeda's ranks. Former DNI Blair has stated: "in Pakistan, news media accounts of heavy civilian casualties are widely believed. Our reliance on high-tech strikes that pose no risk to our soldiers is bitterly resented in a country that cannot duplicate such feats of warfare without cost to its own troops." Congress is expected to maintain close oversight of the use of UAVs in the counterterrorism effort.

Role of the FBI

In the wake of the September 2001 attacks, the FBI was strongly criticized for failing to focus on the terrorist threat, for failing to collect and strategically analyze intelligence, and for failing to share intelligence with other intelligence agencies (as well as among various FBI components). Subsequently, FBI Director Robert S. Mueller III introduced a number of reforms to create a better and more professional intelligence effort in an agency that has always emphasized law enforcement. Congress has expressed concern about the overall effectiveness of these reforms and with the FBI's widely criticized information technology acquisition efforts.[17] These issues came into focus after the November 2009 Fort Hood shooting that claimed the lives of 13 Department of Defense employees. It was determined that the FBI had information about the shooter prior to the attack that it did not fully disseminate to DOD or the other members of the intelligence community. A Senate investigation into the shooting found that "the Fort Hood attack is an indicator that the current status of the FBI's transformation to become intelligence-driven is incomplete and that the FBI faces internal challenges - which may include cultural barriers - that can frustrate the on-going institutional reforms."[18]

Role of the DHS Office of Intelligence and Analysis

The Homeland Security Act of 2002 established within the Department of Homeland Security a Directorate for Information Analysis and Infrastructure Protection with the responsiblity to, among other things, "identify and assess the nature and scope of terrorist threats to the homeland" and "detect and identify threats of terrorism against the United States." The Directorate has since been broken into two components, with intelligence collection and analysis functions falling to the Office of Intelligence and Analysis (I&A). In addition, the Bush Administration announced the establishment of the Terrorist Threat Integration Center (TTIC) in January 2003 under the DCI. In accordance with Executive Order 13354 of August 27, 2004, and the Intelligence Reform Act, TTIC was transferred to the National Counterterrorism Center (NCTC), which constitutes the focal point for assessing information on potential terrorist threats from all sources.[19]

Some argue that the missions of these organizations are distinct. NCTC sits at the nexus between for foreign and domestic intelligence agencies, whereas I&A serves more as a liaison between federal, state and local partners and has a mandate beyond counterterrorism. Nonetheless, in light

[17] For further information, see CRS Report R41780, *The Federal Bureau of Investigation and Terrorism Investigations*, by Jerome P. Bjelopera.

[18] "A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack," The Senate Homeland Security and Government Affairs Committee, February 2011.

[19] See CRS Report R41022, *The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns*, by Richard A. Best Jr.

of the establishment of NCTC and the FBI's efforts to become an intelligence driven organization, Members have sometimes questioned the role and mission of DHS I&A.[20]

The Role of the Under Secretary of Defense for Intelligence

The position of Under Secretary of Defense for Intelligence (USD(I)) was established by the Defense Authorization Act for FY2003 (P.L. 107-314, §901). The statute and DOD directives give the incumbent significant authorities for the direction and control of intelligence agencies within DOD especially in regard to systems acquisition. There are reports that DOD special forces have also been involved in human intelligence collection efforts that are not effectively coordinated with CIA. Some media commentators have pointed to potential conflicts between the office of the USD(I) and the DNI's office. The first USD(I), Stephen Cambone, resigned at the end of 2006; his successor was retired Air Force Lieutenant General James Clapper, who previously served as director of both NGA and DIA and who became DNI in August 2010. Michael Vickers, who had previously served in the CIA, was nominated to serve as USD(I) in January 2011 and was confirmed by the Senate on March 17. In May 2007 the USD(I) was also designated Director of Defense Intelligence and also serves on the DNI's executive committee.

The USD(I) has considerable intelligence budgetary and hiring authority that sometimes rivals or exceeds that of the DNI. Some observers argue that the current working relationship between the DNI and the USD(I) is as much a result of personal relationships and temperament as it is a reflection of sound institutional arrangements between the two positions. Thus, the mission and responsibilities of the USD(I), and the institutional and statutory relationship with the DNI, may be areas of continued congressional interest.

Paramilitary Operations and Defense Humint

Some observers have expressed concern that expanded efforts by DOD intelligence personnel to collect humint overseas and undertake "preparation of the battlefield" operations may interfere with ongoing efforts of CIA humint collectors. Intelligence officials have maintained in congressional testimony that there is no unnecessary duplication of effort and that careful coordination is undertaken during the planning and implementing of such operations. The determination to ensure that such coordination is effective was further reflected in the designation of the DCIA as head of the National Clandestine Service. Members have also questioned the adequacy of DOD's administration of its intelligence personnel, citing cover problems, unproductive deployment locations, and "non-existent" career management.[21]

DOD in April 2012 announced the creation of a new Defense Clandestine Service intended to shift the defense intelligence activities away from tactical support and to focus more on humint operations against national-level priorities. A month later, the Senate Armed Services Committee, in its version of the National Defense Authorization Act of 2013, moved to constrain the growth of DOD's human intelligence personnel. The final bill froze funding for civilian personnel conducting defense human intelligence at the amount necessary to support the number of such

[20] See for example House Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment hearing on "Homeland Security Department Intelligence Efforts", May 12, 2010

[21] S.Rept. 112-173

personnel as of April 20, 2012.[22] The Senate report language accompanying its version of the bill stated:

