

DEPARTMENT OF HOMELAND SECURITY AND INFORMATION SHARING: IS IT WORKING?

BY

LIEUTENANT COLONEL MICHAEL J. PAPPAS
United States Army

DISTRIBUTION STATEMENT A:

Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2010

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.



U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 30 MAR 2010		2. REPORT TYPE		3. DATES COVERED	
4. TITLE AND SUBTITLE Department of Homeland Security and Information Sharing: Is it Working?				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Michael Pappas				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT see attached					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 26	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

PROPERTY OF U.S. ARMY

USAWC STRATEGY RESEARCH PROJECT

DEPARTMENT OF HOMELAND SECURITY AND INFORMATION SHARING: IS IT WORKING?

by

Lieutenant Colonel Michael J. Pappas
United States Army

Professor Frank Jones
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Michael J. Pappas

TITLE: Department of Homeland Security and Information Sharing: Is it Working?

FORMAT: Strategy Research Project

DATE: 22 March 2010 **WORD COUNT:** 5,404 **PAGES:** 26

KEY TERMS: PATRIOT Act, Intelligence Community, FISA, Wiretapping, Terrorism, Nidal Malik Hasan, Umar Farouk Abdul Mutallab, September 11, 2001

CLASSIFICATION: Unclassified

This paper looks at the organization of the Intelligence Community (IC) of the United States prior to September 11th, and the intelligence community reorganization that was the result of the USA PATRIOT Act of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), the creation of the White House's Office of Homeland Security, and later the Department of Homeland Security in 2002. Additionally, the paper will examine the IC and the information/intelligence sharing agreements within the community and explore whether they are working. The paper will consider two recent incidents that occurred in the United States or in the airspace above America. Specifically, the Ft. Hood shooting incident by accused U.S. Army Major Nidal Malik Hasan and the attempted Christmas day bombing of an American airliner by accused attacker, Umar Farouk Abdul Mutallab. Lastly, this paper will examine if the IC created by the PATRIOT Act of

2001 and the Homeland Security Act of 2002 have promoted successful performance and if not, and what lessons learned from these two recent events.

DEPARTMENT OF HOMELAND SECURITY AND INFORMATION SHARING: IS IT WORKING?

The lessons to America are clear as day. We must not again be caught napping with no adequate national intelligence organization. The several Federal bureaus should be welded together into one, and that one should be eternally and comprehensively vigilant.

—Arthur Woods
1919¹

The quote above from Arthur Woods, police commissioner of New York City, was made in reference to intelligence and law enforcement failures in dealing with the espionage directed against the United States by Germany during World War I. This quote could have just as easily been made by a politician or government official after the terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001. This paper looks at the organization of the Intelligence Community of the United States prior to September 11th, and the Intelligence Community reorganization that was the result of the USA PATRIOT Act of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), the creation of the White House's Office of Homeland Security, and later the Department of Homeland Security in 2002. Additionally, the paper will examine the Intelligence Community and the information/intelligence sharing agreements within the community and at the state and local levels and explore whether they are working. The paper will consider two recent incidents that occurred in the United States or in the airspace above America. Specifically, it will look at the Ft. Hood shooting incident by accused U.S. Army Major Nidal Malik Hasan and the attempted Christmas day bombing of an American airliner by accused attacker, Umar Farouk Abdul Mutallab. Lastly, this paper will examine if the Intelligence Community created by the PATRIOT Act of 2001 and the

Homeland Security Act of 2002 have promoted successful performance and if not, and what lessons learned from these two recent events.

Background

Even before the tragedy of Pearl Harbor in December 1941, President Franklin D. Roosevelt was concerned about American intelligence deficiencies. He asked New York lawyer William J. Donovan to draft a plan for an intelligence service.² Donovan created the predecessor to the Central Intelligence Agency, the Office of Strategic Services. Not everyone in the intelligence world was happy with the creation of the OSS because clear lines of responsibilities were not established. Since the early 1930s the FBI had been responsible for intelligence work in Latin America, and the military services protected their areas of responsibility.³ It wasn't until after World War II and the passage of The National Security Act of 1947 that the first steps toward intelligence reform would occur.

