



Intelligence Information: Need-to-Know vs. Need-to-Share

Richard A. Best Jr.
Specialist in National Defense

June 6, 2011

Congressional Research Service

7-5700

www.crs.gov

R41848

Summary

Unauthorized disclosures of classified intelligence are seen as doing significant damage to U.S. security. This is the case whether information is disclosed to a foreign government or published on the Internet. On the other hand, if intelligence is not made available to government officials who need it to do their jobs, enormous expenditures on collection, analysis, and dissemination are wasted. These conflicting concerns require careful and difficult balancing.

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 useful insight into the unfolding plot. A consensus emerged that U.S. intelligence agencies should share information more widely in order that analysts could integrate clues acquired by different agencies in order to “connect the dots.”

Major statutory and regulatory changes were made to facilitate information sharing among agencies. An Information Sharing Environment was created within the new Office of the Director of National Intelligence in order to establish policies, procedures, and technologies to link people, systems, and information from government agencies. In law and in Federal regulations a culture of sharing has been established in the Intelligence Community.

Although government officials maintain that policies designed in recent years to increase sharing have helped prevent a number of serious terrorist attacks and contributed significantly to the May 2, 2011 operation against Osama bin Laden, the results have been uneven and, in some cases, unfortunate. Reviews of the Fort Hood shooting in 2009 and the attempted bombing of a commercial airliner the following Christmas revealed that serious obstacles to information sharing had not been completely overcome. At the same time, wide availability of State Department cables provided the opportunity for massive leaks of classified documents (including some intelligence materials) through the WikiLeaks website and cooperating media.

Despite these developments, support for information sharing among intelligence agencies remains strong within both the executive branch and Congress. Intelligence Community representatives have recently described new technologies and procedures to enhance information security including capabilities to determine who has had access to particular reports. Members of Congress included legislative initiatives to accomplish similar goals in FY2011 intelligence authorization legislation (H.R. 754) that has passed both the House and Senate. The challenge remains, how to manage inherent risks to find the “sweet spot” (the term used by Director of National Intelligence James Clapper) between information security and information sharing.

This report focuses on information acquired, analyzed, and disseminated by agencies of the U.S. Intelligence Community, but these concerns also affect classified information outside the Intelligence Community. Efforts to encourage and regulate sharing between Federal agencies and state, local, and tribal agencies are also important and they are directly addressed in CRS Report R40901, *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*, by Mark A. Randol and CRS Report R40602, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*, by Mark A. Randol. Further background can be found in CRS Report RL34177, *A Summary of Fusion Centers: Core Issues and Options for Congress*, by Todd Masse and John Rollins.

Contents

| | |
|--|----|
| Background | 1 |
| Changes Undertaken in Response to 9/11 | 2 |
| The Information Sharing Environment | 6 |
| Limitations and Risks of Information Sharing | 8 |
| Detroit Bomb Attempt..... | 9 |
| Fort Hood Shooting..... | 9 |
| WikiLeaks..... | 10 |
| Conclusion..... | 11 |

Contacts

| | |
|----------------------------------|----|
| Author Contact Information | 13 |
|----------------------------------|----|

Background

At the heart of the intelligence effort lies a paradox. Intelligence is valuable only if it can be shared with consumers who need it, but, to the extent that it is more widely shared, risks of compromise are enhanced. The necessary goal is to find the best balance between adequate sharing and effective information security. The current Director of National Intelligence (DNI), James R. Clapper, has referred to the need to find the “sweet spot” between sharing and protecting information.¹

On a daily basis, professional intelligence officers attempt to find the “sweet spot.” Compromising secrecy can result in the loss of a source but restricting dissemination of information too narrowly may mean that it does not reach those who need it. The basic approach taken by the U.S. Government has been focused on establishing “need-to-know.” Sensitive information is made available only to those persons with appropriate clearances and a “need-to-know” that information for the performance of their duties. The complex systems for handling classified information, especially intelligence information, require careful background investigations of persons with access to classified information, approval by their agencies, and determinations that specific individuals or offices need to use specific classified information.

The contemporary U.S. Intelligence Community with its sixteen agencies is very large. The Defense Intelligence Agency (DIA) alone is said to have over 16,000 employees and the National Security Agency (NSA), the Central Intelligence Agency (CIA), the National Reconnaissance Office (NRO), and the National Geospatial-Intelligence Agency (NGA) also employ thousands of individuals and contractors. Thousands more work for the intelligence organizations of the four military services.

In many agencies an organizational culture has evolved over time that encourages a deep commitment to the agency’s mission and emphasizes support to a limited number of clients. The CIA and the State Department’s Bureau of Intelligence and Research (INR) focus on cabinet officials and the National Security Council (NSC) staff. Agencies in the Department of Defense (DOD) naturally focus on supporting the work of the Pentagon and the operating forces, especially those engaged in combat. In addition to the challenges involved in keeping information secure, organizational cultures and close ties to specific consumers have, however, the potential to discourage sharing information with other agencies. Some observers of bureaucratic practice have perceived a tendency for agencies to restrict dissemination of information that might provide leverage in the decisionmaking process.

