Strategy Research Project

ASSESSING THE EFFECTIVENESS OF POST-9/11 INTELLIGENCE INFORMATION SHARING

BY

MS. HEATHER N. FREEDMAN
Defense Intelligence Agency

USAWC CLASS OF 2010

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

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 MAR 2010		

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Assessing the Effectiveness of Post-9/11 Intelligence Information Sharing	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Heather Freedman	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220	
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	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**30**	

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.

USAWC STRATEGY RESEARCH PROJECT

ASSESSING THE EFFECTIVENESS OF POST-9/11 INTELLIGENCE INFORMATION SHARING

by

Ms. Heather N. Freedman
Defense Intelligence Agency

Mr. Daniel Coulter
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.

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

ABSTRACT

AUTHOR: Ms. Heather N. Freedman

TITLE: Assessing the Effectiveness of Post-9/11 Intelligence Information Sharing

FORMAT: Strategy Research Project

DATE: 23 March 2010 WORD COUNT: 5,677 PAGES: 30

KEY TERMS: Intelligence Reform, Intelligence Sharing, 9/11 Commission, Homeland Security, National Security, Director of National Intelligence (DNI), Intelligence Community (IC), Information Sharing, Intelligence Reform and Terrorism Prevention Act (IRPTA)

CLASSIFICATION: Unclassified

In the wake of the terrorist attacks of 11 September 2001, the 9/11 Commission determined that intelligence related to the attack was not shared across the Intelligence Community (IC), and especially between the Central Intelligence Agency (CIA) and the Federal Bureau of Investigations (FBI). Specifically the Commission faulted the IC for being parochial, secretive, and delinquent in sharing important intelligence. Despite the 9/11 Commission's recommendations, including the creation of the Office of the Director of National Intelligence (ODNI), and institutions such as the National Counterterrorism Center (NCTC), the parochialism continues and information sharing across the IC remains a critical problem. As the 2009 Christmas Day failed bombing of the Northwest Flight reminded us, the lack of IC sharing can have tragic consequences and that it still remains a work in progress.

ASSESSING THE EFFECTIVENESS OF POST-9/11 INTELLIGENCE INFORMATION SHARING

> The need to share information became an imperative to protect our nation in the aftermath of the 9/11 attacks on our homeland.[1]
>
> —2008 United States Intelligence Community Information Sharing Strategy

Eight years after the catastrophic terrorist attacks of September 11, 2001 (9/11), the Intelligence Community (IC) continues to function as a conglomerate of disparate institutions, hesitant to share information and "stovepiping" intelligence across its 16 components. The lack of information sharing across the IC and law enforcement was identified as one of the key failures leading to 9/11, and since al-Qaeda remains determined to attack the U.S. homeland, it is imperative that the IC transform in accordance with the critical information sharing measures established in the post-9/11 legislative reforms to thwart future terrorist attacks against American interests – both in the United States and abroad.

Background

The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 demanded critical changes to the IC to prevent future terrorist attacks. IRTPA was based on the Commission finding that the greatest impediment to thwarting the 9/11 attack was a lack of, and resistance to, information sharing across the IC. The Commission decided that a new, government-wide approach to information sharing was needed to ensure that terrorism information is shared between Federal, State, local, tribal, and private sector entities. It urged the President to create an Information Sharing Environment (ISE) with a Program Manager (PM-ISE) to facilitate information sharing across this vast enterprise, which comprises a wide array of institutional

cultures.[2] To implement this, IRPTA created the position of the Director of National Intelligence (DNI) to serve as the head of the Intelligence Community, with budgetary authorities (limited in part due to political considerations), to transform and lead the Intelligence Community into the future. The ISE was established as a component of the DNI in 2007.[3]

Since the IRPTA, a number of reforms have strengthened the U.S. Intelligence Community and its information sharing capabilities. The DNI is now fully operational, as is the PM-ISE, the National Counterterrorism Center (NCTC), the National Counterproliferation Center (NCPC), and the National Counterintelligence Executive (NCIX), and most Congressionally-mandated reporting requirements and timelines have been met.[4] However, while many qualitative milestones can be cited as evidence of intelligence reforms and the improvement of information sharing, there are very few quantitative or qualitative metrics to indicate the impact of these reforms in ensuring robust information sharing across the IC.

Some aspects of the post-9/11 U.S. Government (USG) reforms remain a work in progress, such as the creation of the Department of Homeland Security (DHS). In fact, both the 2007 National Strategy for Information Sharing and the IC's 2008 Information Sharing Strategy cite a number of completed post-9/11 reforms but also note the continuing challenges that plague the successful implementation of the transformation required by IRPTA to ensure that terrorism information is shared across the USG, as well as with state, local, tribal, and private sector partners. Such a transformation would enhance our ability to successfully thwart a terrorist attack against U.S. interests. The IC Information Sharing Strategy noted that progress in information sharing to date is

commendable but that these activities are the tip of the iceberg and continued focus on "accelerating information sharing" is needed.[5] The strategy was further reiterated by the Director of NCTC in his 2008 Testimony before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment:

> Information sharing is among NCTC's and our Intelligence Community partners' highest priorities, and significant progress has been achieved. Challenges to information sharing remain as we seek the proper balance between and among a host of technical, legal, security and privacy issues.[6]

