USAWC STRATEGY RESEARCH PROJECT

A FLAWED NATIONAL BLUEPRINT TO HOMELAND INTELLIGENCE REFORM: RIGHT IDEA, WRONG APPROACH

by

Lieutenant Colonel Cary S. Westin
United States Army

Colonel Mark Eshelman
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

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2006		**00-00-2005 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Flawed National Blueprint to Homeland Intelligence Reform Right Idea, Wrong Approach	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Cary Westin	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,Carlisle Barracks,Carlisle,PA,17013-5050	
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**		**22**	

ABSTRACT

AUTHOR: Lieutenant Colonel Cary S. Westin

TITLE: A Flawed National Blueprint to Homeland Intelligence Reform: Right Idea, Wrong Approach

FORMAT: Strategy Research Project

DATE: 13 March 2006 WORD COUNT: 5370 PAGES: 21

KEY TERMS: Intelligence Sharing, Homeland Security, 911 Commission

CLASSIFICATION: Unclassified

The ongoing conflict in Iraq against a determined insurgency highlights the unfortunate fact that the terrorist threat is more serious today than it was prior to September 11, 2001. How prepared are we now to prevent another attack, potentially with greater consequences? The cornerstone for homeland security is the capability of our intelligence and law enforcement agencies at all levels (federal, state, tribal and city) to timely collect, analyze and disseminate critical, actionable intelligence information. There is one critical aspect of intelligence sharing that has been substantively neglected in our national approach to address the problem. Specifically, there are a number of deeply rooted cultural barriers that have become pervasive in law enforcement and intelligence agencies regarding the collection, analysis and dissemination of intelligence related information. These cultural barriers, or biases, have also had a negative impact on the critical information linkage that must exist between federal and state intelligence and law enforcement agencies. This paper will specifically examine current cultural intelligence sharing challenges that are present between the federal and state / local levels of government, followed by policy recommendations for a more comprehensive national approach.

A FLAWED NATIONAL BLUEPRINT TO HOMELAND INTELLIGENCE REFORM: RIGHT IDEA, WRONG APPROACH

The ongoing conflict in Iraq against a determined insurgency highlights the unfortunate fact that the terrorist threat is more serious today than it was prior to September 11, 2001. How prepared are we now to prevent another attack, potentially with greater consequences? The cornerstone for homeland security is the capability of our intelligence and law enforcement agencies at all levels (federal, state, tribal and city) to timely collect, analyze and disseminate critical, actionable intelligence information. Our federal intelligence capabilities down to the key role of our first responders are inextricably linked, because information about an attack that reaches the front lines of local authorities could potentially mitigate its impact, if not stop the attack entirely. Following the attacks on the World Trade Center and Pentagon, the 9/11 Commission Report documented the need to restructure the intelligence community. [1] Most of the initiatives to date have been organizational in nature: Establishing a new Department of Homeland Security Intelligence and Analysis Office, the May 2003 creation of a Central Intelligence Agency (CIA) National Counter-Terrorism Center, and a major reorganization of the Federal Bureau of investigation (FBI) Counter-Terrorism Division to name a few.

Organizational changes alone, however, will not ensure the facilitation of better interagency coordination or procedures to fix the shortfalls that currently exist, and sadly, the intelligence community is struggling to stay ahead of the many threats to our security. There is one critical aspect of intelligence sharing that has been substantively neglected in our national approach to address the problem. Specifically, there are a number of deeply rooted cultural barriers that have become pervasive in law enforcement and intelligence agencies regarding the collection, analysis and dissemination of intelligence related information. These cultural barriers, or biases, have also had a negative impact on the critical information linkage that must exist between federal and state intelligence and law enforcement agencies. This paper will specifically examine current cultural intelligence sharing challenges that are present between the federal and state / local levels of government, followed by policy recommendations for a more comprehensive national approach.

