Statement of Zoe Baird Budinger[1] and Jeffrey H. Smith[2]
Senate Committee on Homeland Security & Governmental Affairs

October 12, 2011

# Ten Years After 9/11: A Status Report On Information Sharing

Thank you Chairman Lieberman and Senator Collins for holding this hearing and for your leadership on this critical issue. This statement is submitted on behalf of the Markle Task Force on National Security in the Information Age.

We commend the Committee for the significant time and energy you have devoted to making homeland security information sharing a top national priority. You have led this effort since the attacks of 9/11 with a singular commitment and have helped make this nation safer. Since 2002, the Markle Task Force has provided policymakers, including this Committee, with recommendations[3] to help accelerate our government's use of information and information technology to better understand the threats we face and make better decisions about those threats, while protecting traditional civil liberties. Our ultimate goal has been to help enable the federal, state, and local governments to work together to protect our nation from terrorism and other threats.

A substantial change has occurred throughout government in the way security professionals do business. Information sharing has become more widespread and the government has made real changes that are necessary to respond to new threats. That said, progress has been too slow in some places and has lacked adequate guidance or oversight in others.

In the decade since the September 11th attacks, our government has answered the threat of terrorism by transforming itself in important ways. The lack of major attacks on our homeland over the past decade, along with a string of notable intelligence successes, including the recent strikes on Anwar al-Awlaki and Osama bin Laden, is a testament to the fact that things have changed. It has been hard to do, and there is much more to be done, but there has been real progress that deserves to be acknowledged.

The attacks on 9/11 showed all of us that the Cold War "need to know" system for managing classified and sensitive information drove a culture of information security that resulted in countless stovepipes and secretive pockets of the nation's most valuable information. It may have worked in the Cold War, but it was not adequate to keep America safe in a world of asymmetric threats. Many realized that protecting America in this new threat environment would require the government to operate in an entirely new way.

You have enacted two major laws that have substantially changed how government understands those who would do us harm and how it acts to prevent that harm. We have tried to contribute to this challenge. Over the course of four reports written between 2002 and 2009,[4] the Markle Task Force

[1] Zoe Baird Budinger is President of the Markle Foundation. She and Jim Barksdale co-chaired the Foundation's Task Force on National Security in the Information Age. She served on the President's Foreign Intelligence Advisory Board from 1993–2001 and the Department of Defense: Technology and Privacy Advisory Committee ("TAPAC") from 2003–2004.

[2] Mr. Smith is a member of the Markle Task Force on National Security in the Information Age and a Senior Partner at Arnold & Porter LLP. He is a former General Counsel of the Central Intelligence Agency and currently serves on the Director of CIA's External Advisory Board. Mr. Smith will provide today's oral testimony.

[3] For more information on all of our previous work on information sharing, please visit www.markle.org/national-security.

[4] All of the Markle Task Force reports are available at http://www.markle.org/national-security/markle-task-force-national-security/reports.

grappled with how the government could operate in a new way. With national security experts from every administration since President Carter, civil liberties advocates, information technology executives, academics, and many from within government and the Intelligence Community, we proposed a collaboration across agencies that would foster a robust sharing of information and ideas. In order for this collaboration to be successful a set of policies was required that would simultaneously empower and constrain government officials by making clear what collection, analysis, sharing, and uses of information were permissible, and what were not. Instead of storing data centrally, we suggested storing data on a distributed network, thus eliminating the gaps between government agencies and empowering all players in the network—including those at the edges—to create and share actionable and relevant information. Such a network is more protective of civil liberties because it avoids a focus on creating large centralized databases and limits access to information to those who appropriately should use it. The objective of this network was to enhance the government's ability to discern indicators of terrorist activity amid overwhelming amounts of information and to create more time for the nation to respond to threats more effectively.

Since 9/11, there has been a shift in federal and state government culture towards this type of information sharing and collaboration model, and some segments of the government have made progress implementing information sharing policies. Government sources report that this approach, in turn, has been very successful. The agility that sharing information has given our government officials has enabled them to better understand our rapidly changing world. If information sharing policies and practices had not been implemented, these successes might have been tragedies. Clearly, now is not the time to turn back the clock on information sharing.