In the aftermath of the 9/11 attacks in 2001, a consensus emerged that information sharing, especially between intelligence offices and law enforcement officials had been deficient and had contributed to the failure to detect the plot in advance. The U.S. Intelligence Community, now concentrating on the counterterrorism mission, moved to ensure that information with any potential relevance was shared with counterterrorism analysts throughout the Federal Government. (To a much greater extent than in other areas of intelligence concern, counterterrorism requires that bits of information from widely disparate sources be pieced together in a coherent pattern.)

¹ See Remarks and Q & A by Director of National Intelligence, Mr. James Clapper, 2010 Geospatial Intelligence Symposium, New Orleans, Louisiana, November 2, 2010.

The consensus in supporting intelligence information sharing persists. At the confirmation hearing for General Clapper as DNI in July 2010, Senator Dianne Feinstein, the Chairman of the Senate Select Committee on Intelligence (SSCI), advised the nominee that “Every day of every week, month by month, the DNI must assure coordination between intelligence agencies to eliminate duplication and improve information sharing.”² In April 2011, President Barack Obama explained his nomination of General David Petraeus to serve as Director of the Central Intelligence Agency: “he understands that staying a step ahead of nimble adversaries requires sharing and coordinating intelligence.”³

Better information sharing throughout the Federal Government and especially among the agencies of the Intelligence Community has become a priority for both the Executive Branch and Congress. In the aftermath of 9/11, major legislation included significant provisions to encourage and, in some cases, mandate greater sharing of information and these provisions have been implemented by both the Bush and Obama Administrations.

Changes Undertaken in Response to 9/11

Investigations of the September 11, 2001 attacks by the two congressional intelligence committees and the 9/11 Commission (the National Commission on Terrorist Attacks Upon the United States) concluded that a central obstacle to acquiring advance information on the plot was the inability to bring together all information that had been acquired about the plotters—there were many clues but they were retained in the files of different agencies. To some extent, information was not shared because of bureaucratic inertia, but in others efforts by determined analysts were quashed by officials determined to ensure that the “wall” between law enforcement and intelligence entities was not breached.⁴

² Hearing of the Senate (Select)Intelligence Committee, Nomination of Lieutenant General James Clapper to be Director of National Intelligence, Federal News Service Transcript, July 20, 2010.

³ White House, Office of the Press Secretary, Remarks by the President in a Personnel Announcement, April 28, 2011.

⁴ Relationships between the Intelligence Community and Federal law enforcement agencies—especially the Justice Department and the Federal Bureau of Investigation (FBI)—have varied between cooperation and competition. Although rivalries have existed since the J. Edgar Hoover era, counterintelligence operations and monitoring the activities of foreign agents in the U.S. required close coordination from the beginning of the Cold War. In general, however, the targets of the two sets of agencies, as well as the means by which information has been acquired, differed greatly. The primary goal of law enforcement agencies is to acquire evidence that can be used in court and the collection of which must comply with laws and regulations. Intelligence agencies, on the other hand, acquire information from any and all sources and ordinarily their products are used by policymakers and military commanders and not in court cases. In reaction to concerns that intelligence agencies used methods to collect information that violated the civil liberties of US persons, a number of restrictions were placed on the use of intelligence methods against U.S. persons, and limits established for the sharing of information regarding U.S. persons that was acquired incidentally. The result was the erection of a “wall” between intelligence and law enforcement agencies and analysts and even between different parts of the Justice Department. The “wall” was embedded in agency practice hindering the efforts to gain insight into the 9/11 plot. The extent to which the erection of the “wall” resulted from excessive zeal of key Justice Department officials during the Clinton Administration remains controversial, nevertheless prior to 9/11 there was little determination to remove it even in the first months of the G. W. Bush Administration, in part because of decisions of the Foreign Intelligence Surveillance Court that tended to reinforce it. The issue of the “wall” was addressed in the report of the National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington: Government Printing Office, 2004), pp.71-107. A more recent assessment may be found in Stewart A. Baker, *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism* (Stanford, CA: Hoover Institution Press, 2010), especially pp. 39-69.

Historically, the Federal Government has taken two complementary approaches to this paradox—intelligence information is provided only to those who have appropriate clearances, *i.e.*, they have had background investigations and been judged to be loyal, trustworthy, and capable of safeguarding classified information.⁵ Having a clearance is not, of course, sufficient to gain access to sensitive information; there must also be a “need-to-know,” *i.e.* the individual must have a work-related requirement for access to the information not just generalized curiosity. In theory everyone obtaining access to a given piece of classified information has (a) a clearance indicating that he or she is loyal and trustworthy and (b) a need for the information to perform his or her professional responsibilities. In actuality, of course, as with any human system, there can be mistakes. The number of genuine “secret agents,” foreign agents who have been successfully deceptive during their background investigations are very few but not non-existent. Much more numerous are individuals who can be bribed or who become disenchanted with their supervisors, or with a current U.S. policy, and proceed to illegally provide classified information to foreign governments or organizations. Also very damaging are individuals (or whole organizations) that become careless in handling classified information.