> The committee notes that President Bush authorized 50 percent growth in the CIA's case officer workforce, which followed significant growth under President Clinton. Since 9/11, DOD's case officer ranks have grown substantially as well. The committee is concerned that, despite this expansion and the winding down of two overseas conflicts that required large HUMINT resources, DOD believes that its needs are not being met.[23]

Congressional Notification Procedures

The intelligence investigations of the 1970s led to eventual enactment of statutory provisions requiring that Congress be informed of covert actions as well as current and anticipated intelligence activities other than covert actions. These provisions require the Administration to keep the two intelligence committees "fully and currently informed" of intelligence activities and significant anticipated intelligence activities. Covert actions must be approved by the President and Congress must be notified, but special provisions were subsequently established to permit in extraordinary circumstances limiting notification of covert actions to the chairmen and ranking minority Members of the intelligence committees, the Speaker of the House and the House minority leader, and the majority and minority leaders of the Senate, the so-called "Gang of Eight." Whether Gang of Eight or even more limited notification can be used for intelligence activities other than covert actions has become a source of controversy in recent years with some Members arguing that the statutes require that all committee members be notified at least in the case of intelligence activities that are not covert actions. The House Intelligence Committee included a provision (§321) in its FY2010 intelligence authorization bill (H.R. 2701) that would remove the Gang of Eight provisions and require that all committee Members be briefed on all intelligence activities, including covert actions, unless the committee itself decided to limit notification. The Administration, in its Statement of Administration Policy issued July 8, 2009, stated firm opposition to Section 321, arguing that it "runs afoul of tradition by restricting an important established means by which the President protects the most sensitive intelligence activities."[24] The Senate version of the FY2010 intelligence authorization bill, which ultimately became P.L. 111-259, addresses notification both of covert actions and intelligence activities generally; it requires that, if the Administration does not provide information to all Members of the two committees, it will be required to notify the committees of the reasons for withholding information and a description of the "main features" of the activity that can be made available to all committee members.

Members have continued to express frustration with the extent to which they are consulted or notified about intelligence activity, most recently during the Senate confirmation of John Brennan as CIA Director. That confirmation was held up while Members demanded to see Department of Justice Office of Legal Counsel opinions about the Administration's targeted killing program. Although such opinions are not governed by congressional notification procedures, some

[22] P.L. 112-81

[23] S.Rept. 112-173

[24] CRS Report R40691, *Sensitive Covert Action Notifications: Oversight Options for Congress*. See also CRS Report R40698, *"Gang of Four" Congressional Intelligence Notifications*.

Members suggested that the initial refusal to share those opinions was indicative of distrust between the intelligence community and its oversight bodies.[25]

Information Security and Unauthorized Disclosures

Unauthorized disclosures of classified information, whether from a media source, government agency or employee, or anonymously, have received significant attention over the past year. The Senate Intelligence Authorization legislation, which passed the House in December and was signed by the President in January 2013, focused on tighter restrictions to prevent disclosures and define consequences. The anti-leak proposals limit interaction between the media and cleared personnel, require the intelligence community to develop an insider threat program, and allow the government to withhold the pension of those who illegally disclose classified data. The bill also revises the definition of "intelligence agency" to include all elements of the intelligence community.[26] Most of the provisions pertaining to unauthorized disclosure of classified information were dropped from the final bill.

The White House in December 2012 released its *National Strategy for Information Sharing and Safeguarding*, which called for structural and policy reforms to address unauthorized disclosures of classified information.[27] The DNI in June 2012 also announced new measures to combat those disclosures.[28] It remains to be seen whether these actions will be effective or whether stronger action will be needed.

Government Accountability Office and the Intelligence Community

The Government Accountability Office (GAO), a legislative branch agency, has statutory authorities to audit and investigate the receipt, disbursement, and application of public funds with a broad right of access to agency records and information. There are, however, specific exceptions that cover many intelligence activities by the CIA and other intelligence agencies. Although oversight of intelligence efforts is undertaken by the two congressional intelligence committees, some Members believe that the GAO should also have a role in intelligence efforts.[29] In recent years, intelligence authorization bills have included provisions expanding GAO's responsibilities in regard to intelligence agencies; both the Bush and Obama Administrations have resisted these proposals. Provisions for an expanded GAO role were included in both the Senate

[25] See for example comments from Senator Rockefeller during the Senate Select Committee on Intelligence hearing on "Security Threats to the United States," March 12, 2013.

[26] U.S. Congress, 112th Congress, 2nd session, Senate, Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2013*, S.Rept. 112-192, July 30, 2012, p. 13, Section 606, refers to Section 3(4) of the National Security Act.

[27] NATIONAL STRATEGY FOR INFORMATION SHARING AND SAFEGUARDING, December 2012.

[28] Director Clapper Announces Steps to Deter and Detect Unauthorized Disclosures, June 25, 2012

[29] See CRS Report RL32525, *Congressional Oversight of Intelligence: Current Structure and Alternatives*, by L. Elaine Halchin and Frederick M. Kaiser, and "GAO Versus the CIA: Uphill Battles Against an Overpowering Force," *International Journal of Intelligence and Counterintelligence*, Fall 2002. Similar proposals have been introduced over a long period, including stand-alone legislation such as S. 385, introduced by Senator Daniel Akaka in the 111th Congress, S. 82, in the 110th congress also introduced by Senator Akaka, and H.R. 978 introduced by Representative Bennie Thompson, and H.R. 3603 in the 100th Congress, introduced by then-Representative Leon Panetta.