Significance to U.S. National Interests (Breaking away from the Cold War construct)

An August, 2003 Government Accountability Office (GAO) Report assessing the status of our nation's intelligence sharing capabilities indicated that "An information-sharing process in which needed information is not routinely received or is received but is untimely or irrelevant hampers the nation's collective ability to effectively unify the efforts of all levels of government."[2]

Exacerbating the problem is that traditionally, protecting the United States from terrorist attacks has been the primary responsibility of the federal government and often states and cities have not been included as partners in a combined and coordinated effort.[3]

The genesis for this rationale goes back to a Cold War cultural way of thinking that is still prevalent today. During the Cold War we faced a geographically known enemy, and generally knew what information to look for and where to find it. For the most part, the information we needed in our collection effort was found overseas, and was primarily based on military activities, thus minimizing our need to collect information in the United States or on U.S. citizens. The intelligence expertise and knowledge was "stove piped" in the federal government, with little to no interaction with the public, the private sector or state and local officials.[4] Quite simply, states and cities were not viewed as having a significant role in securing the nation to prevent terrorism. Therefore, there has been limited involvement in the planning for intergovernmental and agency procedures to receive timely intelligence information and subsequent analysis by most state and local law enforcement agencies. In the fight against terrorism, the intelligence problems are far more complex.

In the Homeland Security Act of 2002, Congress found that the federal government relies heavily on the efforts of state and local personnel to protect the U.S. against terrorist attacks, so their ability to receive threat information is vitally important.[5] The threat to our security is far different today. Globalization has significantly reduced the distances between our borders and has led to an information explosion, making access and reach, whether by cellular telephones or the internet almost instantaneous. We are fighting an information war where understanding enemy intent and plans is far more challenging than in the past. Rapid advancements in technology have made it much easier for terrorists to conceal their activities and operate within our borders. To cite the current threat assessment of the 9/11 Commission:
"The United States confronts a very different world today. Instead of facing a few dangerous adversaries, the United States confronts a number of less visible challenges that surpasses the boundaries of traditional nation-states and call for quick, imaginative, and agile responses."[6]
The transnational nature of the threat makes it imperative that we strengthen the capabilities of our state and city officials and make them equally viable partners in the intelligence sharing process.[7]

The September 11, 2001 attacks demonstrated that those individuals wanting to commit acts of terrorism may very well live within our local communities and be engaged in criminal activities as they plan attacks on targets within the United States. Critical information may be derived from information collected by state, city and local government personnel. The National

Strategy for Homeland Security emphasizes that “America’s first line of defense…is its first responder community – police officers, firefighters, emergency medical providers, public works personnel, and emergency management officials.”[8] In the law enforcement agencies alone, there are over 700,000 officers who patrol the streets daily with detailed knowledge of their communities.[9] They can be tremendous multipliers in gathering, reporting and using intelligence information to prevent terror in our country, but they have to get access to terrorist watch lists and threat indications to be effective. According to the October 2002 Hart-Rudman Report, "When it comes to combating terrorism, the police officers on the beat are effectively operating deaf, dumb and blind."[10] The federal government loses an extremely important capability by not fully integrating state and city governments into the information sharing and policy process. There is a substantial amount of threat information that can be obtained by local city officials, for example, police officers. More importantly, without the full coordination across intelligence and law enforcement agencies, our country potentially risks facing another national disaster like that which occurred just a few short years ago.

9/11 Commission Findings

In July 2004, the National Commission on Terrorist Attacks Upon the United States[11] published a comprehensive report on the facts and circumstances that led to the attacks on September 11, 2001, documenting the shortcomings in law enforcement, intelligence and congressional oversight. The Commission issued 41 recommendations that generally set policy objectives, but focused primarily on government organizational change. Their analysis of the intelligence community highlighted the need to restructure, based on identified problems associated with structural barriers, lack of common standards for foreign and domestic intelligence, divided management of national intelligence capabilities, and a poor capability to set priorities and move resources.[12] Intelligence sharing, as a subset of the broader discussion on intelligence shortfalls received very little attention by the Commission., They provided two specific recommendations: 1) “Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge.”[13] 2) “The President should…coordinate the resolution of the legal, policy, and technical issues across agencies to create a trusted information network.”[14] The idea of making incentives for sharing and creating a trusted network are extremely important components, but they are two of many means, not an end in providing a recommended approach to solve the problem.

Curiously, the Commission’s report indicated that “The biggest impediment…to a greater likelihood of connecting the dots – is the human or systemic resistance to sharing information.”[15]

With that comment they captured the essence of the problem but offered no recommendations focused on changing the human and organizational mindset. It is here where the national approach to information sharing is flawed. The resistance to sharing information is all about organizational, agency and government culture. There may be other causes besides cultural issues that lend to the problems associated with intelligence sharing, but this paper will focus on the primary cultural impediments, because they are the underlying factors that prohibit our country from sharing needed information.