Of course, there are risks inherent in sharing more information, but these risks are outweighed by the risks of not sharing. The attacks on 9/11 are a stark example of this.

We would like to briefly discuss: (i) where we were ten years ago, (ii) where we are now, (iii) where we fall short, and (iv) where we should be going. The Markle Task Force has four concrete recommendations for further improving information sharing and continuing this post-9/11 transformation. We hope our comments will give the Committee a better sense of how far the government has come and what steps still need to be taken.

## I. Where We Were Ten Years Ago: *Failure to Adapt to a Networked World*

In hindsight, it is clear that our failure to discover the September 11th plot was in many ways a failure of information sharing and a failure to empower our best and brightest. It was a disastrous illustration of our government's failure to adjust to a networked world. The U.S. government might have prevented the 9/11 attacks if the Federal Bureau of Investigation ("FBI"), the Central Intelligence Agency ("CIA"), and state and local law enforcement had connected what they each knew about the hijackers and acted upon it.

Ten years ago, our law enforcement and intelligence communities were driven by a Cold War "need to know" culture that stovepiped information and stymied cooperation. As demonstrated by the ten lost "operational opportunities" to derail the September 11th attacks that the 9/11 Commission identified, both the CIA and the FBI failed to disseminate information in the run-up to the attacks. This was, in part, because of the so-called "Wall" between law enforcement and intelligence. What information they did share often lacked the full context that might have shed light on its big picture significance. The culture that led to this failure is vividly illustrated by a CIA analyst who told the 9/11 Commission that he did not volunteer information he knew about a suspected terrorist when the FBI showed him surveillance pictures of the individual because he "was not authorized to answer FBI questions regarding CIA information."[5]

Silos also existed between agencies and within individual agencies that forced people to work in

[5] Thomas H. Kean et al., The 9/11 Commission Report 269 (2004).

hierarchical pyramids, preventing people on the edges of the system from collaborating to chase down leads. For instance, in July 2001, an FBI agent in the Phoenix Field Office prepared a memo on the "possibility of a coordinated effort" by Osama bin Laden to send students to civil aviation schools. A month later, the FBI's Minneapolis Field Office initiated an unrelated investigation into Zacarias Moussaoui, who was taking flight lessons that the Minneapolis office suspected might be part of a plan to hijack a plane. However, having taken no action on the Phoenix memo, FBI headquarters was not sensitized to the potential threat and instructed Minneapolis that it could not share its complete Moussaoui report with the FAA.

These failures to "connect the dots" have become famous in the years since 9/11. However, that phrase oversimplifies a fundamental problem, not only with the sharing of information, but also with the way in which departments and agencies worked together.

## II. Where We Are Now: *Evidence that Washington Can Work*

Over the last decade, our government has embarked on a "virtual reorganization" in how it answers the threat of terrorism. This shift in thinking has inspired reform in the way agencies and people collaborate and communicate. Top al-Qaeda leaders have been killed and new attacks on the homeland have been prevented because of this transformation in how agencies across government work together and share information in order to detect and preempt terrorist attacks. Substantial progress has been made in shifting the "need-to-know" culture toward a "need-to-share" paradigm, in which information flows more freely enabling greater collaboration between federal, state, and local agencies as well as the private sector.

Information is also increasingly decentralized and distributed. Informal and flexible groups of analysts from different parts of government and the private sector are able to work together and share expertise. Today, our government is able to function in hubs and spokes and distributed networks, empowering people at the edges of agencies instead of working in hierarchical pyramids. Information is shared, and teams from disparate parts of government go in and out of the National Counterterrorism Center and fusion centers nationwide. Ad hoc pursuit teams of experts or concerned officials form and disband as they see problems needing attention. The adoption of powerful social networking tools allows analysts to connect with colleagues throughout government. No longer must all information or requests for authority go up a chain of command or come down from on high.