and House FY2011 Intelligence Authorization bill (S. 1494, §335; H.R. 2701, §335) despite Administration opposition.[30] On May 27, 2010, an amendment sponsored by Representative Eshoo was added to the FY2011 Defense Authorization bill (H.R. 5136, §923) on a floor vote that would have required the DNI to provide the GAO with all information necessary to conduct an analysis, evaluation, or investigation requested by one of the congressional intelligence committees. In addition, a separate section would have recognized that GAO audits of intelligence agencies could be requested by any congressional committee with appropriate jurisdiction. In such cases, information relating to intelligence sources and methods or covert actions may be redacted and provided only to the congressional intelligence committees. The version of H.R. 2701 that both the Senate and House approved in late September 2010 required that the DNI issue a written directive no later than May 2011 to govern access by GAO for information held by intelligence agencies. On April 29, 2011, the DNI issued Intelligence Community Directive Number 114, *Comptroller General Access to Intelligence Community Information* which contains provisions designed to encourage cooperation between GAO and intelligence agencies. The Directive states, however, that information will not be provided to support a GAO audit or review of core national intelligence capabilities and activities. The Directive went into effect on June 30, 2011.

GAO's response to ICD 114 stated that it was a "good start" to improving access to information in possession of the intelligence community but that some language in the directive, if interpreted broadly by intelligence agencies, "could significantly hinder GAO's ability to conduct related work that we are routinely requested by the Congress to do."[31] Congress may wish to examine how ICD 114 has been interpreted and to what extent it has improved GAO access.

[30] Office of Management and Budget, Statement of Administration Policy, H.R. 2701, Intelligence Authorization Act for Fiscal Year 2010, July 8, 2009.

[31] GAO Comments on Intelligence Community Directive Number 114, United States Government Accountability Office, April 29, 2011.

Appendix A. Additional Background

The "INTs": Intelligence Disciplines

The intelligence community has been built around major agencies responsible for specific intelligence collection systems known as disciplines. Three major intelligence disciplines or "INTs"—signals intelligence (*sigint*), imagery intelligence (*imint*), and human intelligence (*humint*)—provide the most important information for analysts and absorb the bulk of the intelligence budget. Sigint collection is the responsibility of NSA at Fort Meade, MD. Sigint operations are classified, but there is little doubt that the need for intelligence on a growing variety of nations and groups that are increasingly using sophisticated and rapidly changing encryption systems requires a far different sigint effort than the one prevailing during the Cold War. Since the late 1990s a process of change in NSA's culture and methods of operations has been initiated, a change required by the need to target terrorist groups and affected by the proliferation of communications technologies and inexpensive encryption systems. Observers credit the then-Director of NSA, Lieutenant General Michael Hayden, who later became Director of the CIA in May 2006, with launching a long-overdue reorganization of the agency, and adapting it to changed conditions. Part of his initiative has involved early retirements for some NSA personnel and greater reliance on outsourcing many functions previously done by career personnel. Some of the initiatives relating to acquisition did not, however, meet their objectives.

A second major intelligence discipline, imagery or *imint*, is also facing profound changes. Imagery is collected in essentially three ways: by satellites, manned aircraft, and unmanned aerial vehicles (UAVs). The satellite program that covered the Soviet Union and acquired highly accurate intelligence concerning submarines, missiles, bombers, and other military targets is perhaps the greatest achievement of the U.S. intelligence community—it served as a foundation for defense planning and strategic planning that led to the end of the Cold War. In today's environment, there is a greater number of collection targets than existed during the Cold War and more satellites are required, especially those that can be maneuvered to collect information about a variety of targets. At the same time, the availability of high-quality commercial satellite imagery and its widespread use by federal agencies has raised questions about the extent to which coverage from the private sector can meet the requirements of intelligence agencies. High altitude UAVs such as the Global Hawk may also provide surveillance capabilities that overlap those of satellites.

The National Imagery and Mapping Agency (NIMA) was established in 1996 to manage imagery processing and dissemination previously undertaken by a number of separate agencies. NIMA was renamed the National Geospatial-Intelligence Agency (NGA) by the FY2004 Defense Authorization Act (P.L. 108-136). The goal of NGA is, according to the agency, to use imagery and other geospatial information "to describe, assess, and visually depict physical features and geographically referenced activities on the Earth."

Intelligence from human contacts—*humint*—is the oldest intelligence discipline and the one that is most often written about in the media. The CIA is the primary collector of humint, but the Defense Department also has responsibilities filled by defense attachés at embassies around the world and by other agents working on behalf of theater commanders. Many observers have argued that inadequate humint has been a systemic problem and contributed to the inability to gain prior knowledge of the 9/11 plots. In part, these criticisms reflect the changing nature of the international environment. During the Cold War, principal targets of U.S. humint collection were

foreign government officials and military leaders. Intelligence agency officials working under cover as diplomats could approach potential contacts at receptions or in the context of routine embassy business. Today, however, the need is to seek information from clandestine terrorist groups or narcotics traffickers who do not appear at embassy social gatherings. Humint from such sources can be especially important as there may be little evidence of activities or intentions that can be gathered from imagery, and their communications may be carefully limited.

Placing U.S. intelligence officials in foreign countries under "nonofficial cover" (NOC) in businesses or other private capacities is possible, but it presents significant challenges to U.S. agencies. Administrative mechanisms are vastly more complicated than they are for officials formally attached to an embassy; special arrangements have to be made for pay, allowances, retirement, and healthcare. The responsibilities of operatives under nonofficial cover to the parent intelligence agency have to be reconciled with those to private employers, and there is an unavoidable potential for conflicts of interest or even corruption. Any involvement with terrorist groups or smugglers has a potential for major embarrassment to the U.S. government and, of course, physical danger to those immediately involved.