The 9/11 Commission's recommendations essentially form the blueprint, or roadmap that the nation's efforts have been, and will continue to be, measured against since their published report. Their report failed to capture methods to eliminate the existing cultural biases and overly protective nature of information ownership (the root causes of the deficiencies we have today). Instead, we are proceeding down a path that is emphasizing reorganization which has resulted in political infighting and turf wars that are not making us any better at "connecting the dots." With that said, however, The Bush administration acted swiftly in response to the findings of the 9/11 Commission with a reorganization move in order to establish a governmental focal point for homeland security.

Direction / Focus of the Department of Homeland Security

Executive Order 13228 signed by the President on October 8, 2001 established the Office of Homeland Security, with a mission to "coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States."[16] Shortly thereafter, it became clear that an Executive Office within the White House would be unable to effectively accomplish the comprehensive scope of activities required, so with the Homeland Security Act of 2002, Congress and the President created the Department of Homeland Security (DHS), moving a number of different departmental bureaus and placing them within DHS.[17] The Department's primary mission is to prevent terrorist attacks, reduce vulnerability, and minimize damage in the event of terrorist attacks within the United States.[18] The White House established the Department of Homeland Security with the intent of having a lead Department with responsibility to coordinate and tie together all of the disparate intelligence sources, both foreign and domestic, heightening our nation's preparedness by getting critical information to the right people in a timely manner. [19]

To fulfill this requirement, the DHS established the Directorate of Information Analysis and Infrastructure Protection (IAIP) to coordinate and analyze terrorist threat intelligence information, assess infrastructure vulnerabilities, and be the nation's primary intelligence fusion and analysis

center for disseminating Homeland intelligence information to the private sector and to relevant federal, state and local officials.[20] With an understanding of the role of the Department of Homeland Security, the first cultural challenge that must be addressed is the tendency of federal agencies to overly protect their roles and missions and their insatiable appetite for power. This has become markedly evident over the past few years in observing the actions of the CIA and FBI.

Cultural Turf Wars. DHS Struggle for Relevance

Instead of being the preeminent homeland security organization originally envisioned, according to Seth G. Jones, associate Political Scientist at the RAND Corporation, "DHS has struggled for relevance and become increasingly sidelined in the analysis and dissemination of terrorism related intelligence."[21] He cites a number of significant examples, such as the Central Intelligence Agency's surging role in Homeland Security through the creation of the Terrorist Threat Integration Center in 2003, and a number of FBI initiatives to improve their counter terrorism and intelligence capabilities.[22] Certainly one could argue that the added capabilities of the CIA and FBI have strengthened our ability to thwart terrorist attacks against our country, but the ensuing power struggle between these agencies may actually undermine our national efforts in the war on terrorism.

With the increased capabilities (and responsibilities) of the FBI and CIA, support for the DHS has faded as policymakers question their ability to conduct adequate threat analysis relative to the other federal agencies.[23] The FBI and CIA, while gaining support of political backers, have resisted handing over responsibilities to the DHS, an assertion which is becoming more evident through their expanded homeland security roles and functions.

Although it does not collect domestic intelligence, the CIA has traditionally been the nation's primary agency for counterterrorism overseas. When the idea to create an improved interagency terrorism center surfaced following the attacks on September 11, 2001, the CIA lobbied to keep it under the control of the Director of Central Intelligence.[24] They argued that DHS had nowhere near the experience necessary to coordinate and handle both foreign and domestic intelligence. Secondly, the CIA argued that one center capable of controlling both offensive capabilities (preemption against terrorist organizations) and defensive capabilities (homeland vulnerability analysis) was best suited to their expertise.[25] The outcome of the discussions led to the establishment of the Terrorist Threat Integration Center (TTIC), which was staffed by a number of federal agencies including the CIA, FBI, DHS and the Department of Defense. Although the TTIC was not a part of the CIA organizationally, the CIA held budgetary

control and a significant amount of influence.[26] The Intelligence Reform and Terrorism Prevention Act of 2004 provided statutory authority for the establishment of a National Counterterrorism Center (NCTC), absorbing the TTIC, and placing it under the newly established Director of National Intelligence.[27] This change in structure was prompted by two of the 9/11 Commission recommendations to facilitate better information sharing.[28] The CIA still retains management authority for all overseas human intelligence collection and remains in charge of disrupting terrorist activities abroad.[29]