Many reporters, government personnel, and academics, however, are much sharper in their critique of the status of successful intelligence reforms to date. A Washington Post article dated October 20, 2009 indicates that the Intelligence Community "remains a dysfunctional family with no one firmly in charge."[7] As late as December of 2009, DNI Blair stated the following in the Washington Post:

> …the task of reinventing our intelligence structure and integrating the capabilities, cultures, and information technologies of 16 diverse intelligence agencies is massive, and it is incomplete. Problems persist in our technologies, business practices, and mind-sets. I have no illusions about how challenging they will be to overcome. But there is an ocean of difference between difficult and impossible.[8]

The 16 agencies comprising the IC currently lack the trust required to operate as needed to keep the U.S. safe and to move from the pre-9/11 status quo of "need-to-know" to the post-9/11 intelligence reform status of "responsibility-to-provide," which is reality only in terms of its rhetoric.[9] While it is true that "effective partnerships require a shared vision, shared goals, and shared trust in meeting agreed-upon (shared) responsibilities," the IC still has to learn to work in this manner.[10] As Senator John Kerry (D) from Massachusetts contends:

> …isolating information vital to protecting Americans from terrorists within a single agency sacrifices the rigorous, multidisciplinary analysis required to improve our odds of stopping the next attack. When one agency sits on intelligence essential to another, whether out of ignorance or reluctance to share, the chance of system failure is astronomic. Despite years of rhetoric, some people still don't grasp that we are one team locked in a singular fight.[11]

9/11 Commission, IRPTA, and Intelligence Reform

The National Commission on Terrorist Attacks Upon the United States performed an in-depth review of the situation leading to the terror attacks on September 11, 2001.[12] In its report, the Commission cited intelligence, law enforcement, and congressional oversight failings as the reasons why al-Qaida was able to conduct the attacks. The report cited "…the human or systemic resistance to sharing information as the biggest impediment…to a greater likelihood of connecting the dots…," and called for a sweeping transformation of the U.S. government, including a number of changes to the IC.[13] Specific changes to the IC include the following adjustments to ensure the sharing of terrorism intelligence:

- Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge, and
- The President should coordinate the resolution of the legal, policy, and technical issues across agencies to create a trusted information network.[14]

From the 9/11 Commission's recommendations emerged the impetus for the establishment of a National Intelligence Director (NID), which later became the Director of National Intelligence (DNI), and a National Counterterrorism Center (NCTC), both of which would remove the CIA from its historical IC leadership and management role.[15] The 9/11 Commission Report also called for the creation of an Information Sharing Environment (ISE) to facilitate the sharing of terrorism information among all appropriate

federal, state, local, tribal, and private sector entities, and established an annual requirement for the ISE to report to Congress on the status of information sharing across the federal government.[16] Despite the powerful impact of the 9/11 attack, the White House was concerned about giving the DNI too much power, and did not want to make too many sweeping changes. Therefore, the bill establishing the DNI includes considerable ambiguity to ensure the intelligence agencies retain their "statutory responsibilities," while the DNI shares budgetary authority with the Secretary of Defense.[17]

The Role of the Director of National Intelligence

The IRTPA established the DNI as the "principal authority to ensure maximum availability of and access to intelligence information within the IC."[18] This task is, at best, overwhelming, as the DNI must change the culture of "agencies whose willingness to share closely guarded secrets is notoriously poor and whose suspicion of one another is strong."[19] From its inception, the ODNI has faced disputes "over its size, mission and authority, but forcing information-sharing and enabling the NCTC's best analysts to do their work should not be subject to dispute."[20] The DNI has several critical missions pertaining to information sharing:

- Ensure that timely and objective national intelligence is provided to the President, the heads of departments and agencies of the executive branch; the Chairman of the Joint Chiefs of Staff and senior military commanders; and the Congress
- Ensure maximum availability of and access to intelligence information within the Intelligence Community
- Establish objectives and priorities for collection, analysis, production, and dissemination of national intelligence
- Ensure the most accurate analysis of intelligence is derived from all sources to support national security needs.[21]

Despite the many issues before the DNI, the DNI has endeavored to move the IC from its pre-9/11 parochial nature towards a more integrated community of agencies with a shared sense of purpose. In 2007, then DNI McConnell indicated that the IC had made improvements in information sharing, but that "we have much work yet to do…we still need a high degree of coordination and interaction to improve our collective intelligence capability."[22]

In an effort to improve information sharing in the IC, the DNI announced, in March 2007, "the creation of a new Information Sharing Steering Committee (ISSC), in order to move the Intelligence Community…more to a 'responsibility to provide.'"[23] The DNI established the ISSC to ensure that his office has a single point of contact for policy, budget, process, and technology issues relating to information sharing.[24] The DNI's website, in October of 2009, indicated that the Intelligence Community Information Sharing Executive (IC-ISE) facilitates the "development of standards, policies, and collaborative processes to guide the Community's transition from its historic culture of 'need to know' to one of a 'responsibility to provide'" and provides a point for resolution for intelligence information sharing issues.[25] Additionally, the 2008 IC Information Sharing Strategy indicates that "accelerating and improving Intelligence Community information sharing" is one of the DNI's top priorities.[26] However, the very fact that the 2009 failed Christmas Day aviation plot was attributed by the Chairs of the 9/11 Commission as a failure to share information demonstrates that the DNI's aspirations in this area remain unmet met nearly two years later.[27] Therefore, the question of the DNI's authorities and position must be addressed if information sharing

is to be achieved across the Federal Government as well as with state, local, tribal, and other partners.

