FEDERAL SUPPORT FOR HOMELAND SECURITY INFORMATION SHARING: ROLE OF THE INFORMATION SHARING PROGRAM MANAGER

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

NOVEMBER 8, 2005

Serial No. 109–55

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
35–718 PDF WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

ROB SIMMONS, Connecticut, *Chairman*

CURT WELDON, Pennsylvania
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
STEVAN PEARCE, New Mexico
BOBBY JINDAL, Louisiana
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
PETER T. KING, NEW YORK *(Ex Officio)*
ZOE LOFGREN, California
LORETTA SANCHEZ, California
JANE HARMAN, California
NITA M. LOWEY, New York
SHEILA JACKSON-LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

FEDERAL SUPPORT FOR HOMELAND SECURITY: ROLE OF THE INFORMATION SHARING PROGRAM MANAGER

Tuesday, November 8, 2005

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT,
Washington, DC.

The subcommittee met, pursuant to call, at 2:04 p.m., in Room 311, Cannon House Office Building, Hon. Rob Simmons [chairman of the subcommittee] presiding.

Present: Representatives Simmons, Weldon, Dent, Lofgren, Lowey, Jackson-Lee, and Langevin.

Mr. SIMMONS. [Presiding.] The Committee on Homeland Security's Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment will come to order.

The subcommittee is meeting today to hear testimony on the state of homeland security information sharing to review the progress of the federal government's information sharing efforts and to explore the relationship between the Information Sharing Program Manager and the Department of Homeland Security's Chief Intelligence Officer.

We will hear from two panels today. Our first witness will be Mr. John Russack, Information Sharing Program Manager in the Office of the Director of National Intelligence.

Our second panel of witnesses will be the Honorable Lee Hamilton, vice chairman of the 9/11 Public Discourse Project, and Mr. William Crowell, from the Markle Foundation's Task Force on National Security in the Information age. And I thank them all for being here today.

Prior to being named Information Sharing Program Manager, our first witness, John Russack, was previously the Energy Department's intelligence director and served as deputy chief of external operations and cover division for counterintelligence. He was the deputy assistant director of central intelligence for collection, was the military deputy director of the DCI's Nonproliferation Center and was deputy to the associate director of central intelligence for military support. In other words, he is a seasoned intelligence professional who brings years of experience to the job.

Preventing future terrorist attacks must be the primary goal of our homeland security efforts, and the ability to share relevant terrorist-related information is key to prevention. The Information

Sharing Program Manager is the designated individual responsible for information sharing across the federal government and was given government-wide authority to ensure that all government agencies at the federal, state, local, tribal levels, as well as the private sector, share information about terrorists and terrorism.

The Program Manager, in consultation wit the Information Sharing Council, is responsible for developing, monitoring and managing the information sharing environment, or ISE, which will provide the means for sharing terrorism information among all appropriate federal, state, local and tribal entities, as well as the private sector.

Establishing an information sharing environment is a difficult and complex undertaking and will require a concerted effort at all levels of government.

We look forward to hearing your views on the current status of your efforts and your thoughts about the road ahead. I am especially interested in how your relationship with the Department of Homeland Security's Chief Intelligence Officer is progressing and whether or not you feel that you have the resources that you need and the authority that you need to get the job done.

The chair now recognizes the ranking minority member, the gentlelady of California, Ms. Lofgren, for any comments she might make.

Ms. LOFGREN. Thank you, Mr. Chairman, and I will put my full statement into the record. But I do want to celebrate the fact that we are having this hearing. Probably, as I think about it, we should have had this hearing maybe before the last hearing we had since we need to understand the ISE, which is central to any effective government-wide information sharing effort.

As the Markle Foundation has noted, the ISE should not be limited to promoting communications between the various agencies that comprise the intelligence community. We have all the shared intelligence in the world. If we don't get it out to the state, local and tribal law enforcements, we are not going to achieve our goal. And I am pleased that I believe that Mr. Russack certainly understands that, and it is our job here to try and assist him in getting that accomplished.

I would note that we are way behind in what we need to do. I am very concerned that Mr. Russack's office is not yet properly funded or properly staffed. I think if we are going to ask him to lead the tough job that we have given to him, that we need to make sure he has the budgetary support to accomplish the task.

I also want to note that four years after 9/11 and more than a year after the issuance of the 9/11 Commission report, we are aware that federal departments and agencies are still using arguments based on interpretation of their authority prior to the Intelligence Reform Act to protect their turf. We need to work with our administrative leadership to correct this situation. I think this hearing is a part of that effort but certainly not all that will be asked of us.

And I yield back and will submit the rest of my statement for the record.

PREPARED OPENING STATEMENT OF HON. ZOE LOFGREN

Good afternoon. I, too, am very pleased that this Subcommittee is turning its attention to the critical issue of government-wide information sharing. I would like to extend a warm welcome to Mr. Russack, who I had the opportunity to meet last week, as well as Bill Crowell of the Markle Foundation and Lee Hamilton, former Vice Chairman of the 9/11 Commission.

This hearing builds upon our July information sharing hearing when we explored how well federal agencies were communicating with state, local, and tribal law enforcement authorities and the private sector.

This hearing, by contrast, will focus on how well federal agencies are communicating with each other.

For several reasons, this hearing probably should have happened first.

The Information Sharing Environment (ISE)—initiated as part of last year's Intelligence Reform Act—is central to any effective government-wide information sharing effort. Accordingly, the ISE is an important starting point—in fact, THE starting point—for any coordinated information sharing effort involving the federal government.

As the Markle Foundation has noted, however, the ISE should not be limited to promoting communications between the various agencies that comprise the Intelligence Community. On the contrary, all the shared intelligence in the world is not worth a thing if it is not disseminated to those who can actually use it—namely, the men and women of state, local, and tribal law enforcement who are most likely to encounter terrorists in the communities they protect and serve.

An ISE that incorporates not only the federal Intelligence Community but also our hometown law enforcement authorities holds great promise.

In many respects, this is old news. What we need now is action.

I am saddened to report that while the establishment of the ISE is a step in the right direction, its implementation continues to be plagued by inaction and a lack of cooperation.

How can we expect to have an effective, fully functional ISE if we haven't properly funded or staffed Mr. Russack's office? Indeed, how can Mr. Russack do his job if he doesn't have a budget?

Mr. Russack testified this summer that he had been staffed with only one full-time employee and two contractors to assist him with his work. Indeed, the Markle Foundation recently reported that Mr. Russack's office still needs more full time employee positions and still has key leadership positions open.

While I know from Mr. Russack that he is diligently attempting to fill those spaces, a dedicated funding stream for his office will go a long way to attracting the best and brightest minds to his effort.

At the same time, if we don't foster a greater sense of urgency in terms of implementing and operationalizing the ISE, how can we effectively thwart terrorist plans that are being developed by our enemies?

I note that it was only two weeks ago that the President actually issued Executive Order 13388 establishing the Information Sharing Council—an entity that is supposed to bring all intelligence agencies to the table to work out their differences. The Council is getting started 11 months after Congress provided for its creation and six months after Mr. Russack was appointed.

I question how much they can realistically accomplish together during the 18 months remaining in their terms.

Moreover, if the various agencies that comprise the Intelligence Community can't or won't agree on how to share information with each other as part of the ISE, how can we expect them to communicate homeland-security information with law enforcement officers in the field? Likewise, if the Intelligence Community resists the efforts of the Program Manager to create an ISE that requires compliance with a common set of rules and regulations for information sharing, how can we assure those officers that they will receive a consistent, coherent message from their federal partners?

The Markle Foundation recently reported that four years after 9/11 and more than a year after the issuance of the 9/11 Commission's report, federal departments and agencies are still using arguments from interpretations of their authority prior to the Intelligence Reform Act to protect their turf.

Finally, even if Mr. Russack succeeds in developing rules and procedures designed to ensure effective information sharing, what good will they be if—at the end of the day—they can't be enforced?

Although the Director of National Intelligence has assumed administrative responsibility for the Program Manager, he must also assume responsibility for the success of Mr. Russack's office. That success will manifest itself only when we have

a clear and consistent information sharing policies and procedures that apply to all intelligence consumers as well as clear and decisive consequences—financial or otherwise—for noncompliance.

These are all critical questions that I hope the witnesses will address and the Members present here today will explore. I look forward to all of the testimony today.

Mr. SIMMONS. I thank the ranking member for her statement. I state, for the record, that all members of the subcommittee or the members of the committee who attend can insert opening statements for the record.

PREPARED OPENING OF HON. BENNIE G. THOMPSON

I am very pleased that this Subcommittee is turning its attention to the issue of government-wide information sharing, and more specifically, the progress that is being made—or not being made—with the development of the Information Sharing Environment (ISE).

Congress initiated the ISE last year as part of the Intelligence Reform and Terrorism Prevention Act.

The ISE was intended it to be a decentralized, distributed, and coordinated system for sharing terrorism information among intelligence and law enforcement agencies at all levels of government.

In its hoped-for state, the ISE will be a combination of policies, procedures, and technologies linking people, systems, databases, and information across government and the private sector in order combat terrorism more effectively.

Congress intended the ISE to achieve this function in a way that not only promotes national security but also respects privacy and civil liberties.

Things are moving on all these fronts—but slowly.

To get to where we need to be, we must have everybody on the same page.

Put simply, our intelligence agencies, law enforcement entities, and the private sector must operate under a common set of guidelines and policies for acquiring, accessing, sharing, and using information.

The Intelligence Community, moreover, must be answerable to a single authority to coordinate this effort.

That is where our first witness—Mr. John Russack, the Program Manager of the Information Sharing Environment—comes in.

As former 9/11 Co-Chairman Lee Hamilton recently stated, "The place where it all comes together is in Mr. Russack's position. . . . He's the fellow that has to see that we get all this information shared. And if you don't . . . you are not going to have the most effective means of fighting terrorism."