The National Security Act of 1947 was signed into law by President Harry S. Truman on July 26, 1947. The act created the Central Intelligence Agency (CIA) and the National Security Council (NSC). Further, it charged the CIA with coordinating the nation's intelligence activities and correlating, evaluating and disseminating intelligence that affects the nation's security. In addition, the CIA was to perform such other duties and functions related to intelligence as the NSC might direct. The law also made the Director of Central Intelligence (DCI) responsible for protecting intelligence sources and methods.⁴

The next major change in intelligence reform occurred when President Ford issued Executive Order 11905, United States Foreign Intelligence Activities, on 18 February 1976. The purpose of the order was, "to establish policies to improve the

quality of intelligence needed for national security, to clarify the authority and responsibilities of the intelligence departments and agencies and to establish oversight....”⁵ In this executive order, President Ford thought it necessary to state the duties of the Director of Central Intelligence. Those included, “pursuant to the National Security Act of 1947, [the DCI] shall be responsible directly to the National Security Council and the President.” Additionally, he shall “Act as the executive head of the CIA and the Intelligence Community Staff.”⁶

To understand the Intelligence Community and to appreciate the problems that the 2001 terrorist events pointed out, understanding agencies constitute the Intelligence Community is required. The Intelligence Community (IC) was codified as a group in Executive Order 12333, signed by President Reagan on December 4, 1981. At the time, the IC included: the four military services’ intelligence components as well as the various national intelligence agencies: (the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, the National Imagery and Mapping Agency, the Department of Energy (DOE), the Department of Treasury, the State Department’s Bureau of Intelligence and Research (INR), the Drug Enforcement Agency (DEA), the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA). The Director of Central Intelligence (DCI) was designated the head of the community.

What is important to note about the IC is how many members are a part of the Department of Defense (DoD). With the majority of the agencies as part of DoD, it is easy to see these agencies’ primary role as being to support the military and its requirements. With the IC community being funded by many different appropriations,

there was truly not one individual or organization in charge. Although the DCI was the head of the IC by statute, the truth of the matter came down to who controls the money and in a large part, most of the funding was controlled by the Secretary of Defense.

What happened over the course of time since the National Security Act of 1947 and the creation of all the intelligence organizations was that each member of the IC developed its own culture on sharing of intelligence. The Intelligence Community's "need-to-know" culture, a necessity during the Cold War became widespread throughout the community.⁷ Many members of the community believed that if an agency collected the intelligence, then it was up to the director of that agency to decide who "needed to know". Special intelligence handling caveats such as Originator Controlled kept the intelligence within the agency that collected it. The way the U.S. government is designed as well as this culture drove intelligence into stovepipes. The 9/11 report states,

Lines of operational authority run to the expanding executive departments, and they are guarded for understandable reasons: the DCI commands the CIA's personnel overseas; the Secretary of Defense will not yield to others in conveying commands to military forces; the Justice Department will not give up the responsibility of deciding whether to seek arrest warrants. But the result is that each agency or department needs its own intelligence apparatus to support the performance of its duties. It is hard to break down "stovepipes" when there are so many stoves that are legally and politically entitled to have cast-iron pipes of their own.⁸

This lack of working together led the 9/11 Commission to observe, "National Intelligence is still organized around the collection disciplines of the home agencies, not the joint mission. The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots." No one component holds all the relevant information."⁹

The Terrorist Threat Against the United States

The attacks of September 11, 2001 were not the first indication that the United States needed a strategy for homeland security. Plans to attack the United States were developed with unwavering single-mindedness throughout the 1990s.¹⁰ Usuma Bin Ladin and his Al Qaeda fighters were instrumental in helping Somali Warlords in 1993 defeat the United States in Somalia and begin a purge of American influence in the region. In fact the 9/11 Commission report states that some anti-American operations in Somalia were directly supervised by Al Qaeda's military leaders.¹¹ Additionally, the World Trade Center bombing in 1993, the Embassy bombings in Africa and the plot in 1995 to blow up airliners over the Pacific all have ties to Al Qaeda.¹²

Terrorism and attacks against the United States moved up in priority in the Clinton administration. President Clinton addressed homeland security in his 1996 National Security Strategy stating:

At the same time the challenges to the security of our citizens, our borders and our democratic institutions from destructive forces such as terrorists and drug traffickers is greater today because of access to modern technology. Cooperation, both within our government and with other nations is vital in combating these groups that traffic in organized violence...countering terrorism effectively requires close day to day coordination among executive branch agencies.¹³

Terrorism and transnational threats continued to play an important role in the Clinton administration and were on the President's mind when he issued a new National Security Strategy in 1997. The strategy stated:

Combating these dangers which range from terrorism, international crime, and trafficking in drugs and illegal arms, to environmental damage and intrusions in our critical information infrastructures requires far-reaching cooperation among the agencies of our government as well as with other nations.¹⁴

However, on October 12, 2000, discussion about terrorism and the transnational threat moved to the forefront when the USS Cole was attacked by terrorists in Yemen. The attack severely damaged the ship and left seventeen sailors dead and thirty-nine injured.¹⁵ With a presidential election only days away, Republican presidential candidate George W. Bush stated to CNN, “I hope that we can gather enough intelligence to figure out who did the act and take the necessary action. There must be a consequence.”¹⁶ Lack of actionable intelligence and failure to “connect the dots” in the years before September 11, 2001 and especially immediately preceding the attack would lead the United States to dramatically change the organization of the U.S. government’s executive departments.

Homeland Security

Homeland security and the enormous number of agencies and department with a homeland security role was an issue before September 11, 2001. The U.S. Commission on National Security/21st Century, also known as the Hart-Rudman Commission, identified many problems. In February 2001, it recommended, “significant and comprehensive institutional and procedural changes throughout the executive and legislative branches in order to meet future national security challenges...the creation of a new National Homeland Security Agency to consolidate and refine the missions of the different departments and agencies that had a role in U.S. homeland security.”¹⁷ Additionally, in March 2001, Representative Mac Thornberry introduced a bill to create a National Homeland Security Agency.¹⁸ Thornberry’s bill would combine several separate agencies and offices related to homeland security into a single department. At the time, however, Congress did not have the impetus to make any changes in the executive branch’s organization and no action was taken on Thornberry’s proposal. It

was the events of September 11, 2001 that spurred the Congress to action and before a bill could be created and passed, President Bush acted when he signed Executive Order 13228 on October 8, 2001, creating the Office of Homeland Security in the Executive Office of the President.

When President Bush signed the executive order creating the office, there were more than 40 federal agencies and more than 2,000 separate congressional appropriation accounts that dealt with some kind of homeland security activity.¹⁹ In fact, by June 2002 when the President put forth his proposal to create the Department of Homeland Security (DHS), his proposal identified that responsibilities for homeland security were dispersed among more than 100 different government organizations.²⁰

Additionally in the executive order, the President addressed information sharing by directing that the Office of Homeland Security would:

Ensure that, to the extent permitted by law, all appropriate and necessary intelligence and law enforcement information relating to homeland security is disseminated to and exchanged among appropriate executive departments and agencies responsible for homeland security and, where appropriate for reasons of homeland security, promote exchange of such information with and among State and local governments and private entities.²¹

Less than eight months after signing this executive order, President Bush proposed the creation of a Department of Homeland Security. This approach would give homeland security additional emphasis by establishing cabinet level “authority” and it would demonstrate the importance of homeland security as a separate government function. . President Bush outlined the proposed department’s essential missions:

- Border and Transportation Security – Control the borders and prevent terrorists and explosives from entering the country.
- Emergency Preparedness and Response – Work with state and local authorities to respond quickly and effectively to emergencies.

- Chemical, Biological, Radiological, and Nuclear Countermeasures - Bring together the country's best scientists to develop technologies that detect biological, chemical and nuclear weapons to best protect citizens.
- Information Analysis and Infrastructure Protection – Review intelligence and law enforcement information from all agencies of government, and produce a single picture of threats against the homeland.²²

On June 18, 2002, President Bush formally submitted his proposal to Congress, including draft text for the statute that would become known as the Homeland Security Act of 2002.²³ Congress passed the legislation that the President proposed and he would sign the Homeland Security Act into law on 25 November 2002.

Within a year after the attacks of September 11, 2001 on the United States, the President and Congress enacted two major pieces of legislation, the PATRIOT Act and the Homeland Security Act. Based on these statutes, the homeland was to be more secure and intelligence and information sharing was to improve. But the important questions to ask are what did these two acts allow, and what actually has been the practice in using these acts to protect the homeland?