Lack of Progress in Information Sharing

In a 2008 employee climate survey, 32% of IC employees responded that it was not easy to collaborate with colleagues in other IC agencies on work-related matters.[28] The same survey results noted that 54% of employees across the IC believe in intelligence transformation, that information sharing and collaboration across agencies is critical, and that these goalposts remain difficult to achieve.[29] A 2008 RAND Corporation study determined the same results, as the all-source analysts it interviewed expressed the most concern regarding data sharing and data ownership in the IC.[30]

There are no specific, tangible metrics regarding the progress made to date to ensure terrorism-related information is shared across the IC. The National Strategy for Information Sharing, the Intelligence Community's Information Sharing Strategy, Congressional Testimony from the Director of NCTC, and NCTC's Information Sharing Progress Report of September 2006, all state the need for increased and continual transformation across the IC while citing some improvements in information sharing.[31] However, not one of these documents provides specific metrics from the organizations created post-9/11, or other IC organizations, regarding their ability to secure terrorism information for various elements of the USG to perform their combating terrorism roles and missions. Without metrics regarding intelligence information sharing successes and failures being provided by the Defense Intelligence Unit (DIU)[32] and Interagency Threat Assessment and Coordination Group (ITACG)[33] at NCTC, these documents do not portray the full picture of the progress, or lack thereof, in improving information sharing across the USG and with state, local, and tribal (SLT) partners. In addition to a

lack of metrics charting the progress to date on information sharing across the USG, it appears that the DNI's basic authority as the head of the intelligence community is in question, casting doubt on the USG's ability to achieve any true advancements in information sharing.[34]

In its November 2009 Office of Inspector General (OIG) report on Information Sharing at the National Operations Center (NOC), the Department of Homeland Security's (DHS') OIG reported on the organizational obstacles within DHS that are impacting information sharing.[35] As indicated in the report:

> …the Homeland Security Act of 2002 and the Post Katrina Emergency Management Reform Act of 2006 require the NOC to ensure that critical information is disseminated to key DHS and other government decision makers. However, no statutory authorities require components to forward information to the NOC. For example, DHS components routinely provide information to DHS' Secretary without first informing the NOC. These actions prevent the NOC from fully satisfying its information sharing obligations and could affect its ability to maintain situational awareness…during a…act of terrorism.[36]

The report also cites administrative issues that currently hamper homeland security-related information sharing. For example, operations and law enforcement personnel often do not receive high-level security clearances, making it difficult for them to interact with the NOC's intelligence personnel. This situation results in "…tense relationships between the two sides…negatively affect[ing] information sharing."[37]

In October 2008, the DNI announced a new initiative designed to increase information sharing. The PM-ISE, in conjunction with the Office of Personnel Management, released on September 24, 2008 the guidance for *Inclusion of Information Sharing Performance Evaluation Element in Employee Performance Appraisals* (ISE-G-105), in support of a 2005 Administration request for all federal agencies with intelligence or terrorism information to "add a performance evaluation

element on information sharing" to annual personnel appraisals.[38] It wasn't until 2008 (for fiscal year 2009) that the PM-ISE acted on this three year-old Administration guidance, and PM-ISE Ambassador Thomas McNamara noted that this was a "critical step toward ensuring that information sharing becomes ingrained in the way the federal government operates."[39] Ambassador McNamara indicated that the new policy should assist in removing "cultural barriers and create incentives to encourage collaboration that is so critical to our counterterrorism efforts."[40]

In his January 2010 Congressional Testimony DNI Blair also references the implementation of the Intelligence Information Sharing Dispute Resolution process, which was established in November 2007 to provide an avenue for those requesting information from originating agencies, but were denied access, to gain resolution on these issues from the DNI.[41] In his January 2009 notice to the IC workforce on the progress of this new process, DNI McConnell noted that most of the information sharing cases brought before the DNI:

> …are not simply a matter of providing disputed information to a requester…many have required changes to policy, improved technology…and greater understanding of mission needs. Some cases revealed issues that were actually systemic and Community-wide.[42]

It would appear that the creation of the Resolution mechanism six years after 9/11, paired with the DNI's 2009 explanation of the types of issues brought forward for resolution, prove that the IC remains dysfunctional and some IC agencies remain unwilling to share information. Despite DNI Blair's 2010 messages regarding the progress of information sharing in the IC, it is unlikely that all the information sharing issues have, within one year, been resolved. In fact, DNI Blair, in a January 2010 message to the IC workforce, referenced that he was tasked in the aftermath of the

Christmas Day failed attack, to oversee and manage "distributing intelligence reports more quickly and widely, especially those suggesting specific threats against the U.S."[43] If intelligence sharing within the IC was occurring without issue, and the barriers to information sharing that existed on 9/11 eradicated, the DNI would not have been tasked with this critical mission in 2010.