Responding to allegations that CIA agents may have been involved too closely with narcotics smugglers and human rights violators in Central America, the then-Director of Central Intelligence (DCI), John Deutch, established guidelines in 1995 (which remain classified) to govern the recruitment of informants with unsavory backgrounds. Although CIA officials maintain that no proposal for contacts with persons having potentially valuable information was disapproved, there was a widespread belief that the guidelines served to encourage a "risk averse" atmosphere at a time when information on terrorist plans, from whatever source, was urgently sought. The FY2002 Intelligence Authorization Act (P.L. 107-108) directed the DCI to rescind and replace the guidelines, and July 2002 press reports indicated that they had been replaced.

A major constraint on humint collection is the availability of personnel trained in appropriate languages. Cold War efforts required a supply of linguists in a relatively finite set of foreign languages, but the intelligence community now needs experts in a wider range of more obscure languages and dialects. Various approaches have been considered: use of civilian contract personnel, military reservists with language qualifications, and substantial bonuses for agency personnel who maintain their proficiency. The National Security Education Program, established in 1991, provides scholarships and career training for individuals in or planning to enter careers in agencies dealing with national security issues.

Other "INTs"

A fourth INT, measurement and signatures analysis—*masint*—has received greater emphasis in recent years. A highly technical discipline, masint involves the application of complicated analytical refinements to information collected by sigint and imint sensors. It also includes spectral imaging by which the identities and characteristics of objects can be identified on the basis of their reflection and absorption of light. Masint is undertaken by DIA and other DOD agencies. A key problem has been retaining personnel with expertise in masint systems who are offered more remunerative positions in private industry.

Another category of information, open source information—*osint* (newspapers, periodicals, pamphlets, books, radio, television, and Internet websites)—is increasingly important given requirements for information about many regions and topics (instead of the former concentration on political and military issues affecting a few countries). At the same time, requirements for

translation, dissemination, and systematic analysis have increased, given the multitude of different areas and the volume of materials. Many observers believe that intelligence agencies should be more aggressive in using osint; some believe that the availability of osint may even reduce the need for certain collection efforts. The availability of osint also raises questions regarding the need for intelligence agencies to undertake collection, analysis, and dissemination of information that could be directly obtained by user agencies. Section 1052 of the Intelligence Reform Act expressed the sense of Congress that there should be an open source intelligence center to coordinate the collection, analysis, production, and dissemination of open source intelligence to other intelligence agencies. An Open Source Center was subsequently established, although it has been managed by CIA personnel.

Integrating the "INTs"

The "INTs" have been the pillars of the intelligence community's organizational structure, but analysis of threats requires that data from all the INTs be brought together and that analysts have ready access to all sources of data on a timely basis. This has proved in the past to be a substantial challenge because of technical problems associated with transmitting data and the need to maintain the security of information acquired from highly sensitive sources. Some argue that intelligence officials have tended to err on the side of maintaining the security of information even at the cost of not sharing essential data with those having a need to know. Section 1015 of the Intelligence Reform Act mandated the establishment of an Intelligence Sharing Environment (ISE) to facilitate the sharing of terrorism-related information.

A related problem has been barriers between foreign intelligence and law enforcement information. These barriers derived from the different uses of information collected by the two sets of agencies—foreign intelligence used for policymaking and military operations and law enforcement information to be used in judicial proceedings in the United States. A large part of the statutory basis for the "wall" between law enforcement and intelligence information was removed with passage of the USA PATRIOT Act of 2001 (P.L. 107-56), which made it possible to share law enforcement information with analysts in intelligence agencies, but long-established practices have not been completely overcome. The Homeland Security Act (P.L. 107-296) and the subsequent creation of the Terrorist Threat Integration Center (TTIC) established offices charged with combining information from both types of sources. Section 1021 of the Intelligence Reform Act made the new National Counterterrorism Center (NCTC), TTIC's successor, operating under the DNI specifically responsible for "analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism [except purely domestic terrorism]."[32]

Intelligence Budget Process

For budgetary purposes, intelligence spending is divided between the National Intelligence Program (NIP; formerly the National Foreign Intelligence Program or NFIP) and the Military Intelligence Program (MIP). The MIP was established in September 2005 and includes all programs from the former Joint Military Intelligence Program, which encompassed DOD-wide intelligence programs and most programs from the former Tactical Intelligence and Related

[32] See CRS Report R41022, *The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns*, by Richard A. Best Jr.

Activities (TIARA) category, which encompassed intelligence programs supporting the operating units of the armed services. The Program Executive for the MIP is the Under Secretary of Defense for Intelligence. The bulk of the $50+ billion in national intelligence spending has been "hidden" within the DOD budget. Spending for most intelligence programs is described in classified annexes to intelligence and national defense authorization and appropriations legislation. (Members of Congress have access to these annexes, but must make special arrangements to read them.)

Intelligence spending is authorized in intelligence authorization acts. When intelligence authorization legislation is not enacted (as was the case between FY2006 and FY2010), most intelligence spending is authorized by a "catch-all" provision in defense appropriations acts.[33]