Several things are for certain. Mr. Russack won't be effective if he doesn't have the resources he needs;

He won't be effective if he doesn't have the cooperation from the Intelligence Community he needs;

And he won't be effective if he doesn't have "buy in" from all participants.

The Markle Foundation recently warned the President that "risk aversion and bureaucratic resistance to change continue to hamper the carrying out of the Information Sharing Environment and the policies that support it."

I therefore look forward to Mr. Russack's testimony and that of our second panel witnesses—including Mr. Hamilton and Mr. Bill Crowell of the Markle Foundation Task Force on National Security in the Information Age.

I am certain that Mr. Russack, Mr. Hamilton, and Mr. Crowell all have unique perspectives on the Markle Foundation's concerns as well as other challenges in this critical area.

Thank you all for joining us today.

Mr. SIMMONS. I now would like to welcome Mr. Russack to the subcommittee to remind him that his entire statement will be introduced into the record and that if he is able to limit his oral testimony to around 5 minutes, that will leave an opportunity for questions.

Mr. Russack, thank you for being here.

STATEMENT OF JOHN RUSSACK, INFORMATION SHARING PROGRAM MANAGER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. RUSSACK. Thank you, Mr. Chairman. Thank you, Ms. Lofgren. It is a pleasure to be here.

I would, first of all, like to state that I agree with everything the chairman and the ranking minority member have said about the importance of information sharing to national security. I would also like to say that I care. When I was asked if I would consider doing this job, I said, "Yes," and the reason I said, "Yes," is because I believe that information sharing in our nation—and, again, I emphasize the fact that this is a national issue, it is not a federal issue, it is not a state and local issue, it is everybody's issue—information sharing in our nation is seminally the most important thing we can do to ensure our national security.

And what I intend to do is execute the tasks that the Congress has laid out for me in the Intelligence Reform and Terrorism Prevention Act. We have already turned in a deliverable. That was due to the Congress on the 15th of June. In that, I talked about the impediments to information sharing, and I would like to point out at the onset that technology is not an impediment.

Oftentimes, people tend to talk about information sharing in terms of technology or chief information officers, and many would draw the conclusion that these are technological issues, not that aren't technological issues because there are, but technology is an enabler. It is not an impediment.

Most of the time, there are technical solutions to solve many problems. Once we have identified problems in policy, law, culture in the business model and once we define the business rules, technologically, we can build a system that will in fact enable us to share information.

So I care deeply about this issue. The intention of myself and my staff is to in fact make the existing information sharing environment better. Depending upon where you sit or where you stand and what you do, the scorecard for today's information sharing system would be, if we took a positive side, flawed, doesn't work perfectly. And if we took the negative side, some would argue that it doesn't work at all.

I think post-9/11, across the federal government, we in fact are sharing information. It is not a perfect sharing. We need to do much better. We need to make sharing much more robust, and I think we need to redefine the business rules. I think an awful lot of the problems have to do with roles, missions, responsibilities and authorities in terrorism. If I look at the state, local, tribal and private sector, I think that is where we really need to do a much better job.

And when I talk to people at the state, local, tribal and private sector, people representing those sectors, most of them are unhappy with the quality of information sharing. And I think if we are going to protect America, we need to do better at the federal level, and, clearly, we must do a whole lot better when we deal with state, local, tribal and the private sector.

Protection of sources and methods is an issue; however, clearly, we can share information in a better way, in a much more effective

way, and we can add context and perspective to the information we give to state, local, tribal and the private sector.

We also need to do business specifically for state, local, tribal and the private sector and across our nation. We need to do more business at the unclassified level.

Today, in the 21st century, there are many, many sources of information beyond intelligence. Most large companies and businesses that I know of have their own intelligence organizations. Where do they get their information—Open source.

There is an awful lot of information that is out there at the open source level. If we take that information and combine the information derived from national, technical means, the classified stuff, we ought to be able to do a good job, a great job, a much more adequate job of protecting America.

Thank you.

[The statement of Mr. Russack follows:]

PREPARED STATEMENT OF JOHN A. RUSSACK

INTRODUCTION

Chairman Simmons, Ranking Member Lofgren, and distinguished members of the subcommittee, I consider it an honor to be here today to update you on my efforts to implement the recommendations that Congress prescribed in section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. We need not look far to the tragic events of September 11, 2001, to understand that we have significant work remaining to fully implement an information-sharing environment that more effectively supports our national counterterrorism mission. I believe there is not an issue more seminal to the security of our nation than information sharing. I accepted this responsibility because I am committed to doing something about it. This task is too large and much too important for me to do it alone, which is why Congress must remain fully engaged in this effort and provide its leadership, support, and necessary guidance to transform our current capabilities into a better, more effective Information Sharing Environment (ISE).

In August of 2004, the President issued Executive Order 13356 to ensure that terrorism information is shared broadly among federal agencies; state, local, and tribal governments; and the private sector. Then in response to the IRTP A, on April 15, 2005, the President designatedme as the Program Manger (PM) for the Information Sharing Environment, and on June 2nd, the President directed that the PM be part of the Office of the Director of National Intelligence (ODNI).

On June 15th, I submitted a preliminary report to the President and Congressthe first deliverable mandated by IRTP A. This report identified five broad issues affecting information sharing that will largely define the agenda for my office over the next two years. On October 25th, the President issued EO 13388 establishing the Information Sharing Council (ISC), and I now have an approved charter authorizing the ISC to assist and advise the President and myself in carrying out our duties as described in section 1016 of IRTPA. On October 27th, Ambassador Negroponte sent a letter to Department Secretaries and Agency Directors requesting representatives to the ISC. While the institutional foundations are in place to allow us to make significant progress in the way we share terrorism information, a number of hurdles that exist that will require hard work and leadership to surmount. Weare committed to identifying and removing all impediments that prevent us from providing the best possible information to decision makers, at whatever level.

In fact, significant efforts have been made to meet Congress' intent in making information sharing a priority. In consultation with the ISC, and state, local, and private sector representatives, I will formulate policies and guidelines to enable broader sharing of terrorist information, develop an ISE concept of operations and architecture, and prepare for the President an implementation plan for the Information Sharing Environment. Once the plan is adopted, my office will manage, support, monitor, and assess ISE implementation by Federal departments and agencies, and regularly report my findings to Congress.

I have organized my office around three major priorities: policy, technology, and business process, and I have recruited and staffed senior positions for each of these key areas. My office is currently staffed with 11 Federal employees, with eight more in the hiring process; we are further augmented with six on site contractors. The

quality of personnel now onboard is outstanding, and is representative of all of the agencies and departments of the Federal govemment--not just the Intelligence Community (IC). I am on track to obtain additional Federal Government employees and achieve our established personnel goal of twenty-five.

The following are representative accomplishments associated with the stand-up of my office:

- I distributed a Request For Information (RFI) to industry on August 18, 2005, to develop an Electronic Directory Service (EDS) or the functional equivalent required by section 1016(b) of the IRTPA. Forty-eight responses were received from potential developers, and are now being analyzed. These inputs may provide the basis for a Request for Proposal (RFP).
- The Institute for Defense Analyses (IDA) has been under contract to my office since July 2005 to perform a comprehensive review of the existing ISE. The resulting December 2005 report will serve as a key point of departure for implementing the ISE.
- In October, I established three ISE steering groups: (1) Information Access, Search, and Exploitation; (2) ISE Governance and Collaboration; and (3) Security and Privacy. The ISC and I will look to these groups to be the primary focal points for integrating all work in their respective issue areas. The steering groups will leverage and track ongoing work to avoid duplication, integrate results, and report progress to myself and the ISC. In addition, they will identify any issues not being addressed, assign priorities, and propose options for resolving them.
- My office is engaged in identifying a number of promising information sharing technology pilot programs, including two particularly promising projects—one with the New York Federal Bureau of Investigation (FBI) Field Office on a Sensitive But Unclassified (SBU) technology demonstration; the other a project with our Department of Energy (DOE) national laboratories, to leverage both analytic and technical expertise to counter the potential for nuclear terrorism.

ROLE OF THE PROGRAM MANAGER

The ISE will be a national information-sharing environment enabling frictionless terrorism information access. It is a combination of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of Federal, state, local, and tribal entities and the private sector to facilitate information sharing, access, and collaboration among users to combat terrorism more effectively.

The IRTP A required the President to designate a program manager (PM) "responsible for information sharing across the Federal Government," with government-wide authority. Section 1016(f) outlines the duties and responsibilities that were assigned to me as the Program Manager:

- Plan for and oversee the implementation of, and manage, the Information Sharing Environment;
- Assist in the development of policies, procedures, guidelines, rules and standards as appropriate to foster the development and proper operation of the Information Sharing Environment; and
- Assist, monitor, and assess the implementation of the Information Sharing Environment by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance; and regularly report the findings to Congress.

Since September 11, 2001, significant progress has been made to improve the Nation's ability to access, integrate, and share terrorism-related information. Legislative changes and executive orders have reduced some of the barriers to sharing. New organizations such as the National Counterterrorism Center (NCTC), the Department of Homeland Security (DHS), the Terrorist Screening Center (TSC), and state and local intelligence fusion centers have bolstered our national effort to collect, analyze, and disseminate information. My office will build on these collective capabilities. The ISE that exists today must be more robust and interconnected to ensure our national security. Policies, rules, architectures and systems, which support specific individual missions, must be adjusted to enhance frictionless, rapid information access. One of the functions of my office will be to coordinate these individual efforts so that they are uniformly directed towards a single collective effort to share information throughout the mission space.

The ISE of the future must transform, integrate and connect existing elements into a cohesive framework by providing common polices, guidelines, systems, and architecture. Leveraging existing initiatives will be critical to getting this task done in an expedited manner. The challenge herein is that terrorism information is not limited to intelligence. The counterterrorism mission will require the integration of information from homeland security, private sector, law enforcement, financial, and

bio-surveillance, to name a few. Each of these classes of information possesses its own unique legal requirements, business rules, technical architectures, standards, and capabilities. Therefore, coordinating this effort will be a critical function of my office.