USA PATRIOT Act

The PATRIOT Act as mentioned previously was passed in response to the attacks on the U.S. homeland. According to the Congressional Research Service, the law gave “federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence gathering purposes.”²⁴ Additionally, it strengthened U.S. our borders and provided new authorities to the Department of the Treasury to fight the financial side of terrorism while it created new crimes, new penalties, and new procedural efficiencies for use against domestic and international terrorists.²⁵

To understand what the PATRIOT Act provides with respect to “track and intercept communications”, it is critical to understand the statute’s provisions. Based on previous violations of individual rights, and spying upon its citizens by intelligence and law enforcement agencies, privacy laws were enacted by Congress. As a result, federal law features a three tiered system, erected for the dual purpose of protecting the confidentiality of private telephone, face-to-face, and computer communications while enabling authorities to identify and intercept criminal communications.²⁶ To put this concept of tiered levels in laymen’s terms, the first level prohibits electronic eavesdropping unless the Department of Justice (DoJ) obtains approval through the federal court system. The next level deals with protection of information such as information held in internet storage centers and telephone records. The last level deals with what are known as “pen registers” which are the least obtrusive of collection means, and is basically a form of “caller id” with which most individuals are familiar.

The PATRIOT Act deals with all three levels and is consistent with the protections of the Fourth Amendment to the U.S. Constitution, which safeguards citizens against unreasonable searches and seizures. The PATRIOT Act authorizes nationwide execution of court orders for trap and trace devices and access to stored email or communications records.²⁷ Additionally, the Act treats voicemail like e-mail and allows the intercept of communications to and from a recipient within a computer system (with the permission of the system’s owner).²⁸ What this means is that as long as AT&T or any other company gives the government permission, then the sender or receiver or the information isn’t required to know about the collection of the information.

Foreign Intelligence collection means were also changed with the PATRIOT Act, which clearly contemplates closer working relations between criminal investigators and foreign intelligence investigators, particularly in cases of international terrorism.²⁹ Originally, the Foreign Intelligence Surveillance Act (FISA) required that the reason for the collection of the information was to obtain foreign intelligence or information. Many individuals that were arrested as a result of a FISA warrant questioned whether the information that was used against them in the criminal trial was actually collected as part of a “foreign intelligence” effort or if the information was collected under the guise of a foreign intelligence requirement. The PATRIOT Act amended the FISA laws to encourage intelligence and law enforcement officials to work together.

The PATRIOT Act allows the IC to collect information more easily and to receive information gathered during criminal proceedings. The following perceived shortcomings with FISA were addressed by the PATRIOT Act:

- permits “roving” surveillance (court orders omitting the identification of the particular instrument, facilities, or place where the surveillance is to occur when the court finds the target is likely to thwart identification with particularity)
- increases the number of judges on the FISA court from 7 to 11
- allows application for a FISA surveillance or search order when gathering foreign intelligence is a *significant* reason for the application rather than *the* reason
- authorizes pen register and trap & trace device orders for e-mail as well as telephone conversations
- sanctions court ordered access to any tangible item rather than only business records held by lodging, car rental, and locker rental businesses
- carries a sunset provision

- establishes a claim against the United States for certain communications privacy violations by government personnel
- expands the prohibition against FISA orders based solely on an American's exercise of his or her First Amendment rights.³⁰

Law enforcement and intelligence have always had competing demands. These demands created walls to sharing information between the two organizations to ensure evidence could be admitted in prosecutions. The PATRIOT Act works to remedy this unfortunate artificial wall. In fact, the National Security Act of 1947 states,

elements of the Intelligence Community may, upon the request of a United States law enforcement agency, collect information outside the United States about individuals who are not United States persons. Such elements may collect such information notwithstanding that the law enforcement agency intends to use the information collected for purposes of a law enforcement investigation or counter intelligence investigation.³¹

Even with the PATRIOT Act correcting weaknesses in information sharing among intelligence agencies and law enforcement agencies as well as existing laws speaking directly to intelligence collection and law enforcement (NSA 1947), problems still exist. These problems are a result of two different organizations developing without examining thoroughly the actual laws. Agencies and departments did not ask the correct questions regarding what could and could not be shared. This resulted in a culture of not sharing intelligence or criminal information. So why did these cultural differences create the “wall” between intelligence and law enforcement? The wall was a direct result of intelligence not needing to reach the same level of fidelity as information that was developed to receive a criminal conviction in the judicial system. Consequently, walls developed between law enforcement and intelligence agencies. In fact Executive Order 11905, which was signed by President Ford in 1976, has a section specifically addressing what can and can't be done within law enforcement and intelligence. Section