For a number of years some Members sought to make public total amounts of intelligence and intelligence-related spending; floor amendments for that purpose were defeated in both chambers during the 105th Congress. In response, however, to a lawsuit filed under the Freedom of Information Act, DCI George Tenet stated on October 15, 1997, that the aggregate amount appropriated for intelligence and intelligence-related activities for FY1997 was $26.6 billion. He added that the Administration would continue "to protect from disclosure any and all subsidiary information concerning the intelligence budget." In March 1998, DCI Tenet announced that the FY1998 figure was $26.7 billion. Figures for FY1999 and subsequent years were not released. During consideration of intelligence reform legislation in 2004, the Senate at one point approved a version of a bill which would have required publication of the amount of the NIP; the House version did not include a similar provision and, with the Senate deferring to the House, the Intelligence Reform Act did not require making intelligence spending amounts public. Section 601 of P.L. 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007, requires, however, that the DNI publicly disclose the aggregate amount of funds appropriated for the NIP although after FY2008 the President could waive or postpone the disclosure upon sending a explanation to congressional oversight committees. Consistent with that act, the DNI announced in October 2008 that the aggregate amount appropriated to the National Intelligence Program for FY2008 was $47.5 billion. A year later the NIP for FY2009 was announced as $49.8 billion. In September 2009, DNI Blair stated publicly that total annual intelligence spending is $75 billion, a figure that includes not only the NIP but also military intelligence activities. In October 2010, the DNI announced that the amount appropriated to the NIP for FY2010 was $53.1 billion. Subsequently, DOD announced that the MIP appropriations for FY2010 was $27 billion, including both the base budget and supplemental appropriations. The amount appropriated for MIP in FY2011 was $24 billion, a $3 billion reduction from the year earlier. The amount appropriated for the NIP in FY2011 was $54.6 billion according to an October 2011 announcement. The amount appropriated to the NIP for FY2012 was $53.9 billion, according to an October 2012 announcement from the DNI. The amount requested for the NIP for FY2013 was $52.6 billion. According to a December 2012 statement from the leaders of the congressional intelligence committees, the FY2013 intelligence authorization bill is below 2012's enacted budget but slightly above the President's 2013 request.

Jurisdiction over intelligence programs is somewhat different in the House and the Senate. The Senate Intelligence Committee has jurisdiction only over the NIP but not the MIP, whereas the

[33] See CRS Report R40240, *Intelligence Authorization Legislation: Status and Challenges*, by Marshall Curtis Erwin. The FY2010 Intelligence Authorization Act (P.L. 111-259) was not enacted prior to the end of FY2010 and did not authorize FY2010 intelligence programs although it had significant legislative provisions.

House Intelligence Committee has jurisdiction over both sets of programs. The preponderance of intelligence spending is accomplished by intelligence agencies within DOD and thus in both chambers the armed services committees are involved in the oversight process. Other oversight committees are responsible for intelligence agencies that are part of departments over which they have jurisdiction.

Most appropriations for intelligence activities are included in national defense appropriations acts, including funds for the CIA, DIA, NSA, the NRO, and NGA. Other appropriations measures include funds for the intelligence offices of the State Department, the FBI, and DHS and other intelligence agencies. Although funds for CIA have been included in defense appropriations acts, these monies are transferred directly to the CIA Director. The Senate voted in October 2004 to establish an Appropriations Subcommittee on Intelligence, but this has not occurred nor did the House take similar action. On January 9, 2007, however, the House approved H.Res. 35, which established a select panel within the appropriations committee that includes three members of the intelligence committee to oversee appropriations for intelligence program. The select panel was not continued in the 112th Congress.

Intelligence budgeting issues were at the center of the debate on intelligence reform legislation in 2004. On one hand, there was determination to make the new DNI responsible for developing and determining the annual National Intelligence Program budget (which is separate from the MIP budgets that are prepared by the Office of the Secretary of Defense). The goal was to ensure a unity of effort that arguably has not previously existed and that may have complicated efforts to monitor terrorist activities. On the other hand, the intelligence efforts within the National Intelligence Program include those of major components of the Defense Department, including NSA, the NRO, and NGA, that are closely related to other military activities. Some Members thus argued that even the National Intelligence Program should not be considered apart from the Defense budget. After considerable debate, the final version of P.L. 108-458 provides broad budgetary authorities to the DNI, but in Section 1018 requires the President to issue guidelines to ensure that the DNI exercises the authorities provided by the statute "in a manner that respects and does not abrogate the statutory responsibilities of the heads of" the Office of Management and Budget and Cabinet departments. Observers expect that implementing the complex and seemingly overlapping budgetary provisions of the Intelligence Reform Act will continue to depend on effective working relationships among the Office of the DNI, DOD, and the White House staff. In late 2011 Congress passed the FY2012 Intelligence Authorization bill (H.R. 1892) and the Consolidated Appropriations Act, 2012 (P.L. 112-74). The two acts contained provisions affecting intelligence budgeting. Section 433 of the former authorizes the establishment of Treasury Department accounts to receive funds from defense intelligence elements, the ODNI, and other agencies for authorized programs. The latter contains several provisions (especially Sections 8090, 8092, and 8094) that would bring intelligence budget submissions into alignment with formats established for the Defense Department. Taken together, the provisions may facilitate the DNI's management of intelligence accounts and strengthen congressional oversight even though an earlier initiative by DNI Clapper for the submission of a NIP budget request separate from the DOD budget is precluded (§8116).

The 9/11 Investigations and the Congressional Response

In the aftermath of September 11, 2001, there was extensive public discussion of whether the attacks on the Pentagon and World Trade Center represented an "intelligence failure." In response, the Senate Select Committee on Intelligence and the House Permanent Select

Committee on Intelligence undertook a joint investigation of the September 11 attacks. Public hearings by the resulting "Joint Inquiry" were launched on September 18, 2002, beginning with testimony from representatives of families of those who died in the attacks. Former policymakers and senior CIA and FBI officials also testified. Eleanor Hill, the inquiry staff director, summarized the inquiry's findings:

> the Intelligence Community did have general indications of a possible terrorist attack against the United States or U.S. interests overseas in the spring and summer of 2001 and promulgated strategic warnings. However, it does not appear that the Intelligence Community had information prior to September 11 that identified precisely where, when and how the attacks were to be carried out.