We are pleased that the Markle Task Force contributed to this change by making recommendations that have been adopted in legislation, executive orders, and the 9/11 Commission Report. This Committee deserves special recognition for making these issues a priority and conducting continued oversight to measure progress. Both the Obama Administration and the Bush Administration have worked hard to put policies and processes in place to achieve these changes.

We are delighted that Ambassador McNamara is testifying today, as he played a critical role as the Program Manager for the Information Sharing Environment in making many of these changes.

The result of these reforms is that people within government are starting to work across agency lines in new and more powerful ways to understand the meaning of fragments of information and use that analysis to make better decisions. This "virtual reorganization" can be illustrated through three successes that were only possible because people worked together and shared information in ways that would have been considered impossible before 9/11.

1) Osama bin Laden was killed on May 2, 2011 as a result of a long-term, dedicated multi-agency mission that 9/11 Commission Chairman Lee Hamilton said unquestionably "came about as a result of reforms that . . . yielded much closer collaboration and intelligence sharing."[6] This story

[6] *Threats to the American Homeland After Killing Bin Laden: An Assessment: Hearing Before the H. Comm. On Homeland Sec.*, 112th Cong. (2011) (statement of Lee Hamilton).

can be seen from press reports. Apparently, CIA led the effort that found al-Qaeda's leader, and the Joint Special Operations command, the National Security Agency ("NSA"), the National Geospatial-Intelligence Agency ("NGA"), and the Director of National Intelligence ("DNI") all played critical roles. These agencies are reported to have worked together seamlessly to provide the assault team as much information as possible on what they could expect to find at the compound. Teams of analysts sorted battlefield and all-source intelligence, designated subjects for additional collection, and conducted pattern analysis of relationships among terrorists, couriers, and raw data collected in the field. Collaboration between these agencies and departments helped weave together intelligence from a wide variety of sources in order to locate Bin Laden. Once the compound was identified, an interagency team, led by the CIA, reportedly developed and executed the raid brilliantly. The success of the Bin Laden mission built on the experience and trust gained from the interagency teams that fused intelligence operations and analysis in Iraq.

2) Najibullah Zazi was arrested in September 2009 in connection with an al Qaeda plot to bomb the New York City subway system. Again, press reports attribute this success to collaborative efforts, in this case those of the FBI, the Department of Homeland Security ("DHS"), and the New York and Denver police. Former DNI Dennis Blair also cited the Zazi case as "a prime example [of] the new level of cooperation among FBI, local law enforcement and U.S. intelligence agencies."[7] These agencies successfully thwarted one of the most serious terrorist threats since 9/11 by sharing information in ways that rarely occurred before the creation of state and local fusion centers and the FBI's Joint Terrorism Task Forces ("JTTFs"). According to press reports, counterterrorism analysts first became aware of a link between the Afghan-born Zazi and terrorists late in the summer of 2008, when he flew to Peshawar, Pakistan, a notorious terrorist haven. In September 2009, Zazi traveled to New York, where FBI agents and police detectives on the New York JTTF worked together to covertly monitor Zazi's activities. Press reports indicate that they used wiretaps, surveillance, and a secret court-ordered search to track Zazi and several of his associates. The Colorado Information Analysis Center ("CIAC"), a local fusion center created in response to 9/11, apparently provided analytic support to the Denver FBI and DHS after suspicious activity was reported to the CIAC through its website and 1-800 number.[8] In mid-September, the FBI arrested Zazi after he allegedly tried to build bombs with large quantities of hydrogen peroxide purchased at beauty shops in the Denver area. It is reported that Zazi, a U.S. citizen, had been trained in weapons and explosives in Pakistan and had made nine pages of handwritten notes on how to make and handle bombs. On February 22, 2010, Zazi pled guilty to terrorism charges. Although there were reportedly some internal disputes regarding the timing of Zazi's arrest, his movements were carefully monitored by several agencies, culminating in his arrest and conviction. John Brennan has praised Zazi's arrest as "represent[ing] the coordinated work of countless intelligence, homeland security and law enforcement personnel who have saved countless American lives."[9]