5b provides restrictions on collection by intelligence agencies. To paraphrase the section, intelligence agencies cannot, in most cases, conduct physical surveillance on U.S. persons. Additionally, these agencies may not conduct searches of mail or look at tax returns. Intelligence agencies are very much limited to collection against foreign intelligence services and conducting counterintelligence to protect national security information. The order does try to show how intelligence and law enforcement should work by stating,

These prohibitions shall not, however, preclude: (i) cooperation between a foreign intelligence agency and appropriate law enforcement agencies for the purpose of protecting the personnel and facilities of the foreign intelligence agency or preventing espionage or other criminal activity related to foreign intelligence or counterintelligence or (ii) provision of specialized equipment or technical knowledge for use by any other Federal department or agency.³²

Unfortunately, both the intelligence and law enforcement communities focused on the prohibitions of this executive order instead of what could be shared with each other. After September 11, 2001, both Congress and the Bush administration stressed the need for law enforcement and intelligence agencies to share information about terrorists and their activities more effectively.³³ In fact, the Senate Select Committee on Intelligence observed that, “effective sharing of information between and among the various components of the government-wide effort to combat terrorists is also essential, and is presently hindered by cultural, bureaucratic, resource, training and, in some cases, legal obstacles.”³⁴

The PATRIOT Act was designed to tear these walls down. Congress asked the Department of Justice to comment on the proposed PATRIOT Act and the DOJ listed three items that they would recommend including in the act:

First, it suggested that information generated through the execution of a Title III (wiretapping) order might be shared in connection with the duties of any executive branch official. Second, it recommended a change in Rule 6(e) of the Federal Rules of Criminal Procedure that would allow disclosure of grand jury material to intelligence officials. Third, it proposed elimination of all constraints on sharing foreign intelligence information uncovered during a law enforcement investigation, mentioning by name the constraints in Rule 6(e) and Title III.³⁵ The bottom line is that the DOJ recognized the limitations and perceived limitations put on information sharing between law enforcement and intelligence organizations. By Congress enacting legislation to reduce what could and couldn't be shared, our nation would be more secure and fewer seams in our government could be exploited by our adversaries.

All three of these recommendations can be found with some modification in Section 203 of the PATRIOT Act. Finally in an effort to help intelligence agencies "follow the money", the Act also gave the Secretary of the Treasury additional authorities to combat money laundering and changed monetary limitations that banks were required to report. This sharing of "monetary information" made hiding money and transferring money harder to accomplish in the United States.

Homeland Security Act of 2002

While there were many major changes (including movement and abolishment of certain agencies enacted by this law, it directed the following:

- Requires the Secretary to: (1) establish procedures for sharing information; and (2) appoint a senior Privacy Officer to assume primary responsibility for privacy policy.
- Requires the Secretary to appoint an Officer for Civil Rights and Civil Liberties to assess information alleging abuses of civil rights, civil liberties, and racial and ethnic profiling by DHS employees and officials.
- Homeland Security Information Sharing Act - Directs the President to prescribe and implement procedures under which relevant Federal agencies: (1) share relevant and appropriate homeland security information with other Federal agencies, including DHS, and appropriate State and local personnel; (2) identify and safeguard homeland security information that is sensitive but

unclassified; and (3) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.

- Authorizes Federal investigative or law enforcement officers to share electronic, wire, and oral interception information with foreign investigative or law enforcement officers.³⁶

It is evident that the Congress was addressing the public's reaction to the PATRIOT Act and other perceptions concerning civil liberties when it passed the Homeland Security Act. The Congress addressed these issues by directing the appointment of a Civil Rights and Civil Liberties Officer within DHS. It is also evident that the Congress wanted to insure that information sharing was seen as crucial by directing the President to establish procedures to share information among all agencies. Finally, as discussed earlier in this paper, by directing the creation of a Joint Interagency Homeland Security Task Force that included military and civilian agencies, it is apparent that Congress wanted to break down real or perceived stovepipes in regard to collecting and sharing information on foreign terrorists and other non-U.S persons.

Information Sharing

Information sharing within and between the intelligence and law enforcement communities has been addressed throughout this paper. In fact, it has been pointed out that many Presidents have had to address information sharing specifically though the years and even provide guidance for information sharing in executive orders. Congress has been involved from the earliest days with the National Security Act of 1947 through the Homeland Security Act of 2002 in directing information sharing. The IC has taken the brunt of Congress' anger for "not connecting the dots". So how has enactment of the PATRIOT Act and the Homeland Security Act improved Information sharing?