The two intelligence committees published the findings and conclusions of the Joint Inquiry on December 11, 2002.[34] The committees found that the intelligence community had received, beginning in 1998 and continuing into the summer of 2001, "a modest, but relatively steady, stream of intelligence reporting that indicated the possibility of terrorist attacks within the United States." Further findings dealt with specific terrorists about whom some information had come to the attention of U.S. officials prior to September 11 and with reports about possible employment of civilian airliners to crash into major buildings. The inquiry also made systemic findings highlighting the intelligence community's lack of preparedness to deal with the challenges of global terrorism, inefficiencies in budgetary planning, the lack of adequate numbers of linguists, a lack of human sources, and an unwillingness to share information among agencies.

Separately, the two intelligence committees submitted recommendations for strengthening intelligence capabilities. They urged the creation of a Cabinet-level position of Director of National Intelligence (DNI) separate from the position of director of the CIA. The DNI would have greater budgetary and managerial authority over intelligence agencies in the Defense Department than possessed by the DCI. The committees also expressed great concern with the reorientation of the FBI to counterterrorism and suggested consideration of the creation of a new domestic surveillance agency similar to Britain's MI5.

The Joint Inquiry was focused directly on the performance of intelligence agencies, but there was widespread support among Members for a more extensive review of the roles of other government agencies. Provisions for establishing an independent commission on the 2001 terrorist attacks were included in the FY2003 Intelligence Authorization Act (P.L. 107-306). Former New Jersey Governor Thomas H. Kean was named to serve as chairman, with former Representative Lee H. Hamilton serving as vice chairman. Widely publicized hearings were held in spring 2004 with Administration and outside witnesses providing different perspectives on the role of intelligence agencies prior to the September 11, 2001, attacks. The commission's report was published in July 2004.

Although the 9/11 Commission surveyed the roles of a number of federal and local agencies, many of its principal recommendations concerned the perceived lack of authorities of the DCI. The commission recommended establishing a National Intelligence Director (NID) to manage the National Intelligence Program and oversee the agencies that contribute to it. The NID would annually submit a national intelligence program budget and, when necessary, forward the names of nominees to be heads of major intelligence agencies to the President. Lead responsibility for

[34] The full report was released some months later as H.Rept. 107-792/S.Rept. 107-351.

conducting and executing paramilitary operations would be assigned to DOD and not CIA. The commission also recommended that Congress pass a separate annual appropriations act for intelligence that would be made public. The NID would execute the expenditure of appropriated funds and make transfers of funds or personnel as appropriate. Proposing a significant change in congressional practice, the commission recommended a single intelligence committee in each house of Congress, combining authorizing and appropriating authorities.

On August 27, 2004, President Bush addressed key recommendations of the 9/11 Commission in signing several executive orders to reform intelligence. In addition to establishing a National Counterterrorism Center, the orders provided new authorities for the DCI until legislation was enacted to create a National Intelligence Director. In addition, several legislative proposals were introduced to establish a National Intelligence Director, separate from a CIA Director. The Senate passed S. 2845 on October 16, 2004; the House had passed H.R. 10 on October 8, 2004. Efforts by the resulting conference committee to reach agreed-upon text focused on the issue of the authorities of the proposed Director of National Intelligence in regard to the budgets and operations of the major intelligence agencies in DOD, especially NSA, NRO, and NGA. Conferees finally reached agreement in early December, and the conference report on S. 2845 (H.Rept. 108-796) was approved by the House on December 7 and by the Senate on December 8. The President signed the legislation on December 17, 2004, and it became P.L. 108-458.

The Intelligence Reform Act is wide-ranging, and its ongoing implementation will continue to receive oversight during the 113th Congress. Some observers have suggested that modifications to the legislation may be needed; others recommend that any difficulties be addressed by executive orders or memoranda of understanding.

Terrorist Surveillance Program/NSA Electronic Surveillance/FISA

In December 2005 media accounts of electronic surveillance by NSA authorized outside the parameters of the Foreign Intelligence Surveillance Act (FISA) led to extensive criticism of the Administration. Although the technical details of the effort remain classified, the Bush Administration maintained that communications, which involve a party reasonably considered to be a member of Al Qaeda, or affiliated with Al Qaeda, and one party in the United States, may be monitored on the basis of the President's constitutional authorities and the provisions of the Joint Resolution providing for Authority for the Use of Force (P.L. 107-40) of September 18, 2001. The need for speed and agility required, the Administration further argued, an approach not envisioned by the drafters of FISA. Others countered that FISA should have governed such electronic surveillance. In early March 2006 agreement was reached with the leadership of the two intelligence committees to establish procedures for enhanced legislative oversight of the NSA effort, and legislative initiatives were considered to either modify FISA or establish new statutory authorities for electronic surveillance.

Differing views of Members on the NSA effort were reflected in the House Intelligence Committee's 2006 report on FY2007 intelligence authorization legislation (H.Rept. 109-411). In light of decisions issued by the Foreign Intelligence Surveillance Court (FISC) on January 10, 2007, the Bush Administration advised the chairman and ranking Member of the Senate Judiciary Committee that any electronic surveillance that had previously occurred as part of the Terrorist Surveillance Program (TSP) would thereafter be conducted subject to the approval of the FISC. Further, the Administration indicated that it would not re-authorize the TSP after the expiration of the then-current authorization. On May 1, 2007, the Senate Intelligence Committee held an open hearing on the Administration's proposal to revise FISA to take account of changes in

communications technologies since the 1970s, with Members expressing differing views on the desirability of the legislation.