The FBI has also gone through a transformation after being criticized by the 9/11 Commission for not being proactive enough to counter domestic terrorist threats. In response to the criticism, the FBI Director adopted a preemptive strategy and made counterterrorism his first priority, and establishing broad organizational changes, which included significant resources to stand-up a Counterterrorism Division.[30] The FBI also created 66 Joint Terrorism Task Forces throughout the United States in an attempt to better integrate state and local law enforcement officials.[31] It is ironic that the FBI focused so intently on broadening its coordination capability organizationally, it did so at the expense of the technology infrastructure to adequately support the effort, an aspect that will be discussed in more detail later.

The initiatives of the CIA and FBI have made it exceedingly difficult for the DHS to establish a prominent role for intelligence analysis and dissemination. They frankly don't have the capabilities inherent in their organization to analyze raw intelligence data effectively. They also have had trouble retaining quality analysts, who have been departing their ranks for more lucrative jobs in organizations such as the CIA, FBI, DOD and State.[32] Exacerbating the problem has been direct competition in disseminating and sharing threat information despite President Bush's July 2003 Executive Order giving the Secretary for Homeland Security primary authority. The problem was serious enough for Senator Lieberman to express in a letter he sent to the President on 17 December 2003:

> It appears that, in order to protect their own turf, some key agencies may already be working against the spirit of the legislation…I call on you to intervene immediately and clarify to the intelligence community and the nation that the new department will play the central role in fusing and analyzing intelligence that Congress intended it to play. It is time to nip these damaging bureaucratic turf battles in the bud and ensure from the start that the department has broad access to the information it needs to protect the American people.[33]

The aftermath of this appeal, over two years later and despite the subsequent 2004 Intelligence Reform and Terrorism Prevention Act, is that instead of having a focused capability to collect, analyze, coordinate and disseminate information through one primary office of responsibility, we now have multiple entities executing this function under their own supervision

and control. By way of recent example, the analysts at the NCTC have access to 26 information networks that span across all of the intelligence agencies, but there is no uniting network to bring them together. In order to share information with others outside of the NCTC, analysts must get permission from the originating agency. For example, an FBI analyst wanting to share intelligence with a CIA analyst not working within the NCTC would have to gain permission first from the FBI.[34] This takes us back to the problem of 2001, where information will potentially only be passed if the data owner decides to share it. Adding to the problem, despite the surge in efforts by the FBI, Justice Department Inspector General Glenn A. Fine noted in a congressional hearing just two months ago that the FBI is assigning many of their analysts to duties that have little to do with analysis.[35] This has resulted in an alarmingly high rate of attrition recently from many of their most qualified and educated analysts.[36] Fundamentally, we have not changed the cultural paradigm despite the legislation and reorganization efforts that have been established. To better understand the complications of data ownership and the cultural resistance to share the intelligence information, we must analyze the distinct differences between law enforcement and the traditional intelligence agencies.

Separation of Law Enforcement and Intelligence

The second cultural challenge centers on the differences in purpose of using information that exists in both our intelligence agencies and law enforcement communities. In a Congressional Research Service Report for Congress on Intelligence to Counter Terrorism, Richard Best, a specialist in national defense stated that "Countering terrorism requires close cooperation between law enforcement and intelligence agencies; some terrorists will need to be brought to justice in courts, but others are dealt with by military forces or covert actions."[37] He goes on to highlight that our past failures to prevent terrorist attacks like September 11, 2001 have evolved from poor information exchanges between law enforcement and intelligence communities and "blurred lines of organizational responsibility."[38]

The National Security Act of 1947 generally separated law enforcement functions, prohibiting the Central Intelligence Agency from having "policing," or law enforcement powers. The intention of the act was to hold intelligence separate and distinct from law enforcement functions.[39] Law enforcement agencies typically use information provided as a means to build evidence that will be used to prosecute in a court of law. In other words, the intent is to provide disclosure to the accused. Their efforts are governed by laws and rules that were designed to protect the rights of the accused. In contrast, the methods of Intelligence agencies are far less restrictive, collecting information from sensitive sources or using special methods to protect

sources for future use, and the information is normally documented in a classified report. The interest of the intelligence community is protection of national security from forces that would do our nation harm, and subsequently the culture developed to closely guard the information from enemy access either directly or indirectly. These differing perspectives are at odds with one another when countering international terrorism, since there are typically both criminal and national security components involved.[40] As documented by the 9/11 Commission, the FBI was convinced institutionally, and in practice, that it could not share intelligence information, regardless of using FISA procedures or not, with criminal investigators.[41] The problem is aptly described within the USA PATRIOT Act: "Respect for due process is essential for law enforcement but not a part of successful intelligence activities."[42]