In looking at articles written over the past eight years, it is clear that the change that was expected when enacting these laws has failed in many regards. Michael Moran, an MSNBC investigative reporter, interviewed numerous members of Congress, military experts and administration officials. His interviews resulted in an August 2003 article making the following point: “Nearly two years after 9/11, and contrary to the recommendations of congressional and independent panels of experts, agencies like the CIA, FBI and Defense Department are resisting reforms aimed at reducing turf battles and legal dilemmas....”³⁷ Former Senator Gary Hart, who co-chaired a homeland security study before the September 11, 2001 attacks stated in Moran’s August 2009 article, “Right now, you have bureaucratic warfare all over the place, all about turf, not about American security”.³⁸ Many “unattributed sources” described as intelligence professionals also believe that problems continue to exist, such as “the buck stops nowhere; i.e., that no single official is in charge of American collection.”³⁹ In fact, Moran contends that, “U.S. intelligence agencies remain subject to “stovepipes” – self-contained avenues of information of the kind that allowed warnings before 9/11 by FBI agents...to go unheeded.”⁴⁰ James Gilmore who co-chaired a post-9/11 study agrees and stated, “the culture of law enforcement and intelligence is not to share information. At this point, we’ve made a lot of pronouncements, but we still need to find ways to get information shared.”⁴¹ So, two years after September 11, 2001, opinion is that that not much had changed with respect to information sharing.

Congress was concerned with the problems that existed years after September 11, 2001. To address these concerns, H.R. 1: Implementing Recommendations of the 9/11 Commission Act of 2007 was sponsored by Representative Bennie Thompson and

passed by the House of Representatives in January 2007. The Senate passed a similar act in July 2007 and after differences were resolved in conference, President Bush signed the Act into law in August 2007. The introduction of this legislation and passage into law shows that problems still existed almost six years after September 11, 2001 and passage of the PATRIOT and HSA. Members of Congress and the American people were concerned that recommendations of the 9/11 Commission had not been enacted and that the DHS was not doing enough to share information vertically or horizontally.

Congress reacted to these failings by passing legislation to correct these shortcomings. In fact, this law “requires the secretary of homeland security to establish department-wide procedures by which to receive and analyze intelligence from state, local and tribal governments and the private sector.”⁴² In this Act, the Congress further directs the establishment of the Interagency Threat Assessment and Coordination Group (ITACG) to improve communication within the information sharing environment. The ITACG will exist at the National Counterterrorism Center (NCTC).⁴³

Yet, even this legislation did not produce the desired outcome. In the January 25, 2007 testimony of Charles E. Allen, Assistant Secretary of Homeland Security for Intelligence and Analysis and Chief Intelligence Officer, before the U.S. Senate Select Committee on Intelligence, Allen made the following statement: “as we move toward the implementation of the Information Sharing Environment.”⁴⁴ In other words, the United States is still are moving toward information sharing more than five years after September 11, 2001 and more than four years after Congress passed the PATRIOT Act and Homeland Security Act and President Bush signed executive orders that directed

the an information sharing environment. Twenty months later, on September 24, 2008, Allen testified before the U.S House of Representatives, Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. In this testimony, he addressed his department's policy for Internal Information Exchange and Sharing, known as the "One DHS" memorandum. The purpose of the memorandum, he stated, is, "to promote a cohesive, collaborative and unified Department-wide information sharing environment."⁴⁵ This statement only confirms that if the Secretary of the Department of Homeland Security, the department created to "share intelligence/information", has to issue an "information sharing" memorandum to his department, then significant problems with information sharing remains a problem within his organization. Additionally, it definitely raises questions about how well information sharing is occurring within the government as a whole. Recent events provide some insight into how this reluctance to sharing information continues to affect the U.S. government's ability to counter terrorism.