Obstacles to Information Sharing

Nine years after 9/11, "cultural, bureaucratic, and technological barriers to the sharing of information among federal agencies" continue to hamper the sharing of terrorism intelligence.[44] As the 2009 terrorist incidents at Fort Hood and Detroit demonstrate, there's still work to be done to ensure the safety of U.S. interests worldwide.[45] Information sharing, "including the two-way flow of information and analysis, and cooperation between law enforcement and intelligence entities, remains problematic."[46] Former 9/11 Commission co-chairs Lee Hamilton and Thomas Kean believe that we need to review situations such as those in Michigan and Texas in order to "improve and refine our processes, analysis, and information-sharing responsibilities."[47]

Turf Battles. Despite the expectation that the creation of the DNI would bring the 16 members of the IC together to function as one community, internal power struggles plague the ODNI in its quest to assert its authority over the IC. The Christmas Day 2009 attempted terror attack intelligence failures "…appear to have revived resentments within the intelligence community, particularly between the CIA and the Director of National Intelligence."[48] This refers to an ongoing "turf battle" between CIA Director Leon Panetta and DNI Blair, wherein the DNI issued an Intelligence Community Directive (ICD) in May 2009 regarding his ability to determine which intelligence agency

would serve as the DNI's Representative to foreign partners and international organizations. Although the ICD stated that CIA officers would most likely continue to serve in this capacity, the DNI could, "in rare circumstances," name another IC element's representative for this position.[49] This issue was resolved, six months later, by the National Security Adviser, General James L. Jones, USMC (Ret). In lieu of supporting the designated head of the IC in his organizational role, General (Ret) Jones undermined the DNI's authority by siding with the CIA and determining that CIA officers would continue to serve as the DNI Representative.[50] A quote from former CIA Director Porter J. Goss, who has a particular bias on this issue given his prior position as the CIA Director, illuminates the current CIA/DNI turf battles regarding information sharing issues:

> Everything that happened on December 25 is exactly the stuff that's not supposed to happen anymore because of the new structure created with the DNI. What we're now seeing is that the Office of the Director of National Intelligence has not made one iota of improvement.[51]

Organizational Culture. In a 2010 Op-Ed piece in the Washington Post, DNI Blair stated:

> Our mission is a fully integrated intelligence community, and there is no turning back. My most urgent priorities are to permanently instill this new culture…to build a generation of intelligence leaders for whom this culture is business as usual.[52]

DNI Blair referenced, in 2010 Congressional Testimony, Intelligence Community Directive (ICD) 501 on the "Discovery and Dissemination or Retrieval of Information" as evidence of the IC's progress in policies supporting information sharing.[53] While ICD 501 mandates the sharing of intelligence information, this policy only became effective as of January 21, 2009 when it was signed by DNI Blair. ICD 501 has, as one of its three overall objectives, the requirement to "foster an enduring culture of responsible

sharing and collaboration within an integrated IC."[54] It took eight years after 9/11 for the DNI to create a policy directive regarding information sharing for the IC.[55] Given the timing of this ICD, it's no surprise that, for example, the CIA failed to share a biography it created on the failed Christmas Day 2009 attacker with all 16 members of the IC.[56]

Another example of organizational culture impacting information sharing is the resistance to sharing with non-Federal entities. The Interagency Threat Assessment and Coordination Group (ITACG) was established to "improve the sharing of information with SLT and private sector officials within the scope of the Information Sharing Environment (ISE)."[57] The ITACG resides at the National Counterterrorism Center, and is staffed by federal and law enforcement officials. The ITACG reviews the various databases available at NCTC to find finished intelligence related to homeland security that should be provided to SLT partners, and requests that the originators release these reports to SLT partners. The ITACG has performed its mission well under difficult circumstances, ensuring "the availability of over 350 intelligence products to SLTP consumers."[58] While it is clear that the ITACG provides valuable insight to SLT partners:

> Its value will be further realized when DHS and FBI more fully incorporate the functionality it offers into their production and dissemination processes, and when consideration of SLT stakeholders becomes a normal part of IC business. Senior officials from DHS, FBI, NCTC, and ODNI have continued to make progress and are working to accomplish this.[59]

Another element of the National Counterterrorism Center (NCTC) also serves to ensure that information coming into NCTC is shared outside of the Center – with the Department of Defense (DoD). The Defense Intelligence Unit (DIU), created in 2004, resides in the NCTC Operations Center to ensure that intelligence provided to the

NCTC is also received by DoD for force protection, support to operations, and support to DoD policymakers.[60] If the IC was sharing all terrorism intelligence with all 16 members of the IC and others who require such intelligence, then organizations such as the ITACG and DIU would no longer need to exist. Their very existence is a testimony to the fact that information sharing has not progressed to the point where it needs to be post-9/11, with all IC agencies receiving all intelligence information.[61]

Technology and Knowledge Management. Despite the creation of the DNI, there still is no single computer network, terrorism database, and e-mail system used by the members of the IC. Instead, each intelligence agency maintains its own databases and thereby ensures that it remains difficult to warn of, or thwart, a terrorist attack.[62] DNI Blair touted the availability of more than 30 networks with over 80 different databases at NCTC, which should leave no doubt as to why it was so difficult to "connect the dots" regarding the threat leading to the failed Christmas Day 2009 terror attack.[63]

While information sharing cannot be relegated to only an issue of technical information sharing aspects, including e-mail and knowledge management systems containing databases, the technology issues related to information sharing cannot be overlooked as they contribute to this ongoing issue. A multitude of databases still exist, various law enforcement and intelligence computer systems cannot communicate, and there are a plethora of e-mail systems used throughout the combating terrorism community, virtually ensuring that all parties in this national security arena cannot communicate effectively. While national security officials cannot discount the value of the co-location of personnel from across the national security arena while providing those personnel with unprecedented information access, the reality of this myriad of

information systems renders the job of an NCTC analyst virtually impossible. One simply cannot effectively and consistently "connect the dots" when the dots reside over more than 30 different networks. Nearly nine years after 9/11, it is almost unfathomable that the national security apparatus of the United States faces this issue despite significant government reforms. In his January 2010 Congressional Testimony, DNI Blair stated that he was tasked by President Obama with:

> …accelerating information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence.[64]

Law Enforcement Versus Intelligence. Former FBI Assistant Director James Kallstrom summed up the law enforcement/intelligence divide in a 2010 statement:

> A painful lesson learned from 9/11 is that the bifurcation of our intelligence and law enforcement competencies leads to "stovepiping" of information - a formula for disaster.[65]

What is clear today is that the FBI remains a "gun culture," while being dual-hatted as both an intelligence and a law enforcement agency. The FBI's primary function, and the one that is rewarded by a long career, is that of its Special Agents – the intelligence officials in the FBI remain second class citizens, as "professional support staff" alongside auto mechanics and janitors.[66] In fact, the January 20, 2010 Congressional Testimony of FBI Director Robert S. Mueller before the Senate Committee on the Judiciary proves a startling example of the FBI's continued focus on its law enforcement and investigations role, and the neglect of its intelligence role.[67] In his testimony, Mueller states that the FBI has undergone "unprecedented transformation" since 9/11 and indicates that at FBI information is shared "by rule and withheld by exception."[68] He also provides a laundry list of examples of arrests, charges, and investigations by the

FBI, nine in total, over the course of the past year, and then mentions that intelligence provided to the FBI in support of these investigations is invaluable. However, nowhere in this discussion does he mention the counterterrorism intelligence the FBI collected and disseminated to federal, state, and local partners in the course of these investigations – because, as a matter of course, intelligence information collected by the FBI in the conduct of its terror investigations is considered "evidence" and not "intelligence," and therefore is not shared with the intelligence community.[69] In 2001, for example, the FBI produced no intelligence reports. From 2001 to 2004, the FBI produced 2,648 intelligence reports, or roughly only one report per special agent over a 36- month timeframe.[70]

FBI Director Mueller, in his 2010 testimony, admits his agency's failure to integrate its investigations with its intelligence functions when he discusses the establishment of FBI's Strategic Execution Team (SET), which was tasked with assessing the Bureau's intelligence program. The SET provided multiple recommendations for "accelerating the integration of our intelligence and investigative work" and highlighted the seams that exist as the criminal and counterterrorism elements within the FBI do not work in tandem.[71] The intelligence components in the FBI Field Offices were restructured and a focus has been placed on developing a national collection plan and other basic tenets already long in use by the other members of the IC, and coordinated under the DNI's National Intelligence Coordination Center (NIC-C) for the collection of intelligence, thereby demonstrating just how far FBI remains behind the curve with regard to its required intelligence collection and dissemination functions.[72] The FBI also is working toward:

> …ensuring that intelligence from our field offices is integrated and shared with those who need it at FBI Headquarters and in the larger Intelligence Community.[73]

To anyone outside the U.S. national security community, such statements made nearly 10 years after 9/11 and the Congressionally-mandated reforms to the FBI and the IC were put into place, must have raised the question as to why these reforms are not complete. It also begs the question of why the FBI is still referring to "need to know" when it ought to be referring to "responsibility to provide."[74] Further, a 2006 Presidential Report disclosed that the United States must "continue to improve law enforcement capability, including greater and more effective collection and reporting of intelligence."[75]

It is clear that the sharing of terrorism information remains a daunting task nearly nine years after the attacks on 9/11. To ensure that terrorism information is shared across the USG and elsewhere, a number of reinforcing policy changes are recommended, to include: requiring the provision of information sharing metrics, providing White House support to the DNI, requiring IC and SLT partners to complete information sharing surveys, and increasing congressional oversight of intelligence.

Policy Recommendations

Information Sharing Metrics. In order to secure the United States from terror attacks, the President should require all elements of the DNI, to include the PM-ISE, NCTC, and all sixteen members of the IC, to provide metrics to support stated progress (or lack thereof) in accordance with the guidelines established by the Presidential Memorandum to the Heads of Executive Departments and Agencies of 16 December 2005.[76] The Memorandum required the ISE to develop common standards to maximize the sharing of terrorism information within the IC, establish a common framework for information sharing responsibilities, improve on the sharing of Sensitive but Unclassified

(SBU) information, develop recommendations to achieve improved information sharing with foreign partners, and develop guidelines to protect the rights of Americans.[77]

The PM-ISE produces an annual report to Congress each summer. The metrics should be provided in this document, and they should continue to be made available on the PM-ISE website for viewing by all interested parties. A specific example of the gaps remaining in the current document, which lacks metrics regarding success in obtaining the release of sensitive information, occurs under "Goal 4: Institutionalize Sharing, Issuing Common Information Sharing Standards."[78] The report provides information on the progress made by the PM-ISE, but fails to produce the data to indicate success in compliance with the new and revised standards.[79] The report also fails to describe the specific information sharing progress that occurred based on the establishment of these standards.