Creating an ISE that effectively facilitates the flow of information across agency, jurisdictional, and domain boundaries must be enabled by technology. It is key to note that technology is not the solution but an enabler, and technologies currently exist to meet this challenge. Rewriting the business rules for this new ISE will require that we address all the impediments to sharing—policy, culture, and roles, missions and responsibilities. Critical to this effort is leadership. One of my roles is that of a catalyst in implementing the ISE, creating the conditions necessary to optimize information sharing. Ultimately Federal agencies and all of our non-federal partners will each have to share the responsibility and provide the necessary leadership to make the ISE we need. The success of this effort will be directly related to the commitment that each agency makes to change its culture from the need-to-protect to the need-to-share.

STATE, LOCAL. TRIBAL GOVERNMENT AND THE PRIVATE SECTOR

We must better support the key new partners in our counterterrorism efforts: the state, local, and tribal governments, and private sector. I intend to fully support the efforts currently underway at the Department of Homeland Security, the Department of Justice (DOJ), and the Department of Defense (DaD) to provide actionable information to their customers.

The current federal system (processes, protocols and technology capabilities) that supports the sharing of terrorism-related information and intelligence between Federal, state, local, and tribal governments, and the private sector is not cohesive and has led to the development of an ad-hoc patchwork of informal and formal networks to facilitate the sharing of information among local partners. These "networks" include a variety of organizational structures and processes for gathering, analyzing, and sharing terrorism-related information and intelligence. Most states have begun to establish statewide intelligence fusion centers to serve as central hubs to facilitate statewide efforts to gather and analyze terrorism-related information, blend it together, and then produce and disseminate intelligence products used to support homeland security related prevention, response and recovery activities (operational and planning).

I recognize that statewide and major urban area information fusion centers have the potential to be a critical part of the ISE. Thirty states have information "fusion" centers and 11 more are being developed. Identifying best practices with regard to establishing a fusion capacity within the state and local information-sharing environment will significantly contribute to the ISE implementation. I further support the efforts by the DHS, DOJ, and other relevant Federal entities to coordinate their domestic information and intelligence efforts with these fusion centers.

Effectively engaging state, local, tribal, and private sector authorities in the ISE development process will require overcoming significant frustration by local entities over the perceived "lack of progress" in establishing a national terrorism information sharing system. I know that Members regularly hear from their local law enforcement entities, first responder groups, and the private sector on the continuing lack of coordination among federal entities. We must work together more seamlessly at the Federal level in order to better leverage the capabilities that the state, local, and tribal entities bring to the counterterrorism effort.

Our ISE planning efforts will take into account that:

- Counterterrorism-related prevention, response and recovery efforts carried out at the state, local, and tribal levels must be integrated into their "all-crimes, all-hazards" approach to homeland security;
- In addition to supporting investigations, terrorism-related intelligence is used at the state, local, and tribal levels to support a broad array of activities, including: completion of jurisdictional risk assessments; allocation of fiscal resources; response and recovery planning efforts; and critical infrastructure protection; and
- State, local, tribal, and private sector authorities need more unclassified information and intelligence, and the traditional Federal emphasis on producing and disseminating classified information impedes the effective use of that information to support multi-disciplinary prevention, response, and recovery efforts.

Another important initiative that I will continue to expand is the use of information access pilot programs at the state and local levels. We currently have two pilot programs that involve the FBI and DOE. The FBI New York Office's Special Operations Division currently utilizes handheld wireless devices for field operations. In

addition to emails and alerts, the devices can be used to access various databases. The objective of the FBI pilot project is to facilitate enhanced communications among counterterrorism personnel and provide rapid wireless access to SBU data sources. The DOE is sponsoring a pilot project that will apply technical analytic expertise to intelligence pertaining to nuclear terrorism. The project has established a core group of nuclear expert analysts across five DOE national laboratories, focused on providing both long-term, strategic analysis of the supply-side of nuclear terrorism and better short-term tactical intelligence, with an additional objective of improving potential collection opportunities. Central to the success of this effort is the sharing of all relevant sensitive reporting with these national laboratories. Pilot programs provide valuable end-user input to the technical development of the ISE, and significant buy-in that will be crucial for cultural change in the information-sharing environment.

ELECTRONIC DIRECTORY SERVICES

I am required to provide an electronic directory service (EDS) or a functional equivalent that meets the requirements and objectives of the IRTP A, based on a community-wide, enterprise architecture, to focus on a broad range of threats. The EDS must accommodate increasing numbers of sources, and be implemented utilizing existing technologies and ongoing EDS and collaboration efforts. The EDS will provide a set of capabilities to inform ISE users of the resources available for collaboration, including professionals from across the IC, Federal, state and local governments, as well as private industry, academia and allied countries. Capabilities, such as people and organizational information, will be made available on a realtime basis to all ISE users, employing traditional search and drill-down functionality.

The EDS implementation will be achieved through a three-phased approach. The first phase will start small by leveraging existing IC counterterrorism directory services such as Intelligence Community Full Service Directory (IC FSD) and the National Counterterrorism Center Online (NOL) directory.

The second phase will include people/organization listings from Federal organizations such as use of capabilities of the Department of Justice—Global Justice Information Sharing Initiative, Regional Data Exchange (R–DEx), Law Enforcement Online (LEO), the Regional Information Sharing System (RISS) and the Department of Homeland Security—Transportation Security Administration Operating Platform.

The third phase will include state/local governments, private sector, academia and Allied countries. The use of capabilities such as the Department of Homeland Security Regional Information Exchange System (HSIN), state fusion centers and New York State Directory Service (NYSDS) would provide immediate initial capability.

SUMMARY

I believe there is no higher priority for our national security than the issue of information sharing. Congress has provided us the mandate through legislation; the President has provided us the leadership and further guidelines; now we must finalize the work of transforming our information-sharing environment into one that works more effectively for all. Thousands of men and women work tirelessly to protect this nation from terrorist threats. It is important for us to provide them and other decision makers with the best possible information to do their job to protect the people and interests of the United States against another terrorist attack.

It is important to emphasize that my function in all of this is to serve as an enabler for better access and collaboration. Each department and agency with a counterterrorism mission will retain their current roles. Our collective task is to lead the effort to better clarify these roles, missions, and responsibilities, and implement an ISE that better supports their efforts.

In closing, I would like to leave you with some key priorities in establishing the Information Sharing Environment:

- It is absolutely essential that information flow in two directions. The *"environment"* we create needs to provide better access to Federal terrorism information at the state and local levels—however, and of equal importance, it must also provide mechanisms to allow valuable information gathered by state and local officials to be used by Federal agencies.
- The Intelligence Community no longer serves as the single source for information, particularly where terrorism information is involved. Customers can and do get their information elsewhere. Consumers of terrorism information demand expertise; are substance oriented; and require each of us engaged in countering terrorism to operate in a "fast forward, value added mode."
- While it's true that some in the Intelligence Community have historically regarded protection of intelligence sources and methods as more important than sharing the information, it's an impediment that must be overcome. Protection and sharing of information are not mutually exclusive. We can and will share

the information we collect and analyze, while protecting our most sensitive sources and methods.

• I recognize that there are potentially serious issues affecting privacy, civil liberties and the equities of state and local governments that will need to be addressed before we achieve the two-way flow of information. Close collaboration between officials at all levels will be essential to develop the policies and processes we need. Although some terrorism information must always be classified, our goal has to be that we provide as much as possible at the unclassified level.

• One of my responsibilities is to identify any impediments to effecti ve information sharing and to remove them. Consumers of terrorism information must receive all the information they need from us, quickly and free of unnecessary restrictions.

My office, under the leadership of the DNI, is committed to creating an effective ISE that extends beyond the Intelligence Community. This task will include the development of nationwide policies that will enable individual Federal agencies and key partners to begin to adopt practices that reflect effective information sharing capabilities and procedures. Our state, local, and tribal governments and private sector entities must be full partners in this effort

Mr. Chairman, I appreciate the opportunity to provide this subcommittee an update on the activities of the Program Manager's Office and look forward to your questions. Thank you.

Mr. SIMMONS. I thank you, Mr. Russack, for your testimony.

I would like to make note of your preliminary report on the creation of the information sharing environment. This was your first deliverable, I believe, and you list several issues in here. One is the issue of current authorities and policies, governing rules and responsibilities are in some cases ambiguous and conflicting.

But the second one intrigues me the most: Organizations do not fully trust one another when sharing information.

You served in the intelligence community, you have been part of what I call the secrecy system. I spent 10 years in the CIA and over 30 years in military intelligence. The idea of intelligence information sharing was culturally anathema. You might share information with your colleagues, you might run information up and down your stovepipe, but you certainly were very reluctant to share it across the community for several reasons. One, your source might be jeopardized; two, somebody else might take some credit for what you were doing. And so there is an issue of trust.

There is an issue of whether or not a series of little intelligence bureaucracies can see clearly the national security advantages to sharing with others in a real-time and virtual environment. And this cultural change is very, very difficult to accomplish.

How can you, as a single individual, somehow persuade this large collection of entities who up until recent years have pretty much operated on their own and without sharing, how can you break through this traditional culture and establish as a priority and a need and as a goal for everybody that we need to share this information?

Mr. RUSSACK. Mr. Chairman, let me say, first of all, that you said me, as a single individual. Clearly, me, as a single individual, I am not going to be able to affect the cultural change you describe by myself. So I am going to need the help of the president, the Congress, the executive branch, the entire legislative branch and the heads of the various departments, agencies in our federal government.

And let me take that even into a larger group. All of us that comprise our nation need to demand that people share. We need to incentivize sharing. We need to reward sharing as opposed to re-

ward protecting. It is obviously going to be iterative. We are not going to make fundamental changes in bureaucracy and culture overnight. We have to inculcate this, I think, in our training programs across the federal government and the nation, and I think only then will we be able to overcome concerns about trust.