Recent Events: Case Studies in Information Sharing

Recent events have highlighted the concern that there continues to be lack of information sharing between law enforcement and the IC, making information sharing a critical issue. On November 5, 2009, Army Major Nidal Malik Hasan, an Army psychiatrist stationed at Ft. Hood, Texas, opened fire on fellow soldiers and civilians. In the shooting, he killed thirteen individuals and wounded twenty-nine others. As the investigation continues into the shooting, preliminary evidence suggests that Major Hasan had contact with Iman Anwar al Awlaki, a radical Yemeni cleric famous for his anti-American preaching. In fact, U.S. officials now confirm Hasan sent as many as twenty e-mails to Anwar al Awlaki. Authorities intercepted the e-mails but later deemed

them innocent or protected by the First Amendment to the Constitution.⁴⁶ Additionally, A senior government official informed ABC News that investigators found that alleged Fort Hood shooter Mital Malik Hasan had "more unexplained connections to people being tracked by the FBI" than just radical cleric Anwar al Awlaki.⁴⁷ What is more disturbing is that "finger pointing" has already started. The FBI allegedly turned over the information to the U.S. Army, but Defense Department officials denied that occurred. One military investigator on a joint terror task force with the FBI was shown the e-mails, but they were never forwarded formally senior officials at the Pentagon, and the Army did not learn of the contacts until after the shooting.⁴⁸ It appears that information sharing did not occur once again in a timely manner to prevent an incident.

The December 25, 2009 attempted bombing of a U.S. flight over Detroit is another example of the system not working properly. During a Senate hearing on January 20, 2010, U.S. counterterrorism officials affirmed that they had the first and second name of the Nigerian, Umar Farouk but failed to connect it with his father's warning. "We had a name, Umar Farouk," but analysts "didn't put that together," National Counterterrorism Center director, Michael Leiter stated.⁴⁹ Even more concerning now is that Abdul Mutallab, the alleged terrorist, stated to FBI agents that Anwar al Awlaki, the same radical cleric connected to Major Hasan, "directed him to carry out the attack."⁵⁰ U.S. counterterrorism officials have closely watched al Awlaki after finding evidence of contacts he had with three of the September 11 hijackers.⁵¹ President Obama stated, "probes revealed that U.S. analysts knew alleged attacker Umar Farouk Abdul Mutallab was an extremist and knew Al-Qaeda" and the plot was

“not the fault of a single individual or organization, but rather a systematic failure across organizations and agencies.”⁵²

Final Thoughts

The United States has made some strides, but not enough, in trying to modernize a Cold War intelligence system for the threats presented by today's non-state actors. Although the Congress and President of the United States passed and signed into law legislation intended to remedy these cold war problem, such as the PATRIOT Act, the HSA and countless others since September 11, 2001, the United States government continues to have an information sharing problem. The President, Congress and perhaps the American people believed that the new laws had changed the system and made the United States safer. However, much is left to be done as proven by Umar Farouk Abdul Mutallab alleged attempted terrorist attack on December 25, 2009. President Obama on January 5, 2010 stated the issue was, “not a failure to collect intelligence, it was a failure to integrate and understand the intelligence we had.”⁵³ Information sharing did not flow between the agencies and departments of the U.S. government. The Department of State DHS, DoD and others had pieces of this terrorist's plan but failed to ensure the information was shared. If we do not learn from our mistakes we will continue to hear the words, “intelligence failed to connect the dots.”

Endnotes

¹ Michael Warner, “The Kaiser Sows Destruction,” *Studies in Intelligence* 46, no. 1 (2002): 9.

² John Pike, “CIA History,” fas.org, <http://www.fas.org/irp/cia/ciahist.htm> (accessed January 28, 2010).

³ Ibid.

⁴ Ibid.

⁵ Gerald Ford, "Executive Order 11905: United States Foreign Intelligence Activities," Gerald R. Ford Presidential Library, <http://www.ford.utexas.edu/library/speeches/760110e.htm> (accessed November 26, 2009).

⁶ Ibid.

⁷ John McConnell, "United States Intelligence Community Information Sharing Strategy," DNI.GOV, http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf (accessed November 28, 2009).

⁸ Thomas Kean and Lee Hamilton, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton and Company, 2004), 403, <http://govinfo.library.unt.edu/911/report/911Report.pdf> (accessed December 1, 2009).

⁹ Ibid., 425.

¹⁰ Ibid., 48.

¹¹ Ibid., 60.

¹² Ibid., 68.

¹³ William J. Clinton, *A National Security Strategy of Engagement and Enlargement* (Washington, D.C.: The White House, February 1996), 19-20.

¹⁴ William J. Clinton, *A National Security Strategy for a New Century* (Washington, D.C.: The White House, May 1997), 13.

¹⁵ *Encyclopedia Britannica.*, 2010th ed., s.v. "USS Cole Attack," <http://www.britannica.com/EBchecked/topic/734635/USS-Cole-attack> (accessed December 5, 2009).