3) On May 1, 2010, because of improved watchlisting procedures, Faisal Shahzad was successfully apprehended after his attempt to detonate a car bomb in New York's Times Square. On May 3 — 53 hours and 20 minutes after he left Broadway — federal agents pulled him off of a Dubai-bound flight at JFK Airport, capturing him minutes before he could flee the country. This success was the direct result of improved use of the No Fly List. Although the watchlisting process is not perfect, the time line of events provided by the Terrorist Screening Center demonstrates how improved government watchlists can facilitate the rapid spread of critical information to intelligence and law enforcement agencies as well as private entities. After identifying Shahzad as

[7] Dennis C. Blair, Op-Ed, *Strengthening Our Nation's Front Line of Defense*, Wash. Post, Dec. 18, 2009.

[8] Department of Homeland Security, Fusion Center Success Stories: Fusion Center Supports Zazi Investigation, http://www.dhs.gov/files/programs/gc_1296488620700.shtm#8.

[9] John Brennan, Assistant to the President for Homeland Security and Counterterrorism, Remarks at CSIS: Securing the Homeland by Renewing American Strength, Resilience and Values (May 26, 2010).

the primary suspect in the attempted bombing, the FBI requested that Shahzad be nominated to the No Fly List at 11:40 a.m. on May 3. Within 24 minutes of this request he had been nominated to the No Fly List, and within 45 minutes the Transportation Security Administration was informed of his updated No Fly status. After another 47 minutes, all relevant federal agencies and all airlines were notified of the expedited update to the No Fly List. At 6:27 p.m., Shahzad made a phone reservation. Between 10:30 and 11:00 p.m., Customs and Border Patrol conducted a review of the final flight manifest for Shahzad's flight and identified Shahzad (the airline had run its last check against a list from the morning). At 11:02 p.m., Shahzad was removed from the flight and subsequently arrested. Although coordination between the government and the airlines was not perfect, the watchlist was still an effective information sharing tool because redundant checks were in place to ensure that the plane was not able to take off.

## III. Where We Fall Short: *The Task Remains Enormous*

**Now is not the time to declare victory.** Today, our nation faces diverse threats. While the post-9/11 virtual reorganization has transformed our government and prepared us to face yesterday's terrorist threat, the recent arrest of Rezwan Ferdaus for plotting to attack the Pentagon with explosive-laden model airplanes and the tragedy this summer in Norway demonstrate that the threats we face have also transformed. Although al-Qaeda has been weakened by U.S. efforts overseas, the threats we face have become harder to detect. They are also closer to home because our enemy is more loosely coordinated and is less dependent on training camps in Afghanistan and Pakistan. For example, al-Qaeda offshoots have taken advantage of the Internet in an attempt to radicalize "lone wolves" in the U.S., including, according to press reports, well educated U.S. citizens such as Rezwan Ferdaus.

Much of the Intelligence Community and many in other agencies charged with national security have embraced the objective of collaborating across agency lines and sharing more information with those who need it to fulfill their mission. However, the February 2011 Government Accountability Office ("GAO") report on "high risk" government programs noted, "The government has continued to make progress during the past two years in sharing terrorism-related information among its many security partners, but does not yet have a fully-functioning Information Sharing Environment in place."[10] Implementation of information sharing programs has been uneven across agencies and has not been driven by a government-wide vision of the authorities and constraints necessary to build an effective and trusted information sharing environment.

An essential element of an information sharing environment is that prior to making information available to a wide community, the government should have regulations and processes for controlling access to and use of shared information.

**Our ability to thwart the next Times Square bomber or another attack like Christmas Day, 2009 still depends too much on luck.** Although substantial progress has been made over the past ten years, much still remains to be done, as reflected in recent reports by the GAO and the Congressional Research Service, which cite continued bureaucratic resistance in some agencies and call for developing a vision and roadmap for the future of information sharing.[11]

The government has successfully increased the free flow of information, but, as WikiLeaks' disclosure of hundreds of thousands of the State Department's diplomatic cables demonstrates, that increased information sharing has not always been implemented responsibly. Appropriate policies and technologies to limit the risk of unauthorized disclosure of sensitive information should have been in

[10] GAO, "High Risk Series: An Update," (Feb. 2011), p. 96, available at http://www.gao.gov/new.items/d11278.pdf (last visited 1 March 2011).