I would also say that leaks do not help. I mean, oftentimes, or many times, the federal government does share information, and there have been several instances of sharing and requesting that that information be kept confidential or be kept at a sensitive level, and we find that information above the fold or below the fold on the front page of newspapers and transmitted, broadcast across our country by satellite dishes and the broadcast media.

So trust, I think, is key. I think you pointed that out very, very accurately. Culture has an awful lot to do with this, but we have to train people when we share information that is in fact sensitive to keep it sensitive. And, clearly, we have not done an adequate job in that area.

Mr. SIMMONS. I thank you for that answer. I have got the yellow light. Maybe we will get to a second round.

The chairman recognizes the ranking member.

Ms. LOFGREN. Thank you.

Mr. Russack, I appreciate your reaching out to the committee and your spirit of cooperation with us. I see us as your allies in your mission. And, pursuant to that, I am going to ask you a question I hope that you are able to answer, which is about the budget that you are working with.

We are asking you to implement the information sharing environment, and I want to know the budget that you are working with, from where it is sourced, and what are your needs going to be on an ongoing basis?

Mr. RUSSACK. The budget I am working with, let me go back to fiscal year 2005, and in fact let me go back to December of 2004 when the Intelligence Reform and Terrorism Prevention Act was signed. That bill says that $20 million is authorized over the next 2 years to implement the information sharing environment, or words to that effect.

In 2005, I actually received $9.6 million was appropriated for me to start standing up the office and to get going. In 2006, I do not have a budget line item. So I want to make sure I explain this correctly.

I work for the president through the director of national intelligence. The director of national intelligence is working on a budget for me. I do not have a budget line item anywhere in an appropriations bill. Before I came to this committee, I actually did my homework today before I came to this hearing, and said I know that I don't officially have any money. Obviously, I now have a staff. It is not as large as it is going to be. It is going to be a very small staff once it is stood up. But I need, to answer your question, I think, based on what I intend to do, about $30 million a year.

And to answer your question about the budget right now and fiscal year 2006, the answer is, I am working with the director of national intelligence and his staff to actually come up internal to his budget with a line item. Again, I am looking for about $30 million

to do my job. I think I am going to need $30 million a year to do a job, as a minimum.

Will I get that much money? I truly don't know. I have a feeing I am going to get at least $20 million to do my job. I don't know what the exact number will be, but between the appropriation and some reprogramming done within the DNI's authority to do reprogramming, and in fact if we add supplementals, I will be shooting to get $30 million. I would like to have a line item that had the $30 million figure in it.

Ms. LOFGREN. Well, I will just say that if you could actually accomplish the information sharing environment mission, that would be well worth the investment. It seems to me, the country would be considerably safer.

I will just ask you one quick question before I am out of time. Bill Dawson, the Deputy Intelligence Community Chief Information Officer, was quoted at an information sharing symposium last summer, not this summer but the summer before this, that the DCI had established a mandatory write to release policy and that there was going to be an enforcement mechanism that program funding would be taking away from those who didn't comply.

Are you or the DNI proposing a write to release policy that will be applicable to the entire intelligence community, and will you have that kind of enforcement that was discussed last year?

RUSSACK; Let me, first of all, address the write to release policy. There is already in effect a write to release policy. I think, DCID 8/1, and the DCID is a DCI directive. Those in fact have been renamed something else now that we have a DNI. I do not know what the new name is.

Ms. LOFGREN. Neither do I.

Mr. RUSSACK. But that directive that Bill Dawson talked about last year does in fact talk about write for release, and it does mandate that people producing intelligence write to release. So that policy is in effect. And I think people are writing for release.

But I think one of the things that we need to do within the intelligence community is remind people, educate people. Their customers are in fact not just in the intelligence community. The customer base for intelligence includes people in the state, local, tribal and the private sectors, and many of those people don't have security clearances. So, as I said in my opening statement, we need to do more business at the unclassified level.

We need to do a better job with tear lines. Tear lines we issue at the unclassified level do need to contain context and perspective. They need to contain enough information for people to make decisions to take action and to base action on to protect our country.

Your question regarding are we in fact enforcing that or penalizing in some way people who don't write for release, I would like to take that as a question for the record, and I will get back to you.

Ms. LOFGREN. All right. That is fair enough.

Thank you very much, Mr. Chairman.

Mr. SIMMONS. Thank you.

The gentleman from Pennsylvania, Mr. Dent.

Mr. DENT. Thank you, Mr. Chairman.

Mr. Russack, good afternoon. As you know, the president recently signed an executive order creating the Information Security Coun-

cil. It appears that there are no representatives of any state or local governments on this Council. Doesn't this effectively freeze out states from having any say in what they need from DHS from an intelligence standpoint?

And how can the Council effectively serve the needs of first responders and local homeland security authorities when the states and local authorities are not even invited to participate?

And you have acknowledged that we are not doing as good a job between federal down to state and local officials, so I would like you to answer those questions.

Mr. RUSSACK. Sir, the Information Sharing Council was established about 2 weeks ago, and I am sure that is what you are referring to.

Mr. DENT. Yes.

Mr. RUSSACK. I chair the Information Sharing Council, and I can assure you that we will include—there is nothing in that executive order that precludes the DNI, the director of national intelligence, from reaching out and including state, local, tribal and the private sector in that Council. It is my intention to do exactly that.

I mean, I agree with the thrust of your question. We cannot create an information sharing environment without taking into account the needs of state, local, tribal and private sector people.

My intention is, as the Information Sharing Council—by the way, the first meeting will be a week from this coming Friday—and we will, based on what the discussion items and the issues we are attacking and teeing up for resolution are, reach out and have representatives from state, local, tribal and the private sector help us frame those issues for resolution and help is frame options to solve problems.

Mr. DENT. Well, I am glad to hear you said that. I know it wasn't in the executive order, but I am glad to hear that you are going to include them. But you also acknowledged during your opening comments that many state and local authorities have complained about intelligence or information sharing. I have heard that quite loudly from some of the folks in my home state, and the complaint I often hear is that the products that are disseminated by DHS are either irrelevant or untimely or both.

What suggestions do you have to make DHS better able to suit the needs of these local authorities? Because, as you know, they are the ones who are going to be tasked with responding to assessments that DHS is supposed to be providing.

Mr. RUSSACK. Let me say, first of all, that my deputy—I am going to have two deputies. One of my deputies is here today, Sue Reingold, the lady on my far right. Sue Reingold is from the Department of Homeland Security. She will be a detailee to the Program Manager's staff. Sue comes from the state and local government portion of the Department of Homeland Security. Sue is going to help me in our task of providing state, local, tribal and the private sector with the information we need.

DHS recently selected Charles Eugene Allen, Charlie Allen, to be the assistant secretary for information analysis. I was Charlie's deputy for 2.5 years of my life. He trained me, to some degree. I hope I trained him to some degree also.

But I can assure you that the relationship between my office and the Department of Homeland Security—and we can't leave out the Department of Justice or the FBI when we talk about state, local, tribal and the private sector. We are going to be a team, and we are in fact going to do a better job.

I think all the people who head those agencies—and I mentioned Charlie Allen. I can assure you that he and I had lunch a week ago and we talked about ways in which we would in fact positively affect the way we share information with the customers you describe, and we are going to do it, sir.

Mr. DENT. Well, I am glad to hear you mention Charlie Allen. That was one of my questions, so I am glad to see that that is moving forward well.

But, finally, I just want to suggest one thing. When you do sit down with state and locals, I have some people I think who could you give some guidance as to what types of assistance that you could provide to them, how you can be more helpful to them. And I have some very good contacts. I represent a large state, Pennsylvania, and I think it would be useful to talk to those people about how you go about what you are doing here.

Mr. RUSSACK. Thank you, sir. I look forward to discussing this at greater length with you and getting those names, and I look forward to meeting with those people and finding out what their needs and working as a team to solving them.

Mr. DENT. Thank you.

Mr. RUSSACK. Thank you.

Mr. SIMMONS. The chair recognizes the distinguished lady from New York who has been a great leader in homeland security, Ms. Lowey.

Mrs. LOWEY. Thank you, and I want to thank the chairman and the ranking member for calling this hearing, because it is so important.

And as my colleagues have mentioned several times, I hear about this all the time. And we do hear that it is getting better, but it is just not good enough. So I thank you very much for your testimony.

As you said, it is clear that long-held attitudes and procedures pose a great challenge, which is probably the most understated statement we have made today. And I agree wholeheartedly with the recommendation of the 9/11 Commission with respect to providing incentives for information sharing between government agencies and state and local authorities.

It seems to me it is simply not enough to say, "We support or encourage information sharing, this is tough, it is hard to do, every department has its own procedures in place and they don't want to share." It seems, based upon all the information we have received, there needs to be a comprehensive system of carrots and sticks to ensure that it happens.

Now, according to testimony that we will hear later on in this hearing, the former 9/11 commissioners have indicated that there has been minimal progress toward implementation of this recommendation. So if you could follow up your previous comments and describe your progress toward instituting concrete incentives to encourage information sharing, I would be most appreciative.

I guess what most of us are pretty concerned about is 9/11 is in the past, we have been hearing about information sharing a long time, we have been hearing about the barriers between various officials that don't want to share information. What are you really doing about it and could you describe the progress toward that end?

Mr. RUSSACK. Certainly. Let me, first of all, say that when you ask about concrete incentives, I am going to walk backwards a little bit and say that—

Mrs. LOWEY. I would rather say, you were appointed by the president. He says, "Do it," and that should be enough for any member of the administration, "Just do it." But since that doesn't seem to happen, that is why I am talking about concrete incentives.

Mr. RUSSACK. Mr. Dent mentioned a moment ago the Information Sharing Council. I think the establishment of this Council goes a long way to actually helping us, we the nation, achieve concrete examples of what we are going to do to solve the information sharing problem.