Even as information sharing was being made a statutory imperative, it was widely understood that any effort to share more information among intelligence agencies increased the risks of information being stolen or compromised. Various types of technical approaches were identified to maintain the security of shared information. Considerable attention to these approaches was reflected in the 2003 report of the Markle Foundation’s Task Force on National Security in the Information Age which has had an important influence on approaches to information sharing issues. The Task Force maintained that

There are no smart cards or tokens that cannot be cracked, biometrics are not 100 percent reliable, and high-quality passwords are difficult to remember, manage, and enforce. With all of these technologies there are also people and process issues (such as enrollment procedures and audit trails) that can undermine their integrity. Therefore, a multifactored system is a preferable approach. Multifactor authentication typically combines a password with a token or smart card and can include other forms of authentication including biometrics, challenge codes and questions, and profile access matching. Authentication is strongest when a part of the information resides with the user, a part with the token or smart card, and a part in the network. Credit card companies, good users of multifactor authentication, rely on tokens (credit cards), passwords (PIN), challenge questions (“What’s your mother’s maiden name?”), and profile matching (“Is this a typical charge for this individual?”).⁶

Counterterrorism requires wide varieties of disparate types of information, *e.g.* visa applications, flight manifests, ties to hostile organizations, conversations with known terrorists, efforts to obtain restricted materials, etc. In counterterrorism and other intelligence missions the intelligence analyst may be involved in piecing together stray bits of information. This greatly complicates establishing need-to-know standards. The WMD Commission argued:

⁵ Executive Order 13626, Classified National Security Information, sets forth the framework for designating and managing access to classified information.

⁶ Markle Foundation, Task Force on National Security in the Information Age, *Creating a Trusted Information Network for Homeland Security*, December 2003, p. 15. These technologies have not, however, been fully implemented. “One of the major contributing factors in the WikiLeaks incident was the large amount of data that was accessible with little or no access controls.” Senate Homeland Security and Government Affairs Committee, Hearing of Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration, March 10, 2011, Teresa Takai, Chief Information Officer and Acting Assistant Secretary of Defense for Networks and Information Integration, and Thomas Ferguson, Principal Deputy Under Secretary of Defense for Intelligence, Joint Statement for the Record.

If rigidly applied, the ‘need-to-know rule is incompatible with a networked environment. In a networked environment, providers of information cannot know for sure when a user ‘needs’ a particular piece of information. Instead . . . users of this service must be given access to all information broadly available on the network within the clearance levels of the individual user, and consistent with applicable privacy and civil liberties guidelines.⁷

As the Bush Administration’s 2007 National Strategy for Information Sharing stated:

Information acquired for one purpose, or under one set of authorities, might provide unique insights when combined, in accordance with applicable law, with seemingly unrelated information from other sources, and therefore we must foster a culture of awareness in which people at all levels of government remain cognizant of the functions and needs of others and use knowledge and information from all sources to support counterterrorism efforts.⁸

A particular complication of using information sharing to support counterterrorism efforts is the difficulty in maintaining separate procedures for handling information regarding U.S. persons.⁹ Many types of information including phone or email traffic may involve U.S. persons even if the particular target is a foreign national. Congress and the executive branch continue to address these and related issues in regard to provisions of the Foreign Intelligence Surveillance Act (FISA) and related legislation.¹⁰

Information sharing has proven to be essential for the counterterrorism mission and it is likely to be vital in other areas such as cybersecurity and in counterintelligence efforts aimed at preventing foreign exploitation of sensitive U.S. defense technologies. Other missions, such as gathering intelligence on the military plans and capabilities of foreign countries, may require less information from law enforcement agencies.

A major result of the 9/11 investigations was the USA Patriot Act (P.L. 107-56) and other legislation that removed most of the “wall.” Subsequently, the Justice Department modified the Federal Rules of Criminal Procedure to permit release of information relating to counterintelligence or foreign intelligence from grand jury investigations to other government agencies with strict protections against misuse.¹¹

⁷ 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, p. 439.

⁸ *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*, October 2007, pp. 2-3.