[11] GAO, "Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investment," (July 2011), available at http://www.gao.gov/products/GAO-11-455 (last visited 7 Oct. 2011); Congressional Research Service, "Intelligence Issues for Congress," (Sep. 21, 2011), available at http://www.fas.org/sgp/crs/intel/RL33539.pdf

place prior to making the leaked information accessible to a wide community, as described in detail below.

Addressing these challenges requires the focus to be on people and policies that build trust, not just technical standards for how to exchange more information. Progress in counterterrorism must continue to ensure that information can be located by analysts who need it, regardless of which agency has it.

## IV. Where We Should be Going: *Recommendations and Next Steps*

Information sharing is a means, not an end. The ultimate goal is to change dramatically the way people in government work together across agencies by using technology and the best management know-how to direct human attention to the most pressing issues to facilitate collaboration and improve our ability to develop and act on intelligence. It is critical that in so doing, we protect traditional civil liberties. Done correctly, this can help address the problem of information overload and prevent future leaks while ensuring that decision-makers have timely access to the information they need to make better informed choices.

Four steps are critical to achieving this goal.

**1. Strong leadership from the highest levels of government is required to sustain the progress made since 9/11 and drive our government to continue evolving to confront emerging 21st century challenges.** The "virtual reorganization" on which our government embarked after 9/11 faces constant resistance. There is risk that it will be eroded as a result of bureaucratic turf battles and fears about information security. The leadership in Congress and the executive branch should persistently emphasize that the failure to share information is at least as dangerous as the risk that greater sharing might lead to disclosure of sensitive data. This Committee in particular has a critical oversight role to play. Continuing to hold hearings like this, supporting change, passing needed legislation — and providing adequate funds — are essential to ensure that these issues remain a top priority and that progress continues.

**2. People with a valid mission must be able to discover that relevant information exists and access it under an authorized use standard.**

An effective system for information sharing will make it possible for relevant data to be discovered in an automated manner, allowing both users and the data itself to find relevant information. This enables "data to find data," like an automated triage that helps direct human attention to the most pressing issues. When data finds data, people are no longer required to dream up every smart question because "relevance finds the user" – for example, through automatic alerts. To achieve this, data should be tagged with standardized information that can be indexed and searched.

A concept of authorized use also should be adopted. It provides a standard to determine whether a user is authorized to see what he or she has discovered. Like a library card catalogue that offers information on books, but not the books themselves, discoverability offers users the ability to discover select values (*e.g.*, who, what, where, when) without gaining access to the underlying data until they are granted permission based on a predicated purpose under the authorized use standard. This authorized use standard would overcome obstacles in the present system of classification by permitting an agency or its employees to obtain information based on their role, mission, and a predicated purpose.

An important Intelligence Community Directive, ICD 501, was issued in 2009 that represents a substantial step toward discoverability and authorized use. ICD 501 requires IC agencies to make all information collected and all analysis produced available for discovery by automated means. It also creates a "responsibility to provide." It includes elements of the authorized use standard as well. ICD 501 is being implemented throughout the Intelligence Community, but progress has been slow and much of the early implementation has focused on discovery of published reports. The implementation of ICD 501 should be accelerated and future efforts should extend to discovery of the underlying data, which is provided for under the Directive's existing language. The policies in ICD 501 should also be expanded to apply to relevant agencies outside the IC.

Development of tools like discoverability and authorized use can help solve the current problem of information overload. In the case of the "Underwear Bomber's" nearly successful Christmas Day attack on Flight 253, the key information was available to a number of agencies, but was buried among hundreds of seemingly more dangerous leads. Markle's concept of "data finding data" could have helped make a connection that might have raised this threat out of the "background noise." For instance, when the embassy report from Umar Farouk Abdulmutallab's father was entered into the centralized TIDE database on terrorist identities, this new information should have been automatically linked to the fact that Abdulmutallab had been approved for a visa. An automatic e-mail alert could have brought this connection to the attention of the State Department adjudicator who granted that visa, which would likely have been revoked.