Most of the problems, as I stated before, are not technical problems. They are roles, missions, responsibilities, authorities, problems, policies that we need to change or modify to enable the information sharing.

In June, when I testified before the Senate Judiciary Committee, I had myself and one other person on my staff. Right now, I have a dozen, and we should be up to about 25 by the end of this month. The Information Sharing Council did not exist until a week ago. That is up. The first meeting will be a week from Friday.

I can't really talk in real terms, concrete terms about what my staff has done beyond a few things. The staff has stood up the Information Sharing Council, required by law stood up. Working pilots. I am working two pilot programs right now. I would like to be working 10 or a dozen.

I have a pilot program with the FBI field office in New York City on information sharing where we are taking intelligence community information via the National Counterterrorism Center and getting sensitive but unclassified information to FBI special agents in the field. That has proven to be very, very useful and very, very valuable to them.

I have a plan to export that, not only to the FBI field office in New York City but also to the FBI field office in Washington, D.C. I would like to also get New York City police involved in this pilot program, as well as the Metropolitan Washington, D.C. police involved in that program.

That is one example of a pilot program, something tangible that we are doing. When you do a pilot like that, first of all, it is very cheap, relatively speaking; it does cost money. That is one of the things I would like to put more money into and expand that to some major cities across the country and major police departments.

But when you do a pilot like that, immediately or very quickly after you establish the pilot, you actually are seeing information being shared at a much better level, a much higher level. We are sharing information with them, we are sharing pictures on handheld devices in the field that aids in identification of individuals coming into our country.

Another pilot that we are working is with the Department of Energy and the DOE National Laboratories. It is a pilot that is focused on nuclear terrorism. It is focused on security of fissile material, and it is focused on getting the advantage of the DOE National Laboratories over many people is they have probably the national treasure trove in nuclear expertise. They are the people that build the U.S. government's weapons, they maintain the nuclear stockpile.

So what we are doing is leveraging the DOE National Laboratories and providing them information sharing, information access, providing them with more information with which to help us assess the terrorist threat and to do validation of reporting and in fact to try and get them to help targeting of collection.

So that is two concrete examples of just pilots. And what I would like to do is run 10 or 12 pilots by the end—I can't say the end of the year, we are getting there pretty quickly, but over the next 360 days. If I come back and talk to you a year from now, I would like to tell you about 10 information sharing pilots that we are working, that in fact are giving, providing better information, better quality information to first responders, to state, local, tribal and the private sector.

And at the same time we are giving them information, we are fleshing out policy issues. For example, in the New York City pilot with the FBI, we are actually seeing directives and policy issues that need to be changed to enable a better flow of information.

Mrs. LOWEY. Well, the red light is blinking away. Let me thank you, and I look forward to hearing progress, especially with the New York City pilot, because, as you probably know, after 9/11, the New York City Police Department ended up developing its own counterterrorist intelligence unit. They have people all over the world, because of the lack of appropriate information sharing and accurate information sharing.

So if there is progress, I am really pleased, and I look forward, Mr. Chairman, in getting continuing updates. Thank you very much.

Mr. SIMMONS. And just for the information of the subcommittee, we have done a classified briefing on the New York transit issue, and the Chief Information Office, the Department of Homeland Security attended that, as did other officials. And so we have been doing quite a bit of work in focusing on information sharing relative to that incident. And I believe there will be additional visits to New York City in the future to work that dimension of the problem.

Mrs. LOWEY. Mr. Chairman, if I may just thank you, because I attended one of the meetings and because of a conflict I couldn't attend the second one. But I thought the Department of Homeland Security's response was totally inappropriate and out of order, and I do believe that was the view of almost every member of this committee who attended that meeting.

If they had a beef with New York City—and I will tell you, if I had to depend on—I won't contrast it. Let me just say I have tremendous confidence in Commissioner Ray Kelly, and I think if the Department of Homeland Security thinks they know more and knows different, it shouldn't have been aired on the front pages of

the paper. But we will leave it at that, and thank you for following up.

Mr. SIMMONS. Absolutely.

The chair now recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Mr. Russack, I want to thank you for being here. I appreciate your testimony. I have a couple questions, a follow-on to a question that Mr. Dent had first raised in relation to this, anyway.

It is my understanding that the president has assigned you the responsibility for completing guidelines describing how the intelligence community should convert classified intelligence information to a sharable format for use by state, local and tribal law enforcement officers, an obligation imposed in the Intelligence Reform Act. Those guidelines were due on September 13, 2005 but apparently were delayed because of Hurricanes Katrina and Rita.

So my question is, have the guidelines been completed, and if not, why not? And when can we expect them? And if you would like to comment further, you did, I guess, answer the question of to what extent the Department of Homeland Security's Chief Intelligence Officer, Charlie Allen, has been involved in this process. You could expand upon that, if you would, and, again, state his role in the development of those guidelines.

Mr. RUSSACK. Let me, first of all, address the second part, Charlie Allen's involvement in the guidelines. Charlie hasn't been at the Department of Homeland Security, as you know, sir, very long, I think probably about 3 or 4 weeks at this point.

The Department of Homeland Security, the process for establishing the guidelines, writing the guidelines was that there is an Information Sharing PCC. PCC is a Policy Coordinating Committee. It is chaired by a representative, a senior director, from the Homeland Security Department as well as by a senior director from the National Security Council.

The Information Sharing PCC, along with the members of the PCC—I am a member of the PCC, the DNI's CIO, chief information officer, is a member, most of the federal departments and agencies are members of that PCC. We as a group drafted guidelines, and we drafted guidelines for White House staffing. The Department of Homeland Security was very much involved in the drafting of those guidelines, as were all departments and agencies.

To answer your question on, basically, where are they, the guidelines were drafted and I think—again, I am not an expert on where they stand at the present time, but I know we asked for an extension, we the federal government—I am speaking for the big "we" here—the administration asked for an extension and actually talked to various committees on the Hill because of the hurricanes that you mentioned. And the guidelines are in final staffing.

Mr. LANGEVIN. When can the committee expect them?

Mr. RUSSACK. Can I take that for the record, sir, because I am not sure I am in a position to really answer that. I will have to get back to the people who are actually staffing those and get you an answer.

Mr. LANGEVIN. That would be fine. The committee, I know, would appreciate it and look forward to hearing from you on that.

Mr. RUSSACK. Yes, sir.

Mr. LANGEVIN. Well, the other question I have is, could you describe, basically, your key successes thus far in helping to implement the information sharing environment? And to what extent does success depend on cooperation from various agencies that comprise the intelligence community? In fact, further, are there any members of the intelligence community that are not effectively cooperating with you?

Mr. RUSSACK. Let me go in reverse again, if I can. I think all members of the intelligence community are in fact cooperating, and I can assure you that the director of national intelligence is insisting that they cooperate. And when people don't cooperate with me, I tell my boss. My immediate boss of the DNI, and he is more than happy to pick up the phone or to talk to someone about any lack of coordination. So there is cooperation.

And I can assure you that the DNI wants to share. And I can assure you, as I said earlier today, that we can and will protect sensitive sources and methods, ad we will share the information people need to base decisions on to protect America.

So there is a desire to share, there is in fact the leadership mandating sharing.

Key successes, I think the two pilots I mentioned to the gentle congresswoman from New York are pilots that are going and they will be, I think, very successful. I would like to have, as I said earlier, about 10 or 12 of these pilots operating over the next year.

The fact that we have an Information Sharing Council that, as Congressman Dent mentioned and asked good questions about how we were in fact going to take into account the needs of state, local, tribal and the private sector, the fact that this Council, we have the names of the representatives across our federal government.

We are going to reach out through global justice, through the National Association of Governors and through other mechanisms. We are going to reach out to people in the state, local and the private sector. We are going to in fact find out what is not working the way it should work, what information is not being shared, what information do they need, what are their requirements, and we are going to in fact develop options that will allow information to be shared, allow people to have access to information that they need.

So my staff and my achievements thus far, I mean, I would like to be further ahead of where I am at the present time. As I said earlier, back in June, I had a staff of two. Now, I have a dozen. I have a dozen really good people. I have been offered as many as 50 or 100 people. I have talked to a lot of people. I have not taken anyone on my staff that I have not personally hand selected with the skill sets, the passion, the motivation to get the job done.

So concrete examples of where I am, we have an Information Sharing Council—first meeting will be a week from Friday—we have some pilots in operation. I am working hard on the deliverables I owe to the Congress. The president and I, in conjunction with this Information Sharing Council, are to make a report to you, Members of Congress, by the 17th of June on more specificity on what this new information sharing environment is going to be, how will it work? That is what we are working on.

Right now, we have three working groups, actually steering groups, in place. Those steering groups are actually getting their arms wrapped around existing federal, state, local, tribal, private sector programs that exist, that mandate and foster information sharing.

The steering groups are in fact trying to get their arms around all the working groups that various departments have that are ongoing. For example, inside the DNI's world, there is an entity called, "The Information Sharing Working Group." And then there is the Information Sharing Working Group–L, which deals with foreign liaison. We are taking into account all the things that are going on and getting our arms wrapped around that.

I have a contract with an FFRDC to help me baseline the existing information sharing environment. And one exists now. As I said earlier, it is flawed.

Mr. SIMMONS. For the record, FFRDC, for the record?

Mr. RUSSACK. Federally funded research and development activity. Those are think tanks that are not for profit, sir. I took data that was given to me by the Office of Management and Budget and turned that over to this FFRDC, and I said, "Help me baseline the existing environment. Help me get my arms wrapped around what existing federal programs various departments have."

So what they have done is they have come back to me with a preliminary report, I got it last week, and the four major federal agencies that play in information sharing, the first one being the entire intelligence community, they have given me a preliminary report on what the IC is doing in information sharing, what systems are being used.

The next one is the Department of Homeland Security, what they are doing in information, what systems are being used; the Department of Defense, same for them; and also Justice, Department of Justice, and the FBI.