Because both law enforcement and intelligence agencies are so jointly tied to the war on terrorism, sharing information at all levels, not just between federal entities, can be very complicated. In October, 2001, Congress passed the USA PATRIOT Act [43]which resolves some of the intelligence and law enforcement community sharing issues, establishing the legal framework for more effective sharing. The PATRIOT Act gives federal law enforcement agencies greater freedom to share information and to coordinate their efforts. Where we have still failed to achieve substantial progress is with breaking through barriers in technology and in the cultural aspects of these organizations.

Interoperability issues hinder communications both between federal agencies and federal to state. The Silberman-Robb commission found "…ongoing problems with outdated computer systems that won't allow employees from different intelligence agencies to talk to each other…the existing systems are so outdated that an FBI agent still can't send a secure e-mail to his counterpart at the Department of Homeland Security."[44] Recent initiatives, including a substantial FBI computer revampment were recently halted because of system difficulties.[45] The problem of interoperability and outdated technology is magnified when looking at the requirements to pass information from the federal level down to the myriad of state and city officials. Despite relatively recent legislation to enhance the information flow across agencies, immediate attention and resources must be applied to facilitate broader access.

Security Clearance Access Issues

The third cultural challenge relates to problems accessing intelligence information. Executive Order no. 12958, Classified National Security Information, prescribes the procedures for classifying, safeguarding and declassifying national security information, which includes information related to defending our country against terrorism.[46] In addition, Executive Order

12968, Access to Classified Information, states that access is generally limited to persons who have been granted a clearance and demonstrate a "need to know" within the conduct of their official functions and responsibilities.[47]

As previously mentioned, the federal intelligence community has traditionally not considered state or city government officials needing access to terrorism related information. This mindset has resulted in very few officials at the state and local levels having the necessary clearances required to access intelligence information. Officials at the National Emergency Management Association, representing state and local emergency management personnel expressed serious concerns over security access issues. According to these officials, many state and local directors, fire and police chiefs hold clearances that were granted by the Federal Emergency Management Agency, but are not recognized by the FBI.[48] In addition, most of the state governors don't have the appropriate security clearances to receive classified threat information which significantly impacts their ability to efficiently utilize the National Guard and degrades their emergency response capabilities.[49]

Today's threat conditions require that we broaden our access of actionable information to all levels of government, including our first responders. Complicating this issue even further, the access problem isn't just between federal and state agencies. In the recently established National Counter-Terrorism Center, agents and analysts are still primarily stove-piped in their ability to access information. In a follow-up on actions taken since the 9/11 Commission Report, "The commissioners found that there were no less than nine levels of classified information stored in the center's computers. Analysts from different agencies had different clearances making it difficult for them to talk to one another despite working in the same building."[50] This is in addition to the aforementioned technological interoperability problems the Center is experiencing.

Internally, the FBI is currently stifled by the lack of clear procedures and resources to facilitate good access. As Melanie Sisson, a former intelligence analyst at FBI headquarters from December 2003 to May 2005 pointed out:

> A system in which analysts are not guaranteed access to investigative information, one in which they must ask to be given the intelligence they were hired to assess, marginalizes analysts professionally and demoralizes them personally. It is a circumstance that breeds frustration…by tacitly condoning the perception that analysis is of secondary importance to the FBI, perpetuates the bureau's traditional cop culture.[51]

As David M. Walker, Comptroller General of the United States pointed out in his GAO findings this past year on information sharing, "We agree the intelligence community needs to

move from a culture of "need to know" to "need to share."[52] We are currently still following an "outdated intelligence cycle model that ends with a final intelligence product that very much reflects the bias of whatever organization produced the intelligence…the notion of "data ownership" must be eliminated if we are ever to have real "all-source" analysis."[53] The appropriate response to begin developing this cultural mindset can be influenced by establishing a national trusted network, per the 9/11 commission's recommendation and providing incentives for participation at all levels of our government. Despite a number of positive steps to improve our capabilities since 9/11, this networked information sharing system is not close to being achieved almost five years later.