White House Support. The DNI should be given the ability to serve in the role allocated to him by the post-9/11 legislation establishing the ODNI. That is, he truly must become the leader of the IC and not just a mere figurehead.[80] The President must "be very clear about who is in charge of the intelligence community, where final authority lies in regard to budget and personnel matters."[81] To do so, the DNI must be part of the chain-of-command, serving in the role of supervisor of the heads of the 16 elements and agencies comprising the IC, in conjunction with the Secretary of Defense where applicable. This change would provide him with the level of authority appropriate and required to discipline, and dismiss, the heads of the 16 elements of the IC for failure to perform their mission.

There is no better example of the issue of a lack of White House support for the DNI than the 2009 and 2010 press reporting regarding the power struggle between the DNI and the CIA Director. While this issue played out openly in the press, and even was acknowledged in the press by members of Congress, no action was taken by the Administration to remove CIA Director Panetta from his position, nor was the Administration cited as having supported DNI Blair or reprimanding CIA Director Panetta for his insubordination. Instead, the press reporting indicated that the National Security Advisor backed the CIA Director instead of his boss, the DNI. Immediate dismissal of Director Panetta, paired with a public statement by the President of his support for DNI Blair, would send a very clear signal to the heads of the agencies and elements of the IC that the DNI is in charge and his demands must be heeded. Such a move could prove to be the most significant catalyst yet in improving information sharing across the IC, as IC members quickly would realize that they must accept and implement the DNI's policies, including those regarding information sharing.

Information Sharing Surveys. The President should mandate that all those falling under the PM-ISE, to include federal, state, local, and tribal entities, complete an extensive survey to provide visibility on the most significant information sharing issues as perceived by those with a combating terrorism mission – not reflecting a "good news story" they want to portray, but illuminating the true reality of the status of information sharing today. The PM-ISE should create the survey, which should be an online tool providing the ability to explain the issues facing the respondents. The online tool should allow each respondent to save the completed survey to ensure that their results are included in the output provided to the National Security Staff (NSS). The same results

supplied to the NSS should also be given to each respondent to ensure accuracy, accountability, and inclusion of all perspectives.

Although the ODNI currently, and often, conducts surveys of the IC, the results are for, and at the request of, the ODNI primarily for internal use. The use of the data remains unclear, and there is little evidence to indicate that the results of these surveys are used to ensure improved information sharing across the IC. One method to guarantee the proper use of this data would be to ensure the ODNI, and by extension the rest of the IC, remains under strict scrutiny by both Congress and the National Security Staff. Another method to ensure action is taken in accordance with survey results would be to make these performance measures public. As the 9/11 Commission indicated:

> The American people are entitled to see some standards for performance so they can judge, with the help of their elected representatives, whether the objectives are being met.[82]

Increased Congressional Oversight. Lee Hamilton and Thomas Kean currently are conducting a review of the IRPTA and the effectiveness of the ODNI. In the course of their review, they determined that strengthening the ODNI requires "sustained support from the White House and oversight from Congress."[83] According to the Government Accountability Office's Comptroller General, David Walker:

> Congress has an important role to play – in both its legislative and oversight capacities – in establishing, monitoring, and maintaining progress to attain the goals envisioned by government transformation and reorganization efforts. However, as the 9/11 Commission has noted, past oversight efforts in the intelligence area have been wholly inadequate.[84]

In 2004 Walker advocated not for focusing on reorganization of the U.S. Government post-9/11, but rather being concerned about results or outcomes. Congress should embrace this goal-oriented, measures-based approach for its

intelligence oversight mission.[85] It's not a matter of whether or not we have a DNI, but rather how effective the ODNI is as the organization bringing together all U.S. intelligence capabilities to ensure information sharing and keep our nation, and its interests worldwide, safe from terror attacks.

Conclusion

Nine years after 9/11 is long enough to wait for real transformation of the information sharing environment. As the many initiatives put forth to date truly have not transformed the IC into a cohesive whole, it is imperative that the White House and Congress demonstrate leadership to transform the IC into a community that shares terrorism-related information on a routine and systematic basis. It is only with White House and Congressional leadership that intelligence reform will truly take hold and ensure that terrorism information is shared across the USG, and with state, local, tribal, and private sector entities.

Despite the criticism some of these actions might face, these options must be implemented in order to stave off another catastrophic attack on U.S. soil. Failure to implement the changes envisioned by the post-9/11 intelligence reform legislation is the equivalent of pronouncing a death sentence for hundreds, or even thousands of Americans. The continuing failure to secure information sharing across the USG raises the odds of another terrorist attack happening on U.S. soil – a legacy the current Administration and the Congress surely wish to avoid.

Endnotes

[1] Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy* (Washington, DC: Office of the Director of National Intelligence, February 2008), 3.

[2] *Intelligence Reform and Prevention of Terrorism Act (IRPTA)*, Public Law 108–458, 101st Cong. (December 17, 2004), Section 1016, 29.

[3] Office of the Director of National Intelligence, "Mission Support Activities for the IC Fact Sheet," http://www.dni.gov/aboutODNI/content/ODNI_Org_Chart_2010.pdf (accessed February 1, 2010).

[4] Ibid.

[5] Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy*, 3.

[6] Michael E. Leiter, "Statement for the Record of The Honorable Michael E. Leiter Director, National Counterterrorism Center on Information Sharing with State, Local, and Tribal Authorities before the House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment", September 24, 2008, http://www.nctc.gov/press_room/speeches/sfr-20080924.pdf (accessed 20 January 2010).