So that is probably all I can really say in response to your question on something concrete that we have done thus far.

Mr. LANGEVIN. Well, I see my time is expired, but you have painted obviously a picture of a very aggressive and comprehensive agenda. Perhaps a bit rosy picture you have presented, but I certainly wish you well, and the committee will be looking forward to hearing more from you on the progress that you are making. Thank you.

Mr. RUSSACK. Thank you, sir.

Mr. SIMMONS. I thank the gentleman.

I see that our second panel has arrived, but before I introduce them, I would like to make one comment. You mentioned open sources of intelligence as an important adjunct to the classified side, and, clearly, open sources of intelligence obviate the problems of information sharing. And I think that that is an important capability that we need to think about in the future.

I also note that issue one in your report regarding current authorities concludes that it is not clear at this point whether statutory changes will be required to clarify these governance issues. I would urge you and your staff to notify us of statutory changes are necessary, and this subcommittee would be more than happy to consider those and move those forward on an urgent basis, because

we feel that information sharing is critically important to our national security.

I also note that there are several major reports and guidelines that are coming due in the coming months, and we encourage you to work hard to meet those deadlines, again, because of the importance of these issues.

On the issue of money, the $20 million or $30 million, the ranking member and I will take that issue under advisement and we will do our best effort here to address that issue in the coming weeks and months in a bipartisan fashion.

That being said, on behalf of the subcommittee, I want to thank you for your testimony, but, more important, I want to thank you for taking on a job that is not easy, that involves breaking a little glass, that involves moving our intelligence capabilities in a direction that previously was very difficult to move, and we hope that you will consider this subcommittee to be a co-partner in the enterprise.

Mr. RUSSACK. Thank you, sir.

Mr. SIMMONS. And thank you very much.

Mr. RUSSACK. Thank you.

Mr. SIMMONS. The chair now calls the second panel to the table. The Honorable Lee Hamilton, vice chairman of the 9/11 Public Discourse Project, and Mr. William Crowell from the Markle Foundation's Task Force on National Security in the Information Age.

The Honorable Lee Hamilton is the director of the Center on Congress at Indiana University and also serves as president and director of the Woodrow Wilson International Center for Scholars here in Washington, D.C.

He served from 1965 to 1999 as the U.S. Representative from Indiana. During his tenure, he served as chairman and ranking member of the House Committee on Foreign Affairs and was also chairman of the Permanent Select Committee on Intelligence.

He served as vice chairman of the National Commission on Terrorist Attacks Upon the United States, or the 9/11 Commission, and is now vice chairman of the 9/11 Public Discourse Project.

Welcome, Mr. Hamilton.

And now I would like to yield to the ranking member for the introduction of Mr. Crowell.

Ms. LOFGREN. Thank you, Mr. Chairman. It is nice to split up the introductions.

Bill Crowell, until recently a constituent of mine, is an independent consultant, also director and chairman of the Board of BroadWare Technology, director of ArcSight and director of NARS. He was appointed in 2003 to the Unisys Corporate Security Advisory Board to address emerging security issues and best practices. And in September 2003, he joined the Advisory Board of ChoicePoint, a data aggregation company.

Bill Crowell served as president and chief executive officer of Cylink, a leading e-business security solution company until it was acquired in February 2003 by SafeNet.

Prior to all of this, and when I first met him, Mr. Crowell served for nearly 4 years as deputy director of the National Security Agency where he had held a series of senior positions, including deputy director of operations. He also, in 1999, was appointed to the Presi-

dent's Export Council and chaired the PEC Subcommittee on Encryption where he did good work. And in March of 2001, the secretary of defense appointed him to the Federal Advisory Committee that conducted a comprehensive review of the U.S. Nuclear Command and Control System.

As you have noted, Mr. Chairman, he served on the Markle Foundation Task Force since 9/11, and I would say, really, Bill in his entire professional career as well as a volunteer has spent his life trying to make sure our country was safe, for which we thank him and also welcome his testimony today.

Mr. SIMMONS. Thank you.

The chair now recognizes the Honorable Lee Hamilton. Welcome. Thank you for being here. Good to see you again. We look forward to your testimony.

STATEMENT OF HONORABLE LEE HAMILTON, VICE CHAIRMAN, 9/11 PUBLIC DISCOURSE PROJECT

Mr. HAMILTON. Thank you very much. It is a pleasure to be here, Chairman Simmons and Ranking Member Lofgren and the distinguished members of the subcommittee.

The first point I want to make, simply, is an expression of thanks to you for your efforts on oversight of the intelligence sharing, information sharing problem. I think it is enormously important that that be done and that you keep close track of it, and I am pleased that you are doing that.

And I think the view of all the commissioners no single step is more important than information sharing in our efforts to strengthen the intelligence community and thereby ensure the safety and security of the American people.

In our view, it was poor information sharing that was the single greatest failure of our government in the lead-up to the 9/11 attacks. And it was a contributing factor to the government's missteps in understanding and responding to the threat of al-Qa'ida.

If you looked at the missed opportunities, and we laid them out in our report, they are a good many of them, almost all of them involved in some way or the other the failure to share information.

The second point I want to make is with regard to the 9/11 Commission recommendations. We really made two in this area. One is that information procedures have to provide incentives for sharing to restore a better balance between security and shared knowledge. That is not easy to do, we recognize that, but it is essential. And, secondly, the second recommendation was that the president has to lead the government-wide effort to bring major national security institutions into the information revolution. He only is the person that can coordinate and do it.

You have now, of course, enacted into law the Intelligence Reform and Terrorism Prevention Act, and I will give you a quick view of how we look at the progress under that act thus far.

Despite the enactment of the statute, despite the creation of the Program Manager Office, it is our view that we have really made minimal progress toward establishing a seamless information sharing system. You can change the law, you can change the tech-

nology, you still have to change the culture, and you need to motivate institutions and individuals to share information.

We commend Mr. Russack and his small team. We think they are demonstrating a very strong commitment to the whole concept of information sharing. Congress has authorized but not yet, as I understand it, appropriated funding for the Program Manager's Office, and he and the Information Sharing Program need a lot of support.

It is our view that agencies still want to control the information they produce. They view it as their property, rather than the property of the entire government and the property of the American people. And for information sharing to work, of course, the right people have to get the right information at the right time.

We are particularly concerned about the poor information sharing with state and local authorities. We are troubled by a number of stories. We have heard about that. I will not go into that in detail unless you want to on the questions.

Let me just conclude my remarks by saying that we think there are several important steps that need to be taken. One, to press the Congress to ensure that the Program Manager gets the funding and the resources and the personnel he needs to carry out his very important mission. If that is not done, you will not get good flow of information.

Second, the Program Manager will need very strong support from the president and direct engagement of the senior leadership of the Homeland Security Council.

Third, to press the executive branch to produce the information sharing reports that are already required by law. I was listening to the testimony a moment ago and it is encouraging, but what struck me about is just the few minutes I was sitting here is that it is very future-oriented.

The important thing is what are the capabilities now? What can they do right now? The terrorists are not going to wait. We have to have these capabilities in place now. And when I hear this testimony, not just from the Program Manager but others, I just don't have a sense that they have a sense of urgency about this problem. It is kind of a business as usual approach.

So these reports are required by law. The September guidelines from the president to the executive agencies are late already. The December report is a crucial report, and I urge the committee, the subcommittee here, to make completion of the report and its implementation a very high priority.

Fourth, I believe this committee should revisit the question as to whom the Program Manager reports to. He reports now to the DNI, but his responsibilities with regard to information sharing inside the intelligence community go beyond that, include information sharing for other federal agencies for state and local, tribal authorities in the private sector, and I think you ought to consider very carefully whether or not he would be more effective if he were placed in the executive office of the president with direct line authority from the president.

So to conclude, we need to change from a system in which the originating agency of classified information is the sole arbiter of which other agencies are allowed to see the information. That is

the deeply routed culture in the intelligence community, and that is far too restrictive for the kind of information flow you need in a good counterterrorism strategy. The right information must be made available instantly at all levels of government and to the private sector, and that requires a change in the culture.

The actions of those who would do us harm are not under our control, but our system of information sharing is under our control. It demands urgent attention. We can fix it. There certainly will be no excuse if we fail to do it.

Thank you very much for the attention you are paying to this critical problem. All of us on the Commission, former commissioners, are grateful to you, and we look forward to your continued oversight of this very important matter.

[The statement of Mr. Hamilton follows:]

PREPARED STATEMENT OF HON. LEE H. HAMILTON

Chairman Simmons, Ranking Member Lofgren, distinguished members of the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment: It is an honor to appear before you today to discuss the important issue of government-wide counterterrorism information sharing and the role of the Program Manager.

At the outset, I want to commend you for holding this hearing. Information sharing across our government benefits directly from the focus you bring to it. Those who are charged with improving information sharing need your oversight and support.

The guidance you provide will help break down barriers to information sharing among the authorities in our federal, state, and local levels of government.

It is my firm belief that no single step is more important than information sharing as a way to strengthen our intelligence and thus ensure the safety and security of the American people.

I. What the 9/11 Commission Found

Poor information sharing was the single greatest failure of our government in the lead-up to the 9/11 attacks. The failure to share information adequately, within and across federal agencies, and from federal agencies to state and local authorities, was a significant contributing factor to our government's missteps in understanding and responding to the growing threat of al-Qa'ida in the years before the 9/11 attacks. There were several missed opportunities to disrupt the 9/11 plot. Most of them involved the failure to share information.

The 9/11 Commission found that the biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systemic resistance to sharing information. We believe the "need-to-share" principle must be accorded much greater weight in the balance with the longstanding "need-to-know" principle of information protection.

Given the changes necessary across the government, it is clear to us that no single agency can bring about these changes alone. Only presidential leadership, with robust congressional oversight, can bring about the necessary changes in information sharing.