The Need for a Trusted Information Network

The 9/11 Commission's recommendation to establish a "trusted network," in other words, a network where users don't fear that their mission or sources will be compromised, is a necessary component to address cultural information protection issues. Trust has to be developed on the disposition of the information that is to be shared. The two obstacles to enable this network involve classification and information security.[54] The current system makes broad assumptions that it is possible to know in advance which agencies need the information. "The risks associated with disclosure are greater than the potential benefits of wider information sharing"[55] according to Bill Crowell, from the Markle Taskforce on National Security in the Information Age. Incentives are established to protect information, not provide it, which leads to the over classification problem.[56] The network, to be effective, must be decentralized and incorporate procedures to both push and pull information, generating reports that allow access to be based on authorization vice classification.[57] Regularly producing sanitized threat information is not a common practice among our nation's intelligence agencies, and the process is slow and cumbersome. Instead, we should examine the potential benefits of creating "tear line" reports in which an agency produces a less classified version along with the classified report. An example of this is at the highest level of classification, the report would reveal source information; at the next level of classification explicit details on the threat information; and an unclassified version that might only contain tasks, or actions that should be implemented by those in the network.[58] By making this a national framework, it will enable change across all levels of government. Serious thought is needed in revising current legislation and procedures for this to become a reality.

Uncoordinated Information Sharing Initiatives

The fourth cultural challenge revolves around independent initiatives to obtain information. It is hardly surprising that the attacks on September 11, 2001 created an outgrowth of initiatives at all levels of government to better share and access intelligence information related to terrorist threats. For example, California has established a terrorist related information repository that is disseminated to their law enforcement officers, and New York has established a Joint Counterterrorism Committee combining both their state law enforcement and the FBI.[59] The problem resulting from these initiatives is that there is no central management, or national level strategy leading to their development, nor was there a national architecture or blueprint on the interoperability of these initiatives with other agencies across the United States. Instead, there are many state and federal stove-piped systems with selective user participation.
While the intentions for improved collaboration are good, there is a danger in having multiple independent systems. "Officials from the Central Intelligence Agency acknowledged that states' and cities' efforts to create their own centers are resulting in duplication and that some cities may be reaching out to foreign intelligence sources independently from the federal government."[60] Another obvious, but important limitation to point out is that while these initiatives may promote the sharing of information between partners, they exclude those not participating. There is also the potential for federal agencies to establish informal partnerships to meet their information requirements outside of the management of the Department of Homeland Security's overall national collection and dissemination efforts, enhancing the probability that we will not be able to adequately identify threats by combining both national and regional information on a potential attack.[61]

The complexity and vast amount of information that must be sorted and pieced together to identify threats to our country is a daunting challenge. The implementation of policy measures should include a combination of actions: revising legislation, fixing technology interoperability shortfalls, as well as taking active steps to reform the human capital aspects that drive our current intelligence and law enforcement culture. The following recommendations are too closely intertwined to prioritize one over the other. They should be approached and resolved concurrently because of their dependence to effectively create the necessary intelligence sharing environment that has been envisioned since the 9/11 report.

Policy Recommendations

I recommend the following actions be implemented to resolve our information sharing shortfalls:

- The Federal Intelligence and law enforcement agencies must fully integrate states and cities into the intelligence planning process. At a minimum there should be national and state advisory boards established to determine interoperability and information needs both horizontally (between peers), and vertically (between federal, state and city officials). Dialogue over information protection issues will enhance development of a trusted network mutually reinforcing across all levels of government.
- Develop a national level terrorism intelligence and information network and computer database vice state and regional repositories. This will require establishing common information technology standards, as well as resources to upgrade both federal and state communications and information technology systems. The Department of Homeland Security and the Director of National Intelligence should assess the current state and federal systems that are now established so that the choice of a common standard will capitalize on existing technology that has already been developed. A "new start" system will likely be too prohibitive in terms of cost and time involved to build the new infrastructure. By establishing this construct, we will be better able to integrate many of the uncoordinated information sharing initiatives that exist today at the state and city level.
- Amend the language in Executive Order 12968, Access to Classified Information, so that state, local and private sector officials have access to required information, but safeguards must be established. Sanitizing the threat information should not become policy as a means to just increase nation-wide access. De-sensitizing threat information without establishing clear procedures will likely lead to not having enough fidelity in the detail that is necessary to fully understand and take action on the threat. Our policy should identify the appropriate individuals needing access, and reduce the timelines that currently exist to process the proper clearances. This assessment should also look at potentially broadening the audience of those that require clearances under the auspices of "needing to share". In other words, we have to review the classification system currently in place and develop effective procedures to prevent over- classification. Language in the amendment should insist on implementing common clearances that will be recognized at all levels of the government.
- We must take direct steps to remove the cultural barriers that have solidified organizationally since the Cold War. An initial step is to implement robust internal information sharing procedures which protects the mission requirements of often