[7] Amy Zegart, "Our Clueless Intelligence System," *The Washington Post,* July 8, 2007, B1.

[8] Dennis C. Blair, "Strengthening our nation's front line defense: Reinventing our Intelligence structure is a massive challenge – but we're making real progress," *The Washington Post*, December 18, 2009, A31.

[9] Office of the Director of National Intelligence. *Intelligence Community Directive Number 501 – Discovery and Dissemination or Retrieval of Information Within the Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, January 2009).

[10] Government Accountability Office, *David M. Walker, Comptroller General of the United States. Testimony before the Committee on Government Reform, U.S. House of Representatives. "9/11 Commission Report – Reorganization, Transformation, and Information Sharing,"* (Washington, DC: Government Accountability Office, August 2004), 23.

[11] John F. Kerry, "Terrorism Fight Requires Intelligence Accountability," *Boston Globe*, January 9, 2010.

[12] Lee Hamilton, Thomas Kean et al., *Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC: The 9/11 Commission, 2004), http://www.gpoaccess.gov/911/pdf/fullreport.pdf (accessed January 17, 2010).

[13] Ibid, 434.

[14] Ibid, 436.

[15] Government Accountability Office, *David M. Walker, Comptroller General*, *2.*

[16] Program Manager-Information Sharing Environment, *PM-ISE Information Sharing Environment, Progress and Plans Annual Report to Congress*, June 2009, http://www.ise.gov/docs/reports/ISE_2009-Annual-Report_FINAL_2009-06-30.pdf (accessed 15 January 2010).

[17] Daniel Eisenberg, "Bush's New Intelligence Czar," *Time*, February 28, 2005, 33.

[18] Office of the Director of National Intelligence, Intelligence Community Information Sharing Executive, *Intelligence Community Information Sharing Facilitation and Resolution Annual Report* (Washington, DC: Office of the Director of National Intelligence, December 19, 2008), 1.

[19] Eisenberg, "Bush's New Intelligence Czar," 32.

[20] Hamilton and Kean, *Final Report of the National Commission*, 9.

[21] Office of the Director of National Intelligence, "About the ODNI," http://www.dni.gov/who.htm (accessed December 28, 2009).

[22] Office of the Director of National Intelligence, "Creation of New Information Sharing Steering Committee for the Intelligence Community," ODNI News Release No. 06-07, March 6, 2007, http://www.dni.gov/press_releases/20070306_release.pdf (accessed December 28, 2009).

[23] Ibid.

[24] Ibid.

[25] Office of the Director of National Intelligence, *Intelligence Community Information Sharing (ICIS) Home Page*, http://www.dni.gov/ICIS/index_public.html (accessed on October 7, 2009).

[26] Office of the Director of National Intelligence, *Intelligence Community Information Sharing Strategy*, 3.

[27] Spencer S. Hsu, "U.S. Officials Admit to Intelligence Failures in Connection with Bomb Plot," *The Washington Post*, January 20, 2010.

[28] Office of the Director of National Intelligence, *IC 2008 Employee Climate Survey: Summary of Results*, http://www.dni.gov/reports/IC-Survey_2008.pdf (accessed January 23, 2010).

[29] Ibid.

[30] Gregory F. Treverton and C. Bryan Gabbard*, Assessing the Tradecraft of Intelligence Analysis*, (Santa Monica, CA: The RAND Corporation, 2008), 9.

[31] George W. Bush, *National Strategy for Information Sharing*: *Successes and Challenges in Improving Terrorism-Related Information Sharing* (Washington, DC: The White House, October 2007). Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy*. The National Counterterrorism Center, *NCTC and Information Sharing Five Years Since 9/11: A Progress Report*, (Washington, DC: National Counterterrorism Center, September 2006).

[32] National Counterterrorism Center, "National Counterterrorism Center" brochure, 2008.

[33] Ibid.

[34] Walter Pincus, "Setting an Intelligence Turf War," *The Washington Post*, November 17, 2009, 1.

[35] Office of the Inspector General, Department of Homeland Security. *Information Sharing at the National Operations Center (Redacted)*, OIG-10-15 (Washington, DC: Department of Homeland Security, 2009).

[36] Ibid, 16.

[37] Ibid, 22-23.

[38] Office of the Director of National Intelligence, "New Policy Makes Information Sharing a Factor in Employees' Performance Reviews", ODNI News Release No. 16-08, October 6, 2008, http://www.dni.gov/press_releases/20081006_release.pdf (accessed October 7, 2009).

[39] Ibid.

[40] Ibid.

[41] Statement for the Record of Dennis C. Blair, Director of National Intelligence, and Michael E. Leiter, Director of the National Counterterrorism Center before the Senate Homeland Security and Governmental Affairs Committee, "Intelligence Reform: The Lessons and Implications of the Christmas Day Attack," January 20, 2010, http://www.dni.gov/testimonies/20100120_1_testimony.pdf (accessed January 20, 2010). E-mail correspondence from then-DNI J.M. McConnell to the Intelligence Community workforce, January 26, 2009.

[42] E-mail correspondence from former DNI J.M. McConnell to the Intelligence Community workforce, January 26, 2009.

[43] Director of National Intelligence Dennis C. Blair, message to the IC workforce, January 7, 2010, http://www.dni.gov/press_releases/20100107_release.pdf (accessed January 20, 2010).