II. Recommendations to Improve Information Sharing

The 9/11 Commission made two recommendations to improve information sharing:

First, "Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge." (*The 9/11 Commission Report,* p. 417)

Second, "The president should lead the government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a "trusted information network." (*The 9/11 Commission Report,* p. 418)

III. The Intelligence Reform and Terrorism Prevention Act of 2004

Last December, President Bush signed into law the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA). The Act drew upon the 9/11 Commission's recommendations and created a program manager for information sharing. Specifically, Section 1016 directs the program manager to "facilitate information sharing

between Federal departments and agencies and State, tribal, and local governments . . . and the private sector."

In April the President selected Mr. John Russack for that important post. An executive order placed Mr. Russack's office under the new office of the Director of National Intelligence.

The Act also called for the establishment of an Information Sharing Council (ISC). On October 25, President Bush issued an executive order creating the ISC, which will bring together the heads of at least 12 federal agencies to provide advice on how to share information about potential terrorist activity. The President has asked these top officials to assist the program manager to ensure that counterterrorism information is broadly shared across the federal government and among state and local authorities, and the private sector.

IV. Information Sharing Still Far from Optimal

Despite the enactment of the statute, and the creation of the office of Program Manager, we have made minimal progress toward the establishment of a seamless information sharing system. You can change the law, you can change the technology, but you still need to change the culture; you still need to motivate institutions and individuals to share information.

We commend Mr. Russack and his small team: they are demonstrating a strong commitment to enhancing information sharing. Congress has authorized, but not yet appropriated, funding for the Program Manager's office. The Information Sharing Program Manager needs strong congressional oversight and support so that it can accomplish its important mission.

We note that the National Counterterrorism Center has implemented a system in which analysts have access to streams of information from 26 different systems. Representatives of those agencies involved in counterterrorism have access to this pool of information within the NCTC. This is a positive development at the federal level but this is too narrow.

Agencies still control the information they produce. They view it as their property, rather than the property of the entire government, and the property of the American people. For information sharing to work, the right information must get to the right person at the right time. Moreover information sharing with state and local authorities has only marginally improved.

V. Poor Information Sharing with State and Local Authorities

Frankly, my fellow Commissioners and I are troubled by stories we have heard from federal, state, and local officials with knowledge of the state of information sharing. They tell us they do not get the information they need from the federal government. Communication and collaboration between the Department of Homeland Security (DHS) and state homeland security officials nationwide is not what it should be. Communication between the FBI and local law enforcement also falls short.

Historically, federal law enforcement agencies have been unwilling to share information with their state and local counterparts. Distrust continues to exist between federal and local partners. State and local officials, for their part, traditionally have kept information to themselves, and have been frustrated by the lack of a system into which to feed their information. Federal authorities need to build confidence with state and local officials by developing systems on which they are trained, a broad concept of operations they understand, and a standard reporting procedure that they know how to use.

Federal agencies cannot expect state and local officials to cooperate with them if they do not provide reliable and consistent leadership. The recent controversy over the credibility of a threat to New York City's subway system is a case in point. On October 6, the New York Police Department reacted to information from the FBI which suggested the system was at risk of being attacked in the next few days. DHS, however, took a different position, and evaluated the information as less than credible.

I believe the NYPD acted responsibly, based on the information it was given. But clearly in a dynamic situation such as this, there needs to be far better coordination between federal and local authorities. Action cannot wait until final analysis of intelligence is made. But the federal government needs to do a better job in sending a consistent message to local officials as a situation develops, both in how the threat is evaluated and acted upon.

Relationships with state and local authorities need to be strengthened. State and local authorities need to know that the information they provide to DHS will be properly integrated and not ignored. They need to know that DHS will provide the necessary information to them in return.

We hear reports that the FBI does not recognize clearances granted by DHS to state and local authorities. A police chief could not visit his own officers detailed to an FBI Joint Terrorist Task Force, because his clearances did not come through the FBI.

State and local officials have been unable to get secure telephones for conversations with federal officials about sensitive information. Therefore, necessary conversations take place late if they take place at all.

Understandably, state and local officials resent being cut out of the information loop.

The information sharing provisions of Intelligence Reform and Terrorist Prevention Act, which are intended to implement common standards and bring feuding federal, state, and local agencies together, are still a long, long way from being implemented. Given the urgency of the threat, this is unacceptable. We must do better. And we must do it sooner rather than later.

VI. Scorecard on Information Sharing

On October 20, the former 9/11 Commissioners issued a scorecard evaluating progress the government has made in implementing the Commission's recommendations concerning institutional reform in the aftermath of 9/11. Here's what we said with respect to our two recommendations on information sharing:

INCENTIVES FOR INFORMATION SHARING

"Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge." (p. 417)

Grade: MINIMAL PROGRESS

What has happened: According to the Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108–458), the President shall require the heads of federal departments and agencies to promote a culture of information sharing by both reducing disincentives and providing affirmative incentives for sharing information. The DNI also has responsibility for establishing policies and procedures to ensure the maximum availability of, and access to, intelligence information within the intelligence community. A program manager has been designated by the President as responsible for information sharing across the federal government. This office is still a start-up. So far, if there have been changes in incentives, in favor of information sharing, they have been negligible.

Why this is still important: The 9/11 story included numerous examples of how a mentality of limiting information sharing to those with a "need to know" in fact kept information from getting to the right people at the right time. Cultures will not change without policies in place that actively encourage such change, and without the sustained implementation of those policies.

What needs to be done: The President and the DNI need to make change in the culture of information sharing a priority through clear and visible support. They need to develop positive incentives for information sharing to balance the many disincentives on the books. Personnel should be evaluated on how well they share information rather than how well they hoard it. Agency leaders should be evaluated on how well they create an environment that promotes sharing. Information sharing must be improved not only across the federal government but with state and local authorities.

PRESIDENT SHOULD LEAD NATIONAL SECURITY INSTITUTIONS INTO THE INFORMATION REVOLUTION

"The president should lead the government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a 'trusted information network.'" (p. 418)

Grade: MINIMAL PROGRESS

What has happened: The Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108–458) required that the President create an information sharing environment to provide and facilitate the means for sharing information through the use of policy guidelines and technologies. Within the intelligence community, the DNI has all necessary support and authorities from the President to ensure maximum availability of and access to intelligence information. Outside the intelligence community, a program manager has been designated by the President as responsible for information sharing across the federal government, yet there are few signs of the actual implementation of a "trusted information network." The program manager does not yet have the personnel and resources necessary to assert authority across the federal government.

Why this is still important: Only with White House leadership can legal and policy obstacles be overcome to bring our national security institutions into the information revolution.

What needs to be done: The President needs to make information sharing a priority. Designating officials to be in charge is not enough; they need resources and active presidential backing to change the information systems that enable information sharing, the policies and procedures that compel sharing, and the systems of performance evaluation so that personnel are appraised on how they carry out information sharing.

We noted that the Director of National Intelligence needs to be a driving force to improve information sharing but that he must be given strong support by the President. Ten months have passed under the new law. Progress is minimal. To his credit, the DNI is seized with the issue of information sharing, but the horses are barely out of the gate. He must press the issue and press it very hard. We said that the DNI will be judged in part on information sharing. His customers are not just in the federal government; they are state and local officials as well.

VII. Next Steps

Mr. Russack, who has one of the most difficult jobs in government, will need strong support as he seeks to resolve the legal, policy, and technical problems that impede information sharing.

I urge the Homeland Security Committee to do the following:

First, to press the Congress to insure that the Program Manager gets the funding, resources and personnel he needs to carry out his mission.

Second, the Program Manager will need strong support from the President and the direct engagement of senior leadership of the Homeland Security Council.

Third to press the Executive branch to produce the information sharing reports required by law. The September guidelines from the President to the Executive agencies are late. The December report is a crucial report—spelling out an Information Sharing Environment for the entire government. This report is the implementation plan for information sharing. I urge this Committee to make the completion of this report—and its implementation—a high priority.

Fourth, I believe this Committee should revisit the question as to whom the Program Manager reports. Currently, he reports to the DNI, but his responsibilities go beyond information sharing inside the intelligence community and include the facilitation of information sharing for other federal agencies, state, local and tribal authorities, and the private sector.

Information sharing is not just a federal problem, it's a national problem. The Program Manager should be placed in charge of the policy committees that are charged with improving information sharing across the government. Congress should consider whether he would be more effective if he were placed in the executive office of the president with direct line authority from the president.

VIII. Conclusions

Mr. Chairman, we need to change from a system in which the originating agency of classified information is the sole arbiter of which other agencies (federal, state, or local) is allowed to see the information. This is far too restrictive for the flexible adversary we face. Information collected by any federal agency is the property of the federal government and by extension the property of the American people.

The right information must be made available instantly, at all levels of government and to the private sector, to those men and women who have both the mission and the means to act against our enemies before they can act against us.

Success requires that the flow of information be not just a one-way street. Federal, state and local agencies must exchange intelligence, and cooperate in planning and executing joint operations.

The actions of those who would do us harm are not under our control. But our system of information sharing is under our control. It demands urgent attention. We can fix it. There will be no excuse for a future failure if we do not.

I commend this Committee for its important attention to information sharing. I look forward to working with you, and would be pleased to answer your questions.

Mr. SIMMONS. I thank you for that testimony.

The chair now recognizes Mr. Crowell.

STATEMENT OF WILLIAM CROWELL, MARKLE FOUNDATION TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE

Mr. CROWELL. Chairman, Congressman Lofgren and distinguished members, thank you very much for allowing me to be here and testify before this subcommittee.

I have had the privilege of being a member of the Markle Task Force on the National Security in the Information Age since its inception in March of 2002, and it was created specifically to focus on how best to mobilize information and intelligence resources to improve security, while still protecting privacy and civil liberties.