⁹ It is noteworthy that the National Strategy for Information Sharing provided that Federal agencies must “share protected information only to the extent that it is terrorism information, homeland security information, or law enforcement information related to terrorism.” (P. 27) “Protected information” is that which is covered by privacy protections of various laws, directives, and policies. Thus, these types of information would apparently not be shared for non-terrorism related efforts. However, the USA Patriot Act (P.L. 107-56) envisioned sharing of law enforcement information dealing with foreign intelligence, the national defense or the conduct of foreign affairs. (P.L. 107-56, sec. 203(b)(2)(B), 115 Stat. 280)

¹⁰ See CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Set to Expire May 27, 2011*, by Edward C. Liu

¹¹ See CRS Report RL31377, *The USA PATRIOT Act: A Legal Analysis*, by Charles Doyle; also CRS Report R40980, *Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization*, by Elizabeth B. Bazan, Charles Doyle, and Edward C. Liu, also CRS Report RL30252, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, by Richard A. Best Jr. There remain significant issues in regard to the co-mingling of foreign intelligence and U.S. person information. In testimony regarding the (continued...)

It was recognized, however, that removing restrictions on information sharing was by itself inadequate; there was a need to establish an organizational structure to ensure that information sharing was not just legally possible but institutionalized in routine agency practice. The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) established the position of the DNI with statutory authorities to foster information sharing. Specifically, the legislation provided that the DNI:

Shall have principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements.

Further, the DNI shall:

- (A) establish uniform security standards and procedures;
- (B) establish common information technology standards; protocols, and interfaces;
- (C) ensure development of information technology systems that include multi-level security and intelligence integration capabilities;
- (D) establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods;
- (E) develop an enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture; and
- (F) have procurement approval authority over all enterprise architecture-related information technology items funded in the National Intelligence Program.¹²

The National Counterterrorism Center (NCTC) was also established within the Office of the DNI with specific statutory authorities providing access to all information relevant to terrorist plots.¹³ NCTC analysts make use of data from all intelligence and law enforcement agencies as part of its counterterrorism responsibilities.

In addition, the Bush Administration published Executive Order 13388 on October 25, 2005 that mandated sharing of terrorist information and established an Information Sharing Council chaired by the Information Sharing Environment Program Manager and composed of representatives from major agencies with counterterrorism responsibilities. In October 2007 a National Strategy for Information Sharing described and provided guidance on information sharing at the Federal, state, local and tribal levels and with the private sector and foreign partners.¹⁴

(...continued)

Christmas 2009 bombing attempt, Russell Travers, a senior NCTC official indicated that privacy and policy concerns rather than technological capabilities limit the capabilities of analysts to perform searches across domestic and foreign intelligence databases. See U.S. Congress, Senate, Committee on Homeland Security and Governmental Affairs, "The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening," March 10, 2010, Federal News Service.

¹² P.L. 108-458, section 1011; 118 Stat. 3650.

¹³ See CRS Report R41022, *The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns*, by Richard A. Best Jr.

¹⁴ Efforts to share information with state and local authorities, with private organizations, and with foreign countries is (continued...)

The Information Sharing Environment

The President was also directed by the Intelligence Reform and Terrorism Prevention Act to establish an Information Sharing Environment (ISE) to facilitate the sharing of information relating to terrorism among all Federal agencies and state, local and tribal entities.¹⁵ The ISE, with a very small staff, is not focused solely on intelligence agencies, but works to establish consistent policy guidelines and technologies across five major communities—defense, intelligence, homeland security, foreign affairs, and law enforcement.¹⁶ It also reaches out to other agencies in the Federal Government and to state, local and tribal entities that are concerned with security issues.

The Act established the position of ISE Program Manager who prepares plans to improve information sharing and monitor implementation. The ISE extends beyond the Intelligence Community; indeed, it was designed to include State, local, and tribal entities and the private sector by providing policy guidelines and technological standards. The current ISE Program Manager, Kshemendra Paul, explained the role of his office in March 2011 testimony by use of a highway construction analogy: “[W]e are not pouring the concrete—rather, we are providing leadership and coordination of a complex set of factors that make the highway safe and navigable: governance and engagement, strategy and policy alignment, business process harmonization, guidelines, standards, and architecture. This leadership and coordination enables our mission partners—the general contractors building and managing the day-to-day operation of the highways—to build to common specifications.”¹⁷ The goal has been to

normalize federal security practices and risk management methodologies to foster acceptance government-wide. That acceptance then leads to ‘reciprocity’ between agencies, i.e., recognition that each organization’s protection processes and systems are trusted to perform securely and predictably.¹⁸

As ISE Program Manager, Mr. Paul does not control information sharing among agencies but rather his office issues “government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE.”¹⁹

(...continued)

discussed in CRS Report R40901, *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*, by Mark A. Randol and CRS Report RL34070, *Fusion Centers: Issues and Options for Congress*, by John Rollins.

¹⁵ ISE is the term used to describe the “collection of end-to-end mission processes and supporting core capabilities, enabled by standards, architecture, security, access, privacy protection, policy, governance, and management.” Program Manager, Information Sharing Environment, *ISE: Information Sharing Environment: Annual Report to the Congress*, July 2010, p. xi.