disparate organizations such as law enforcement and intelligence agencies. An example includes developing screening tools to automatically alert disseminators when sensitive information is going to be transmitted, or when information is going to be sent to those without the requisite access.[62] There are many other automated information security tools that can easily be utilized, or developed to enhance the trust in how information will be passed over the network. This will certainly be a positive step to reduce the information barriers that currently exist today, and parallel the first recommendation on developing a structured partnership among federal and state agencies in establishing common procedures.

Conclusion

Resolving our information sharing shortfalls is vitally important to prevent a repeat of the terrorist attacks on our country. The current process in sharing information, although somewhat improved, is too reliant on a rigid hierarchy and bureaucracy that is cumbersome, slow and resistant to change. Efforts to date, relative to the status quo prior to September 11, 2001 may seem optimistic to some, but there is great danger in thinking that the status quo is good enough to prevent another attack. There is too much at stake for the protection of our nation. While organizational transformation dominates our homeland security reforms to date, our priority efforts must move away from grand designs towards more practical measures to improve established capabilities for dealing with the threats that our country faces today. The first step in reforming our approach must include as a first priority, procedures to strip away the organizational cultural aspects impeding the sharing of intelligence information. If we don't seriously focus our efforts in this direction, we are surely susceptible to another disastrous attack against our nation in the future. That is a risk we can't afford to take.

Endnotes

[1]: U.S. National Commission on Terrorist Attacks Upon the United States , *The 9/11 Commission Report* (Washington: GPO, 2004), 407.

[2] U.S. General Accounting Office, *Homeland Security: Efforts to Improve Information Sharing Need to be Strengthened* (Washington D.C.: U.S. General Accounting Office, August 2003), 5.

[3] Ibid., 7.

[4] James B. Steinberg, *Consolidating Intelligence Analysis: A Review of the President's Proposal To Create a Terrorist Threat Integration Center,*1, available from

http://www.brookings.edu/printme.wbs?page=/pagedefs/69b111d46553ff3c173a72ca0a1; Internet; accessed 25 Nov 2005.

[5] *Homeland Security Act of 2002*, sec. 102, 16 (2002), available from http://news.findlaw.com/hdocs/docs/terrorism/hsa2002.pdf; Internet; accessed on 28 Nov 2005.

[6] *The 9/11 Commission Report*, 399.

[7] Ronald Marks, "Homeland Security's Biggest Challenge: Too Much Information," The Christian Science Monitor, 21 November 2005, 9.

[8] George W. Bush, *National Strategy for Homeland Security* (Washington D.C.: The White House, July 2002), 41.

[9] Michael W. Ritz, Ralph G. Hensley, Jr., and James C. Whitmire, *The Homeland Security Papers: Stemming the Tide of Terror* (Alabama: USAF Counter proliferation Center, 2004), 168.

[10] Gary B. Hart and Warren Warren B. Rudman, *America Still Unprepared – America Still in Danger: Report of an Independent Task Force Sponsored by the Council on Foreign Relations* (New York: Council on foreign Relations, Inc., 2002), 19.

[11] The National Commission on Terrorist Attacks Upon the United States is informally known as the 9/11 Commission.

[12] *The 9/11 commission Report*, 408-409

[13] Ibid., 417.

[14] Ibid., 418.

[15] Ibid., 416.

[16] George W. Bush, *Establishing the Office of Homeland Security and the Homeland Security council, Executive Order 13228* (Washington, D.C.:The White House, 8 October 2001), sec.3; available from <http://frwebgate.access.gpo.gov/cgi-bin/ getdoc.cgi?dbname=2001_ register&docid=fr10oc01-144.pdf>; Internet; accessed 5 December 2005.