[44] Lee Hamilton and Thomas Kean. "'There's Work to be Done,' 9/11 Commission Chairs Say," *USA Today*, January 11, 2010, 9.

[45] Ibid.

[46] Daniel S. Gressang IV and Jeffrey A. Baxter, "Crawling into the Terrorist's Head: Coordination and Cooperation Across Levels of Government," *Defense Intelligence Journal*, 14-1 (2005): 124.

[47] Hamilton and Kean, "'There's Work to be Done,'" 9.

[48] Carrie Johnson, Karen DeYoung, and Anne E. Kornblut, "Obama Vows to Repair Intelligence Gaps Behind Detroit Airplane Incident," *The Washington Post*, December 30, 2009, A01. Spencer S. Hsu, "U.S. Officials Admit to Intelligence Failures."

[49] Pincus, "Setting an Intelligence Turf War," 1.

[50] Ibid, 2.

[51] Karen DeYoung, "Obama to Get Report on Intelligence Breakdown: Agencies Didn't Share or Flag Information on Man Accused in Attempted Plane Bombing," *The Washington Post*, December 31, 2009, 1.

[52] Blair, "Strengthening our nation's front line defense," A31.

[53] Statement for the Record of Dennis C. Blair and Michael E. Leiter, "Intelligence Reform."

[54] Office of the Director of National Intelligence. *Intelligence Community Directive Number 501.*

[55] The IC operated under DNI Intelligence Community Policy Memorandum (ICPM) 2007-500-3, *Intelligence Information Sharing*, from December 22, 2007 until January 21, 2009.

[56] The White House, "Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack," http://www.whitehouse.gov/sites/default/files/summary_ of_wh_review_12-25-09.pdf (accessed January 20, 2010). Mark Mazzetti and Eric Lipton, "Spy Agencies Failed to Collate Clues on Terror," *The New York Times*, December 31, 2009, 1. "Why Didn't They See It," *The New York Times*, January 3, 2010, 20.

[57] Program Manager-Information Sharing Environment, *Report on the Interagency Threat Assessment and Coordination Group (ITACG): Second Report for the Congress of the United States, the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence*, (Washington, DC: Program Manager-Information Sharing Environment, November 2009), 3 and 6.

[58] Ibid, 12.

[59] Ibid, 17.

[60] National Counterterrorism Center, "National Counterterrorism Center" brochure, 2008.

[61] The author previously served as the Chief of the Defense Intelligence Unit (DIU) at the National Counterterrorism Center (NCTC).

[62] Office of the Director of National Intelligence, *Intelligence Community Information Sharing Strategy*, 3.

[63] Statement for the Record of Dennis C. Blair and Michael E. Leiter, "Intelligence Reform."

[64] Ibid, 2.

[65] James Kallstrom, "Op-Ed on FBI's Post-9/11 Counterterrorism Efforts," January 12,2010, http://www.fbi.gov/pressrel/pressrel10/oped_011210.htm (accessed January 12, 2010).

[66] Amy Zegart, "Our Clueless Intelligence System," B1. *Federal Bureau of Investigation Jobs Page,* http://www.fbijobs.gov/128.asp (accessed January 28, 2010).

[67] Robert S. Mueller, Congressional Testimony Before the Senate Committee on the Judiciary, January 20, 2010, http://www.fbi.gov/congress/congress10/mueller012010.htm (accessed January 20, 2010).

[68] Ibid.

[69] Henry A. Crumpton, "Intelligence and Homeland Defense," in *Transforming U.S. Intelligence*, ed. Jennifer E. Sims and Burton Gerber (Washington, DC: Georgetown University Press, 2005), 207. Robert S. Mueller, Congressional Testimony. Amy Zegart, "Our Clueless Intelligence System," B1.

[70] Crumpton, "Intelligence and Homeland Defense," 207.

[71] Robert S. Mueller, Congressional Testimony.

[72] Ibid.

[73] Ibid.

[74] Office of the Director of National Intelligence. *Intelligence Community Directive Number 501.*

[75] Office of the President of the United States, *9/11 Five Years Later: Successes and Challenges,* (Washington, DC: Executive Office of the President, September 2006), 21.

[76] Office of the President of the United States, "Presidential Memorandum to the Heads of Executive Departments and Agencies," December 16, 2005, http://www.ise.gov/docs/Memo_on_Guidelines_and_Rqmts_in_Support_of_the_ISE.pdf (accessed January 7, 2010).

[77] Ibid.

[78] Program Manager-Information Sharing Environment, *PM-ISE Information*, xi.

[79] Ibid, 28-29.

[80] Karen DeYoung, "Obama to Get Report on Intelligence Breakdown," 1. Thomas H. Kean, co-chair of the 9/11 Commission, said the DNI ought to be strengthened to enforce intelligence sharing among agencies.

[81] Hsu, "U.S. Officials Admit to Intelligence Failures." This quote is from 9/11 Commission Chairman Lee H. Hamilton. Hamilton, "'There's Work to be Done,'" 9.

[82] Government Accountability Office, *David M. Walker, Comptroller General,* 17.

[83] Jennifer E. Sims and Burton Gerber, "Meeting the Challenge: Action Now," in *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005), 271. Hamilton, "'There's Work to be Done,'" 9.

[84] Government Accountability Office, *David M. Walker, Comptroller General,* 13.

[85] Ibid, 17.