¹⁶ See Government Accountability Office, *Information Sharing Environment: Definition of the Results to be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GAO-08-492, June 2008. According to GAO, in 2008 the ISE had a staff of 11 government officials and 31 contractors organized into three divisions—technology, policy and planning, and business process. (P. 11) At that time the GAO concluded that “the ISE is still without a clear definition of the specific results to be achieved as part of the ISE or the projects, stakeholder contributions, and other means needed to achieve these results.” (P. 31)

¹⁷ Kshemendra Paul, Program Manger for the Information Sharing Environment, Statement for the Record before the Senate Homeland Security and Governmental Affairs Committee, March 10, 2011.

¹⁸ ISE, *Annual Report to the Congress*, July 2010, p.p53-54.

¹⁹ *Ibid.*, p. 61.

Separate from the ISE is the *Intelligence Community Information Sharing Executive (IC ISE)* whose responsibilities extend only to intelligence agencies. Under the direction of the DNI, the IC ISE prepares plans for encouraging information sharing among intelligence agencies and monitors their implementation with periodic progress reports to the DNI. In March 2011 testimony the IC ISE, Corin R. Stone, described the three-pronged IC ISE strategy for maintaining the security of information within the context of information sharing:

- The first is ACCESS: ensuring that the right people can discover and access the networks and information they need to perform their duties, but not to information that they do not need. This is a complex matter that is centered on the principle of determining “Need to Know.”
- The second element is TECHNICAL PROTECTION: technically limiting the ability to misappropriate, manipulate, or transfer data, especially in large quantities, such as by disabling or prohibiting the use of removable media on classified networks, including thumb drives and CDs.
- The third area is AUDITING and MONITORING: taking actions to give the IC day-to-day confidence that the information access granted to our personnel is being properly used. This involves monitoring and auditing use activity on classified computer systems to identify anomalous activity, and following up accordingly.²⁰

The IC ISE is working to provide end-to-end management technology; it is implementing user authentication by the first quarter of FY2012. During FY2012, there are plans to leverage an Enterprise Audit Framework to enhance the sharing of audit data across the Intelligence Community.²¹ From the testimony it was unclear, however, how much of this effort involves the ISE establishing technical standards and procedures and how much it involves the acquisition of new systems and their deployment.

Information sharing has become a central mission for intelligence agencies. In addition to statutory mandates in the Intelligence Reform Act of 2004 and other legislation, the DNI issued **Intelligence Community Directive 501**, Discovery and Dissemination or Retrieval of Information within the Intelligence Community, on the last day of the G.W. Bush Administration. This Directive requires (section D.1) that “IC elements shall treat information collected and analysis produced as national assets and, as such, shall act as stewards of information who have a predominant ‘responsibility to provide.’” The Directive adds, (in section D.2.(b.)): “‘Stewards’ . . . shall fulfill their ‘responsibility to provide’ by making all information collected and analysis produced by an IC element available for discovery by automated means by authorized IC personnel, unless otherwise determined by the DNI.” Those who are authorized, according to section D.3., “have a ‘responsibility to discover’ information believed to have the potential to contribute to their assigned mission need.” These policy documents and repeated statements by senior intelligence officials have made it quite clear that the formal framework of intelligence collection and analysis is now built around the imperative of sharing information.

²⁰ Corin R. Stone, Intelligence Community Information Sharing Executive, Office of the Director of National Intelligence, Statement for the Record before the Senate Homeland Security and Governmental Affairs Committee, March 10., 2011

²¹ Ibid.

Congressional backing for information sharing within the Intelligence Community appears solid. In addition to the comments by Senator Feinstein noted above, Representative Mike Rogers, the Chairman of the House Permanent Select Committee on Intelligence (HPSCI), has been a strong proponent of integrating information across the Community.²² Support for sharing has not just been verbal; section 402 of the Intelligence Authorization Act for FY2010, P.L. 111-259, enacted October 7, 2010 provided the DNI authority to transfer funds to non-intelligence agencies that maintain systems to store and disseminate intelligence information.

At the same time there are efforts to better protect the security of shared information. In March 2011, DNI James Clapper signed Intelligence Community Directive 502, Integrated Defense of the Intelligence Community Information Environment. This directive mandates the development and implementation of an Intelligence Community-wide approach to defending the intelligence information environment. A concept of operations is to be developed and issued later in 2011 and will establish standards for all intelligence agencies.

The FY2011 Intelligence Authorization bill, H.R. 754, that has been passed by both chambers, includes a provision (section 402) that mandates an effective automated insider threat detection program to be established by October 2013. The report accompanying the Senate version of the bill (S. 719) does not provide details of the program but the use of the term “automated” suggests capabilities to ensure that data is not downloaded or transmitted without authorization, and that a record of transmissions be maintained.²³

Limitations and Risks of Information Sharing

Intelligence sharing has contributed to a number of significant successes. Often mentioned is the arrest of Najibullah Zazi before he could successfully detonate explosives in the New York City subway in 2009 along with a number of other plots planned to occur in the U.S. and against U.S. interests abroad. Most recently, the successful attack on Osama Bin Laden in May 2011 has been officially credited to cooperation among the CIA, NSA, and NGA in particular.²⁴

However, despite the best efforts—and significant successes—of the Intelligence Community in recent years in identifying terrorist plots and providing solid intelligence to policymaking agencies and to military forces fighting in two wars, several important cases suggest that significant impediments to information sharing have persisted. On the other hand, sharing of information led to unauthorized disclosures on the Internet and in the media that have reportedly jeopardized intelligence sources and undermined U.S. diplomacy.