According to media reports, a judge on the FISC at some point in 2007 ruled that a FISC order was required for surveillance of communications between foreign persons abroad if the communications passed through the United States. On August 2, 2007, the DNI issued a statement on FISA modernization in which he contended that the intelligence community "should not be required to obtain court orders to effectively collect foreign intelligence from foreign targets located overseas." Although details of the effort remain classified, there appears to have been wide agreement among Members that FISA needed to be amended to permit surveillance without a court order of such foreign to foreign communications regardless of whether they were routed through the United States.

The Protect America Act (PAA) (P.L. 110-55), signed on August 5, 2007, after extensive congressional debate, excluded from the definition of "electronic surveillance" under FISA surveillance directed at a person reasonably believed to be located outside the United States. In addition, under certain circumstances, FISA, as amended by this legislation, permitted the DNI and the Attorney General, for periods up to one year, to authorize acquisition of foreign intelligence information "concerning persons reasonably believed to be located outside of the United States," apparently including U.S. persons, and to direct a communications provider, custodian, or other person with access to the communication immediately to provide information, facilities, and assistance to accomplish the acquisition. Those receiving such directives had the right to contest them in court. The DNI and the Attorney General were required to certify, in part, that this acquisition did not constitute electronic surveillance, and the Attorney General was required to submit the procedures by which this determination is made to the FISC for review as to whether the government determination was clearly erroneous. On a semiannual basis, the Attorney General was to report to congressional oversight committees on instances of noncompliance with directives and numbers of certifications and directives issued during the reporting period. P.L. 110-55 expired on February 1, 2008, and efforts to extend it further failed in the House when H.R. 5349 was rejected on February 13. Acquisitions authorized while the PAA was in force may continue until the expiration of the period for which they were authorized.

The Protect America Act was strongly criticized by some Members; on November 15, 2007, H.R. 3773, the RESTORE Act (the Responsible Electronic Surveillance that is Overseen, Reviewed, and Effective Act of 2007) was passed by the House in an attempt to clarify that a court order is not required for the acquisition of the contents of communications between two persons neither of whom is known to be a U.S. person, and both of whom are reasonably believed to be located outside the United States, regardless of whether the communications passed through the United States or if the surveillance device was in the United States. If, in the course of such an acquisition, the communications of a U.S. person were incidentally intercepted, stringent minimization procedures would have applied. Court orders would, however, have been required if the communications of a non-U.S. person reasonably believed to be located outside the United States were targeted where the other parties to the target's communications are unknown and thus might include U.S. persons or persons located physically in the United States. Some Members argued that this provision would unnecessarily tie the hands of intelligence agencies and jeopardize the counterterrorism effort. The RESTORE Act would have also provided for increased judicial oversight and would have required quarterly implementation and compliance audits by the Inspector General of the Justice Department, and added related congressional reporting requirements.

On October 26, 2007, the Senate Intelligence Committee reported its own version of a FISA amendment. The Senate bill (S. 2248), as amended, contained provisions authorizing the Attorney General and the DNI jointly to authorize targeting of persons, other than U.S. persons, reasonably believed to be outside the United States to acquire foreign intelligence information for periods up to one year. Under the Senate bill, FISC approval would have been required for targeting a U.S. person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance under FISA, or the acquisition of stored electronic communications or stored electronic data that requires an order under FISA, and the acquisition is conducted in the United States. The Senate bill would have also provided some retroactive immunity to telecommunications companies from civil suits in federal and states courts related to assistance that they have provided to the government in connection with intelligence activities between September 11, 2001, and January 17, 2007.

A central issue was the role of the judicial branch, and the Foreign Intelligence Surveillance Court (FISC) in particular, in approving and/or overseeing surveillance that does not target but may involve individuals who are U.S. persons. Some argued that only the independent judiciary could ensure that intelligence efforts would not become improperly or illegally directed towards Americans. At the time FISA permitted electronic surveillance to gather foreign intelligence information pursuant to a FISC order of U.S. persons where there was probable cause to believe they were foreign powers or agents of foreign powers if other statutory criteria were met. Some argued, however, that changes in technologies since FISA was enacted in 1978 made case-by-case judicial review of each international communication link that might involve a U.S. person impractical and risky to national security. Details of this issue are complex and, in many cases, classified. The Senate approved S. 2248 on February 12, 2008 (and incorporated it into H.R. 3773).

On March 14, 2008, the House approved an amendment to the version of H.R. 3773 that had been approved by the Senate. The House amendment would have required judicial review by the FISC of procedures for targeting a non-U.S. person located outside of the United States even if the person was not reasonably believed to be communicating with a U.S. person or a person in the United States. The House amendment would have required either a prior FISC order approving the applicable certification, targeting procedures, and minimization procedures or a determination that an emergency situation exists in which case a certification would have to be filed with the FISC within seven days. The Bush Administration argued that this requirement added unprecedented requirements for targeting communications of non-U.S. persons that could result in delaying collection efforts and the loss of some intelligence forever.

If the target of an acquisition were a U.S. person reasonably believed to be outside the United States, then, except in emergencies, the House-passed amendment would have required a FISC order approving an application for an acquisition for a period up to 90 days. The acquisition could have been renewed for additional 90-day periods upon submission of renewal applications. If the Attorney General authorized an emergency acquisition of such a U.S. person's communications, the Attorney General would have had to submit an application for a court order within seven days of that authorization.