**3. As new and more powerful ways of sharing information are developed, both privacy and security protections must be increased simultaneously in order to keep pace.**

WikiLeaks is not an argument for less information sharing. Doing that would compromise our national security. The lesson from incidents like the WikiLeaks breach is that as we improve our capabilities to better share information, we should simultaneously deploy better policies and technologies to control its access and use. Security mechanisms, such as active audits that monitor behavioral changes and immutable audit logs, should be implemented along with dynamic permissioning and granular access controls, like the authorized use standard discussed above.

We should also increase privacy and civil liberties protections. While the development of robust privacy offices within key agencies like the DNI and the Department of Homeland Security represents significant progress, critical oversight mechanisms must also be established and supported. More detailed government-wide privacy policies that address the hard questions are necessary as well, as opposed to existing policies that state that agencies must comply with the law without providing guidance on how to do so.

These policies should address the new challenges posed by the evolving terrorist threat, such as al-Qaeda's increased use of U.S. citizens like Rezwan Ferdaus, who planned to use model aircraft filled with C-4 to attack targets in D.C., or Faisal Shahzad, the Times Square car bomber who was reportedly in contact with Anwar al-Awlaki, the radical U.S. citizen cleric in Yemen who was recently killed in a drone strike. Such policies must clearly address treatment of U.S. Person information, other persistent questions about secondary use and redress, and the emerging questions posed by the collection of vast amounts of data in the private sector. The government should also find ways to publicly discuss the legal authorities associated with data collection, sharing, and use as well in order to ensure public trust in the policies and adequate oversight.

Increasing both privacy and security protections will help build trust on two fronts. First, such protections will help the American people trust that the government is protecting their civil liberties. Second, they will help people within government trust each other when information is shared, confident that such activities are both secure and legal. Such a system of checks and balances builds trust that information is used in accordance with our nation's core values, enables greater public-private cooperation, and pushes decision making and initiative to the edges of the system — to local police, for example — where threats are most likely to be seen.

**4. Information sharing is a tool that can help make the entire government more efficient.** The issues associated with the trusted use of information in government decision-making are not unique to counterterrorism. Information sharing best practices can help decision-makers in all areas of government by giving them timely access to better information so they can make more informed choices.

Changing how people work together and use technology can make the whole of government more effective, as it has for many private sector businesses. In light of the very real fiscal constraints that our government faces today, we need to do more with less in many areas of national security including cybersecurity, counter proliferation, chemical and biological threats, and energy security. The answer is not spending more money to create new institutions, like the host of fusion centers created after 9/11.

Instead, the focus should be on changing the culture within agencies through new business processes and technologies that empower trust and collaboration. Informal and flexible groups from different parts of government and the private sector should be able to work together on the full range of crosscutting issues to share expertise — as they do for counterterrorism. This flexible new way of working can empower people at the edges of agencies because information and requests for authorization no longer need to work their way up the chain of command as they do in government's traditional hierarchy.

The "virtual reorganization" that started after 9/11 has not been easy, but it demonstrates how much more effective our government can be when new ways of doing business allow people to collaborate horizontally across agencies and use information in new and more powerful ways. This transformation we are seeing in counterterrorism is built upon principles and practices that can be extended to other key homeland security priorities so that our government can work in a more modern, decentralized, public-private manner to address growing challenges like cybersecurity and economic security. The Obama Administration has already undertaken efforts to identify crosscutting areas in the President's budget where new management constructs can help leverage existing resources. Congress should work with the Administration through the budget process to increase efficiency by increasing the flow of information and empowering people who are closest to the facts on the ground to quickly form teams that draw on experts with different backgrounds in government, academia, and the private sector. This will provide decision-makers access to better information so they can make more informed choices, and this more agile decision making will save money.

***

We thank Chairman Lieberman, Senator Collins and the Committee for your leadership on these important issues.