²² See Council on Foreign Relations, Transcript, Mike Rogers, Chairman, Permanent Select Committee on Intelligence, U.S. House of Representatives, *Intelligence Lessons Learned from the Recent Osama Bin Laden Operations*, May 11, 2001.

²³ U.S. Congress, Senate Select Committee on Intelligence, 112th Cong., 1st sess., *Intelligence Authorization Act for Fiscal Year 2011*, S.Rept. 112-12, April 4, 2011, pp. 3-4.

²⁴ Office of the Director of National Intelligence, *Statement of the Director of National Intelligence James R. Clapper on the Death of Osama Bin Laden*, May 2, 2011.

Detroit Bomb Attempt

One significant lapse was the so-called Christmas bombing of December 2009 in which a Nigerian man, Umar Farouk Abdulmutallab, attempted to detonate an explosive on a plane approaching Detroit. The attempt failed because of action by passengers and crew but many questioned why the individual had been allowed to board the aircraft. Concerns grew when it was revealed that the bomber's father had actually warned U.S. embassy officers in Nigeria that his son may have become radicalized. A report by the Senate intelligence committee concluded that there were various failures to sharing information. "The inconsistencies in distributing key intelligence reports may have contributed to the failure of the Intelligence Community to identify Abdulmutallab as a potential threat. While there was no intent to limit access to the reports, processes failed to disseminate relevant intelligence to all offices and individuals with a need to know."²⁵ In particular, reporting was not disseminated to all appropriate CIA elements, some reporting was not disseminated until after the attempted attack, some FBI counterterrorism analysts could not access all relevant reports, and analysts at the National Counterterrorism Center did not connect "key intelligence reporting with the other relevant reporting."²⁶ President Obama described it as "a failure to connect the dots of intelligence that existed across our intelligence community and which, together, could have revealed that Abdulmutallab was planning an attack."²⁷ In additional views to the Senate Report, Senators Saxby Chambliss and Richard Burr targeted technological issues:

. . . technology across the Intelligence Community still is not adequate to provide search enhancing tools for analysts. Several of the intelligence analysts involved in the Abdulmutallab case said that they were unable to link together the various reports on Abdulmutallab due to the struggle to balance searching the large volume of terrorism-related intelligence available with their daily workloads. The large number of intelligence databases compounded this problem by forcing some analysts and collectors to search multiple databases. NCTC officials told Committee staff that NCTC does not have the technical ability to follow or process all leads. Rather, NCTC is dependent on its personnel to conduct complex searches in multiple intelligence databases and to rely on the memory and knowledge of those analysts to link intelligence. CIA has similar problems with its main all-source counterterrorism database. This remains a problem today.²⁸

Fort Hood Shooting

In another incident, Army Major Nidal Hasan, was accused of shooting some 45 servicemembers at Ft. Hood, Texas on November 5, 2009, of whom 12 died in addition to one civilian. An investigation by the Senate Homeland Security and Governmental Affairs Committee concluded that information about his contacts with foreign terrorists had not been appropriately shared. The committee report found that:

the FBI and DOD failed to recognize and to link the information they possessed even though they had advantages with respect to Hasan as compared to other lone wolves: (1) Hasan was

²⁵ U.S. Congress, Senate, Select Committee on Intelligence, 111th Congress, 2nd sess., *Attempted Terrorist Attack on Northwest Airlines Flight 253*, May 24, 2010, S.Rept. 111-199, p. 5.

²⁶ *Ibid.*, pp.2, 7.

²⁷ U.S. President, Remarks by the President on Strengthening Intelligence and Aviation Security, January 7, 2010.

²⁸ S.Rept. 111-199, p. 12.

a military officer who lived under a regimented system with strict officership and security standards, and (2) the government had learned of communications from Hasan to the subject of an unrelated FBI terrorism investigation [REDACTED].²⁹

Senators Lieberman and Collins further underscored the reason for information sharing: “As has been proven time and again in the intelligence context, information that may not appear troubling to one analyst may complete the puzzle for another analyst who has a different perspective or access to other information.”³⁰

Their report criticized in particular the role of the FBI’s Joint Terrorism Task Forces (JTTFs) for failing to ensure that analysts could access all available information. It was unclear to the Committee if officials “detailed” to JTTFs from agencies outside of the FBI were serving as representatives of their home agencies or as part of the JTTF analytical team. The committee noted a tendency not to share FBI information with the detailees. “As revealed in the Hasan case and reinforced by other evidence, detailees to JTTFs have often lacked adequate access to databases and training but paradoxically are relied upon to lead JTTF investigations.”³¹ Further, the FBI itself had problems with finding relevant information.