[17] *Homeland Security Act, U.S. Code, vol. 6, sec. 101 (2002)*; available from <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?bdname=107_cong_public_laws&docid=f: public296.107.pdf>; Internet; accessed 5 December 2005

[18] Ibid.

[19] Dana R. Dillon, "Breaking Down Intelligence Barriers for Homeland Security," The Heritage Foundation Backgrounder, no. 1536 (15 April 2002); available from http://www.heritage.org/library/backgrounder/bg1536.html; Internet; accessed 1 December 2005.

[20] Seth G. Jones, "Terrorism and the Battle for Homeland Security," 21 May 2004; available from http://www.fpri.org/enotes/20040521.americawar.jones.terrorismdhs.html; Internet; accessed 5 September 2005.

[21] Ibid.

[22] Ibid., 2.

[23] Ibid.

[24] Ibid., 3.

[25] Ibid.

[26] Ibid.

[27] Helen Fessenden, "The Limits of Intelligence Reform," *Foreign Affairs*, Vol 84, Issue 6 (Nov/Dec 2005):5 [database on-line]; available from ProQuest; accessed January 5 2006.

[28] Ibid., 2.

[29] Ibid., 5.

[30] Jones, 3.

[31] Ibid., 4.

[32] John Mintz, "*At Homeland Security, Doubts Arise Over Intelligence* ," Washington Post, July 21, 2003.

[33] Katherine McIntire Peters, "Five Homeland Security Hurdles," 15 February 2003; available from http://www.govexec.com/features/0203/0203s1.htm; Internet; accessed 2 October 2005.

[34] Fessenden, 6.

[35] Melanie M. Sisson, *"The FBI's 2nd-Class Citizens,"* Washington Post, December 31, 2005.

[36] Ibid.

[37] Richard A. Best, "*CRS Report for Congress: Intelligence to Counter Terrorism: Issues for Congress*", 21 February 2002; available from http://fpc.state.gov/documents/ organization/ 21217.pdf; Internet; accessed 12 December 2005, 1.

[38] Ibid.

[39] U.S. General Accounting Office, *Homeland Security: Efforts to Improve Information Sharing Need to be Strengthened*, 8.

[40] Dillon, 26.

[41] *The 9/11 Commission Report*, 79.

[42] Michael Isikoff and Daniel Klaidman, *Look Who's Not Talking-Still*, Newsweek, 4 April 2005, 30.

[43] Public Law 107-56 (enacted Oct 26, 2001), *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act(USA PATRIOT ACT) of 2001*.

[44] Kurt M. Campbell and Michele A. Flournoy, *To Prevail: An American Strategy for the Campaign Against Terrorism* (Washington D.C.: The Center for Strategic and International Studies, 2001), 100.

[45] Ibid., 31.

[46] Executive Order No. 12958, *Classified National Security Information*, April 17, 1995.

[47] Executive Order No. 12968, *Access to Classified Information*, August 2, 1995.

[48] U.S. General Accounting Office, *National Preparedness: Integration of federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security* (Washington D.C.: U.S. General Accounting Office, April 2002), 14.

[49] Ibid., 14.

[50] Isikoff and Klaidman, 31.

[51] Sisson.

[52] U.S. General Accounting Office, *9/11 Commission Report: Reorganization, Transformation, and Information Sharing* (Washington D.C.: U.S. General Accounting Office, August 3, 2004), 5.

[53] Saxby Chambliss, "We Have Not Correctly Framed the Debate on Intelligence Reform," Spring 2005; available from http://carlisle-www.army.mil/usawc/parameters/ 05spring/ chambliss.pdf; Internet; accessed on 20 December 2005, 12.

[54] Bill Crowell, "Too Many Secrets: Overclassification as a Barrier to Information Sharing," 24 August 2004; available from http://www.fas.org/sgp/congress/2004/082404crowell.html; Internet; accessed on December 27 2005.

[55] Ibid., 2.

[56] Ibid.

[57] Ibid., 4.

[58] Crowell, 3.

[59] U.S. General Accounting Office, *Homeland Security: Efforts to Improve Information Sharing Need to be Strengthened*, 14.

[60] Ibid.

[61] Ibid, 15.

[62] Ibid.