The House version of H.R. 3773 would also not have granted retroactive immunity to telecommunications companies but would have allowed them to present evidence in their defense to a court. In addition, the House bill would have established a commission on warrantless electronic surveillance activities conducted between September 11, 2001, and January 17, 2007. The House version of H.R. 3773 did not come to a vote in the Senate and, after considerable

discussions, Representative Reyes introduced a new bill, H.R. 6304, on June 19, 2008, that strengthened the role of the FISC in approving procedures for intelligence surveillance and provided telecommunications companies an opportunity to demonstrate to the courts that they had acted in response to a request for support from the executive branch. H.R. 6304 was passed by the House on June 20, 2008, and by the Senate on July 9, 2008; it was signed by the President on July 10, becoming P.L. 110-261.

At the end of 2009 three FISA provisions, dealing with "Lone Wolf" terrorists, roving wiretaps, and access to business records, were set to expire unless extended. They were extended until February 28, 2010, by a provision of the Defense Appropriations Act for FY2010 (P.L. 111-118) and separate legislation (P.L. 111-141) extended them until February 28, 2011. They were subsequently extended until May 27, 2011, by P.L. 112-3, and until June 1, 2015, by P.L. 112-14.

Appendix B. For Additional Reading

U.S. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, March 31, 2005.

U.S. Congress. Committee of Conference Intelligence Authorization Act for Fiscal Year 2005: Conference Report. December 7, 2004. 108th Congress, 2nd session (H.Rept. 108-798).

——. *Intelligence Reform and Terrorism Prevention Act of 2004*. December 7, 2004. 108th Congress, 2nd session. (H.Rept. 108-796).

U.S. Congress. House of Representatives. Permanent Select Committee on Intelligence. Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence*, Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*. December 2002. 107th Congress, 2nd session (H.Rept. 107-792). [Also, S.Rept. 107-351]

——. *Intelligence Authorization Act for Fiscal Year 2005*. June 21, 2004. 108th Congress, 2nd session (H.Rept. 108-558).

——. *Intelligence Authorization Act for Fiscal Year 2006*. June 2, 2005. 109th Congress, 1st session (H.Rept. 109-101).

——. *Intelligence Authorization Act for Fiscal Year 2007*. April 6, 2006. 109th Congress, 2nd session (H.Rept. 109-411).

——. *Intelligence Authorization Act for Fiscal Year 2008*. May 7, 2007. 110th Congress, 1st session (H.Rept. 110-131).

——. *Intelligence Authorization Act for Fiscal Year 2008*. Conference Report. December 6, 2007. 110th Congress, 1st session (H.Rept. 110-478).

——. *Intelligence Authorization Act for Fiscal Year 2009*. May 21, 2008. 110th Congress, 2nd session (H.Rept. 110-665).

——. *Intelligence Authorization Act for Fiscal Year 2010*. June 26, 2009. 111th Congress, 1st session (H.Rept. 111-186).

——. *Intelligence Authorization Act for Fiscal Year 2011*. May 3, 2011. 112th Congress 1st session (H.Rept. 112-72).

——. *Intelligence Authorization Act for Fiscal Year 2012*. September 2, 2011. 112th Congress 1st session (H.Rept. 112-197). (Text of Managers Amendment printed in *Congressional Record*, December 14, 2011, pp. S8613-8617.)

——. Subcommittee on Terrorism and Homeland Security. *Counterterrorism Intelligence Capabilities and Performance Prior to 9-11*. July 2002.

U.S. Congress. Senate. Select Committee on Intelligence. *Report of the Select Committee on Intelligence on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*. July 9, 2004. 108th Congress, 2nd session (S.Rept. 108-301).

——. *Intelligence Authorization Act for Fiscal Year 2006*. September 29, 2005. 109th Congress, 1st session (S.Rept. 109-142).

——. *To authorize Appropriations for Fiscal Year 2005 for Intelligence and Intelligence-Related Activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System*. May 5, 2004. 108th Congress, 2nd session (S.Rept. 108-258).

——. *Intelligence Authorization Act for Fiscal Year 2007*. January 24, 2007. 110th Congress, 1st session (S.Rept. 110-2).

——. *Intelligence Authorization Act for Fiscal Year 2008*. May 31, 2007. 110th Congress, 1st session (S.Rept. 110-75).

——. *Intelligence Authorization Act for Fiscal Year 2009*. May 8, 2008, 110th Congress, 2nd session (S.Rept. 110-333).

——. *Intelligence Authorization Act for Fiscal Year 2010*. July 22, 2009 [S.1494]. 111th Congress, 1st session (S.Rept. 111-55).

——. *Intelligence Authorization Act for Fiscal Year 2010*. July 19, 2010 [S.3611]. 111th Congress, 2nd session (S.Rept. 111-223).

——. *Intelligence Authorization Act for Fiscal Year 2011*. April 4, 2011 [S.719]. 112th Congress, 1st session (S.Rept. 112-12).

——. *Intelligence Authorization Act for Fiscal Year 2012*. August 1, 2011 [S.1458]. 112th Congress, 1st session (S.Rept. 112-43).

——. *Intelligence Authorization Act for Fiscal Year 2013*. July 30, 2012 [S.3454]. 112th Congress, 2nd session (S.Rept. 112-192).

——. *Report of the Select Committee on Intelligence United States Senate covering the period from January 5, 2011 to January 3, 2013*. March 22, 2013. 1123th Congress, 1st session (S.Rept. 113-7).

——. *Unclassified Executive Summary of the Committee Report on the Attempted Terrorist Attack on Northwest Airlines Flight 253*. May 18, 2010.

U.S. Department of Justice, Commission for Review of FBI Security Programs, *A Review of FBI Security Programs*, March 2002.

U.S. National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*, July 2004.

Author Contact Information

Marshall Curtis Erwin
Analyst in Intelligence and National Security
merwin@crs.loc.gov, 7-7739