The report points out that the FBI could not easily link Hasan’s initial communications with the Suspected Terrorist to his later communications, and the failure to do so was a factor in the government not intervening against Hasan before the attack, and the FBI should have identified and remedied its inability to link his communications together prior to the attack.³²

WikiLeaks

In addition to other factors, the Detroit bomb attempt and the Fort Hood shooting resulted from failures to share available information, to analyze disparate pieces of intelligence, and provide notice to responsible officials in a timely manner. On the other hand, the WikiLeaks disclosures that began in 2010, have drawn considerable attention to the risks that widespread information sharing entails. One U.S. soldier in Iraq was reportedly able to download many thousands of State Department cables and transfer them to unauthorized recipients who published them on the Internet and in a number of newspapers.³³ Most of the messages disseminated to the media were not from intelligence agencies and damage to U.S. intelligence efforts has not been publicly addressed.³⁴ According to congressional testimony by DOD officials in March 2011, forward

²⁹ Chairman Joseph I. Lieberman and Ranking Member Susan M. Collins, U.S. Senate Committee on Homeland Security and Governmental Affairs, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government’s Failure to Prevent the Fort Hood Attack*, February 2011, p. 8.

³⁰ *Ibid.*, p. 75.

³¹ *Ibid.*, p. 87.

³² *Ibid.*, p. 65.

³³ According to media reports large volumes of documents were downloaded onto CD’s, a far easier process than those followed in previous decades when copying large quantities of documents required that paper copies be acquired, removed from government offices, copied overnight or on weekends on private copiers, and then carefully returned to their storage facilities before their loss could be discovered. See, for instance, David Rudenstine, *The Day the Presses Stopped: A History of the Pentagon Papers Case* (Berkeley, CA: University of California Press, 1996), p. 42, and Ronald J. Olive, *Capturing Jonathan Pollard* (Annapolis, MD: Naval Institute Press, 2006), pp. 69-73.

³⁴ Most of the publicity surrounding the events has focused on State Department operational cables, a number of which did discuss intelligence matters; as Bill Keller, the editor of the *New York Times*, has noted some of the material “included sensitive American programs, usually related to intelligence. We agreed to withhold some of this (continued...)”

deployed units had access to a network (the Secret internet Protocol Router Network (SIPRNet)) that has between 400,000 and 500,000 DOD users. As DOD officials testified, “The expanded use of computer networks has also increased the opportunity for even a single authorized user to access, copy, manipulate, download, and intentionally publicize enormous amounts of information from the interconnected databases of interconnected agencies.”³⁵ State Department representatives at the hearing indicated that the practice of making diplomatic cables available on SIPRNet has ended.

The WikiLeaks incident reflects a number of concerns that affect intelligence information sharing. First, there are inevitably communications personnel and message handlers who are in a position to do serious damage. Secondly, widespread use of computer databases increases the number of individuals with access as well as the number of documents that are accessible. Furthermore, intelligence officials have to be aware that once information is made available to bloggers or journalists, with a number of exceptions, there are very few legal restraints on their ability to make it public on the Internet or in the media.³⁶

In the wake of WikiLeaks and other disclosures of classified information some observers may call into question the advisability of greater and more routine information sharing among intelligence agencies. Indeed, as Representative Rogers, the HPSCI Chairman, has commented: “Need-to-know is an important provision when you are trying to do some operation to keep us safer. But need-to-share got us into trouble with WikiLeaks and with other leaks.”³⁷ Mass leaks of documents that reveal the names of U.S. contacts in foreign countries and foreign governments, including their intelligence services could result in severe repercussions and even death for individuals who have attempted to assist the U.S. Observers also believe that public revelations about U.S. successes in monitoring foreign communications channels would lead to their discontinuance. There is, some observers suggest, a reasonable likelihood that greater restrictions on dissemination of sensitive intelligence lowers the chances for leaks and compromises.

Conclusion

There are a number of technical approaches to reducing opportunities for unauthorized sharing of information. Computers can be configured to prevent downloading of large document files. Computers can also be programmed to make any downloads identifiable by date, time and individual. According to media accounts some of these features have been available on government systems but were not activated. Congress may choose to determine if these reports are accurate and if changes currently being planned by the Intelligence Community have been

(...continued)

information. . . .” He also noted that “One of our first articles drawn from the [leaked] diplomatic cables. . . reported on a secret intelligence assessment” Bill Keller, “The Boy Who Kicked the Hornet’s Nest,” *New York Times Magazine*, January 30, 2011, p. 38.

³⁵ U.S. Congress, Senate, Committee on Homeland Security and Governmental Affairs, “Hearing on Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration,” Joint Statement for the Record, Teresa Takai, Chief Information Officer and Acting Assistant Secretary of Defense for Networks and Information and Integration, and Thomas Ferguson, Principal Deputy Under Secretary of Defense for Intelligence, March 21, 2011.