¹⁶ I Thomas Kean and Lee Hamilton, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton and Company, 2004), 218, <http://govinfo.library.unt.edu/911/report/911Report.pdf> (accessed December 1, 2009).

¹⁷ Elizabeth Borja, "Brief Documentary History of the Department of Homeland Security 2001-2008," dhs.gov, http://www.dhs.gov/xlibrary/assets/brief_documentary_history_of_dhs_2001_2008.pdf (accessed December 31, 2009).

¹⁸ Ibid

¹⁹ Ibid

²⁰ George W. Bush, *The Department of Homeland Security* (Washington, D.C.: The White House, June 2002), 1.

²¹ Ibid

²² Elizabeth Borja, "Brief Documentary History of the Department of Homeland Security 2001-2008," dhs.gov, http://www.dhs.gov/xlibrary/assets/brief_documentary_history_of_dhs_2001_2008.pdf (accessed December 31, 2009), 5.

²³ Ibid, 6.

²⁴ Charles Doyle, "The USA PATRIOT Act: A Sketch," fpc.state.gov, <http://fpc.state.gov/documents/organization/10092.pdf> (accessed January 2, 2010), 1.

²⁵ Ibid.

²⁶ Ibid, 2.

²⁷ Ibid, 6.

²⁸ Ibid, 5.

²⁹ Ibid, 8.

³⁰ Ibid, 14.

³¹ Harry Truman, "National Security Act of 1947," intelligence.gov, http://www.intelligence.gov/0-natsecact_1947.shtml (accessed December 7, 2009), 14.

³² Gerald Ford, "Executive Order 11905: United States Foreign Intelligence Activities," Gerald R. Ford Presidential Library, <http://www.ford.utexas.edu/library/speeches/760110e.htm> (accessed November 26, 2009), 14.

³³ Charles Doyle, "The USA PATRIOT Act: A Sketch," fpc.state.gov, <http://fpc.state.gov/documents/organization/10092.pdf> (accessed January 2, 2010), 19.

³⁴ Ibid.

³⁵ Ibid, 19-20.

³⁶ Congress, "PUBLIC LAW 107-296—NOV. 25, 2002," dhs.gov, http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (accessed December 7, 2009).

³⁷ Michael Moran, "Is the U.S. vulnerable?'Bureaucratic warfare' foils reform efforts," msnbc.com, <http://www.msnbc.msn.com/id/3071399/print/1/displaymode/1098/> (accessed December 17, 2009), 1.

³⁸ Ibid.

³⁹ Ibid

⁴⁰ Ibid, 2.

⁴¹ Michael Moran, "Tilting at 'stovepipes?," msnbc.com, <http://www.msnbc.msn.com/id/3071393/print/1/displaymode/1098/> (accessed December 17, 2009).

⁴² Mike Leiter, "Eight Years After 9/11: Confronting the Terrorist Threat to the Homeland," Congressional Record (September 30, 2009)

⁴³ Ibid

⁴⁴ Charles E. Allen, "Intelligence Reform and Homeland Security Intelligence," Congressional Record (January 25, 2007)

⁴⁵ Ibid.

⁴⁶ Martha Raddatz, "Senior Official: More Hasan Ties to People Under Investigation by FBI," abcnews.com, <http://abcnews.go.com/Blotter/official-nidal-hasan-unexplained-connections/story?id=9048590> (accessed January 7, 2010).

⁴⁷ Ibid.

⁴⁸ Ibid.

⁴⁹ Paul Ohia, "Abdul Mutallab: US Intelligence Failed to Act Despite Warning," This Day Online, http://www.thisdayonline.com/nview.php?id=164685&printer_friendly+1 (accessed January 26, 2010).

⁵⁰ CBS/ AP, "Abdul Mutallab: Cleric Told Me to Bomb Jet," cbsnews.com, <http://www.cbsnews.com/stories/2010/02/04/national/main6174780.shtml> (accessed February 5, 2010).

⁵¹ Ibid

⁵² Stephen Collinson, "Obama on Mutallab U.S. intelligence flaws: 'buck stops with me'," usafricaonline, <http://www.usafricaonline.com/obama-on-mutallab-u-s-intelligence-flaws-buck-stops-with-me> (accessed February 5, 2010).

⁵³ Barrack H. Obama, "Remarks by the President on Security Reviews, Washington, D.C., Grand Foyer, The White House, January 5, 2010.