³⁶ See CRS Report R41404, *Criminal Prohibitions on the Publication of Classified Defense Information*, by Jennifer K. Elsea.

³⁷ J.J. Green, “U.S. Intelligence Agencies ‘Sharing Too Much,’” January 19, 2011, <http://www.wtop.com/?sid=2240792&nid=778>.

instituted. In calling for legislation to address the dangers of unauthorized information sharing, HPSCI Chairman Rogers emphasized the need for “smart access,” which is “an identity-based information security management system that improves our ability to detect and deter the few bad actors, and not unnecessarily punish responsible actors by denying them access to the sensitive information they need to get their work done.”³⁸

Congress may wish to review the Information Sharing Environment to ensure that there are proper boundaries to intelligence information sharing and that appropriate metrics are established to assist in determining what information must be limited to a very narrow set of consumers. As noted above, however, it may be very difficult, given the requirements of counterterrorism, to know in advance what information a counterterrorism analyst will “need to know.” Although these analysts will need to be able to draw on a multiplicity of databases, observers suggest that there are ways to categorize information according to especially sensitive programs and all agree that not every analyst needs to be able to see every piece of information.³⁹ An oft-cited concern is the tendency to over-classify documents which adds to administrative burdens and undermines respect for the classification process.

It is possible to limit dissemination of especially sensitive information, whether it is sensitive because of the nature of its contents or because it was acquired from an especially sensitive source. It is also possible to prevent the downloading and reproduction of large masses of information. It is possible to trace the identities of those who had access to particular pieces of information. Ultimately, however, security depends on the loyalty of cleared officials at all levels. A clerk with the right access can unlawfully transfer highly sensitive information as readily or more readily than a senior official. Some highly sensitive information—the identity of an agent or the fact that a code has been broken—can be found in a short document or even memorized for verbal transmission.

Those responsible for information security must of course be aware of the extent of the interest in acquiring classified U.S. information. Foreign countries (including friendly ones or even allies) may not turn down opportunities to gain insight into U.S. policymaking or military capabilities. Various anti-American organizations worldwide eagerly seek information that can damage or embarrass the U.S. Government. Major media outlets, not all of which are in foreign countries,⁴⁰ consider themselves free to publish classified information regardless of possible damage to U.S. persons, interests, or foreign supporters. There is, in short, an active market for classified information held by U.S. intelligence agencies with thousands of officials having some access. Personnel security is a crucial part of the problem. Despite procedural and technical approaches taken to limit misuse of classified information, disloyal or careless officials can be the source of leaks.

³⁸ House Permanent Select Committee on Intelligence, Chairman Mike Rogers Opening Statement, Worldwide Threat Hearing, February 10, 2011.

³⁹ In particular, only a small percentage of intelligence analysts will have a continuing need to review diplomatic cables that report sensitive conversations between senior U.S. officials and their foreign counterparts.

⁴⁰ Sarah Ellison, “The Man Who Spilled the Secrets,” *Vanity Fair*, February 2011, describes the process by which the *Guardian* newspaper in the U.K. set up a secretive “research bunker” to process documents obtained by the WikiLeaks organization. The *Guardian* sought an American media partner to assist with publishing the documents since “it is unlikely that U.K. courts could block publication, but it’s even more unlikely that the U.S. government would go after *The New York Times*, given the strong First Amendment protections and the precedent set by the Pentagon Papers case.” (P. 146.)

For the U.S. Intelligence Community, the policy decision of whether the emphasis should be on “need-to-know” or the “need-to-share” can be viewed as a false choice. Information must always be shared with those with a genuine need to know even if this potential universe is a large one. At the same time, Congress may wish to ensure that clearance procedures are thorough as well as expeditious. More rigorous analyses of instances in which cleared personnel have transferred or sold classified information may lead to improved procedures for maintaining security. There may well be more technological approaches that will make it possible to establish greater accountability for the use of classified intelligence information

Intelligence efforts are never risk-free. Acquiring information is often hazardous; analysis efforts can be wrong and result in mission failure and the loss of life. Good analysis can be delayed or not provided to the right consumer in a timely manner resulting in expensive wasted efforts. Congressional oversight of intelligence activities can improve executive branch performance and provide encouragement to intelligence officials to prevent compromises of sensitive materials. Ultimately, however, a degree of risk seems inevitable.

Government officials must also accept the enduring reality of a media culture that is prepared to publish official secrets and considers such disclosure a patriotic contribution to democratic discourse. That individual civil servants or servicemembers can be very harshly punished for their role in releasing information while editors and reporters are honored and celebrated seems to some as paradoxical. Ultimately the security of information, as is the case with the security of the nation, depends on those who willingly uphold the oaths that they have taken.

Author Contact Information

Richard A. Best Jr.
Specialist in National Defense
rbest@crs.loc.gov, 7-7607