The Markle Foundation has issued two reports. Both of those reports have stressed the importance of a decentralize network of information sharing and analysis that achieves security, while at the same time protecting our civil liberties. And it has also stressed the need to have clear and understandable rules and business practices on collection and sharing of information that is permissible and that which is not permissible. And I will stress that point a couple of times in my opening remarks.

On September 6 of this year, co-chairman Jim Barksdale and Zoe Baird, sent a letter to the president on behalf of the task force and our thoughts on the progress of the information sharing environment. The letter is attached to my testimony, along with the response from the White House.

In addition, Zoe Baird testified to the House Intelligence Subcommittee on Oversight in an open hearing on October 19, 2005, and my remarks today largely parallel and mirror the letter and the subsequent testimony.

I really recognize that John Russack has a very, very difficult job, but I would like to try and outline five points that we, in the Markle Foundation, believe are important to getting on with the task.

The first one is to reestablish a sense of urgency to share information. To the earlier point made, we have a lot of information today and we can share it today. We don't have to wait till tomorrow to begin doing that.

So getting the information sharing business right will pay dividends not just for preventing terrorism attacks but also for dealing with natural disasters as well. And so consistent and persistent leadership is needed in order to put all of the well-meaning people on the right path to getting this done.

The second point is to empower the Program Manager with the resources and statute he needs to create the information sharing environment. John now has 12 people, according to his earlier testimony. He obviously needs many more than that. He needs a budget and budget line item that he can depend on and be able to plan against. And I think, by the way, that giving him the position of chair of the Information Sharing Policy Coordinating Committee would go a long way toward increasing this statute and getting this job done.

Third point is, translate the law and executive orders into government-wide consistent guidelines. What we have today is an agency-by-agency interpretation of what they can and cannot do, and it varies widely, both in the areas of security and in the area

of privacy, which is an impediment to getting on with this job. So new laws and executive orders have not yet been translated into new practices and guidelines. And it is business as usual. Nothing has really changed.

So the ambiguities in the lines of responsibility are actually impeding people's agreement to move toward a vision of sharing information.

So we need guidelines that will establish uniform rules and procedure for the security of information and for protection of privacy and civil liberties. We need to update the U.S. person rule, which in many agencies restricts the flow of information when the information was lawfully collected in the first place, but restricts it for reasons that are not clear in terms of protecting personal privacy.

We need to change the classification procedure. This is a crucial topic, as has already been mentioned. Many agencies believe they own the information. They express that ownership in the form of originator-controlled information, and that should be used very judiciously. And the rules regarding classification should clearly distinguish between information that is actionable and the sources and methods from which that information came from.

We should ensure policy compliance oversight and dispute resolution structures that keep the policies viable. I can't emphasize enough the need to have dispute resolution structures, because people are going to want to break crockery in getting actionable information to state, local and tribal and private sectors.

John's comment on technology was appropriate. It is not an impediment; it is a path and an enabler. But I would point out that the acquisition of new technology must be streamlined, and new legislation that has given agencies the flexibility they need to buy needed IT systems are not being used or not being used effectively by those agencies.

Fourth point, we need to adopt a risk management approach to information sharing. We are not advocating that all information be shared with everyone. We suggest, though, that when information has real actionable value, the way should be found to share that information.

And perfect information security in this trusted system is not going to be possible, and the cost of getting it might be too high. The current approach does not consider risk from failing to share, and I don't think you can connect dots that you can't get access to.

Finally, the fifth item, we think we need to focus on establishing trusted information sharing relationships, particularly with the state, local, tribal organizations and private sector, rather than on continuous reorganizations of the manner in which we address this.

Many state and local officials and the private sector feel disenfranchised, and the community of intelligence and law enforcement needs to treat them as partners.

The final comment I would make has to do with responsibility and accountability. The law and executive order now gives responsibility for creating the ISE to the director of national intelligence, and this creates a particular problem for the Program Manager as he tries to reach out to the other components that are outside the DNI. He cannot really look to DNI resources for the law enforce-

ment and for some of the other activities that he will be involved in, and that poses and interesting but certainly solvable problem.

My conclusion is this is all about leadership. It is about a common vision, a vision of sharing information in order to protect the American public. It is about a common strategy, how to get there, and it is about accountability, and I would urge that this committee continue to review the progress. It is a very important area for the nation.

And, once again, thank you very much for the opportunity to testify.

[Information follows:]

MARKLE FOUNDATION
Task Force on National Security in the Information Age

September 7, 2005

The President
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Re: Building the Information Sharing Environment

Dear Mr. President:

We write on behalf of the Markle Foundation Task Force on National Security in the Information Age. At our August 2005 meeting, the Task Force asked that after Labor Day we convey to you some thoughts as you prepare the report due this month to Congress on the Guidelines and Requirements to Implement the Information Sharing Environment mandated by the Intelligence Reform and Terrorism Prevention Act of December 2004 (the Act). We reconsidered sending the letter in light of the terrible loss from Hurricane Katrina, but concluded that you would appreciate this input since so many of the issues may be similar to those Secretary Chertoff and others have suggested be examined in an after action report on the response to the hurricane.

As you know, the Markle Task Force has issued two reports that frame a decentralized network of information sharing, guided by policy principles that simultaneously empower and constrain government officials and provide meaningful privacy and civil liberties protections for our people. The information sharing environment requires, as we stated, clear and understandable rules and business practices on collection and sharing of data that is permissible, and that which is prohibited.

Your Executive Orders and the Act have generated genuine progress toward creating an Information Sharing Environment (ISE), and individual and agency initiatives show good promise. We remain concerned, however, that risk aversion and bureaucratic resistance to change continue to hamper the carrying out of announced new policies. The constitutional and statutory authorities to do what needs to be done exist. We urge you to reiterate to your Cabinet officers and all U.S. Government officers that they should interpret all applicable laws and regulations to enable information sharing rather than use ambiguities between the Act and prior law which Congress left unresolved as an excuse to protect prior approaches. They need to embrace rather than resist the change.

It is our view that we as a nation must move to create the ISE with great urgency, and that we should not be satisfied with the first steps – as major as they are – that have been taken in the four years since the 9/11 attacks. The same sense of urgency and focused attention exercised by our military men and women in the battlefield must be applied to reforming how government agencies work together to understand and prevent the threats to the nation.

In your report to Congress, we believe it will be helpful if you address the following:

1. Make clear that the Director of National Intelligence (DNI) has responsibility for the creation of the ISE. Since the ISE Program Manager (PM) has been placed administratively in the DNI's office, the DNI must assume the responsibility to ensure that the PM creates an effective ISE with the full recognition that such a system extends beyond the Intelligence Community. Because successful implementation of the ISE is critical to achieving intelligence goals and meeting other responsibilities of the DNI such as providing the President with a well-informed briefing, nothing in his portfolio is more fundamental.

2. Emphasize the development of government-wide policies and guidelines immediately as the foundation for the adoption of information sharing capabilities and procedures. Sweeping change is needed to remove any pre-9/11 confusion about information sharing that, regrettably, still exists in some departments and agencies. A single set of policies across the government, while recognizing the need for some additional rules depending on agency-specific missions, should end confusion and interagency battles about whose rules apply in particular situations.

3. Consistent with our earlier recommendations, and as required by the Act, these policies should address four key issues.

   - Clear and enforceable rules and procedures are needed that ensure information is accessed, shared, handled, and retained in a manner that meets operational efficiency and security, while protecting our nation's privacy and civil liberties. Perhaps most urgently, the government needs to create new guidelines governing information sharing of "U.S. persons" data since that designation is an outdated boundary for what is permissible.

   - A clear and consistent government-wide process must be created that guides classification decisions to protect sources and methods while enabling access and sharing without undue or arbitrary dependence on originator control (ORCON).

   - Technical and organizational mechanisms for policy compliance, oversight, and dispute resolution are needed to minimize and adjudicate failures to share information. This will reduce risk aversion by government officials who might be concerned about the personal impact of wrong decisions in a new environment.

   - A comprehensive and independent assessment of the value being created by the ISE for different participants, including policymakers is needed.

   We believe that addressing these fundamental policy challenges will accelerate the implementation of the ISE consistent with privacy and civil liberties concerns and national security needs.

4. The PM should immediately be given the resources needed to get the job done by both Congress and the Administration. The White House staff and the DNI should ensure obstacles are removed. Because his responsibilities extend beyond the Intelligence Community, the PM should have enhanced authority within the Executive Office of the President. Thus, we recommend the PM chair the Information Sharing Policy Coordinating Committee in addition to chairing the Information Sharing Council.

5. Creating the Privacy and Civil Liberties Oversight Board in the Executive Office of the President was a key step in ensuring that effective information sharing for national security conforms to our nation's traditions and values. We hope the board will engage quickly as the policies and guidelines are developed.

The nation has only begun to mobilize the tremendous resources provided by the capabilities of its people and its advanced technology. We cannot afford to lose the innovation race to the terrorists who are aggressively using technology like the Internet to connect and train recruits as well as plan and execute operations. We must train government employees to work in new ways, sponsor research on new technologies and methods, and create systems that manage information in smarter and more cost-effective ways, while providing real security improvements and accountability. It is our sense that people in government are already working hard and therefore instead of asking them to work harder, the leadership must create an environment that allows them to work smarter.

We remain concerned that if another terrorist attack were to take place in the U.S., the immediate reaction could cause the pendulum to swing toward measures that impinge on our privacy and civil liberties. Any potential future intelligence failures will not rightly be blamed on legal constraints that prevent sensible information collection and sharing. The authorities to collect and share information exist, but cannot be realized without clear government-wide guidelines on how this can be maximized while protecting the security of information and the civil liberties of our people.

The Markle Task Force stands ready to assist in any way you may find useful.

Respectfully yours,

Zoë Baird Jim Barksdale

Co-Chairs of the Markle Task Force on National Security in the Information Age

Cc: Stephen J. Hadley
Assistant to the President for National Security Affairs

Frances Fragos Townsend
Assistant to the President for Homeland Security

Joshua B. Bolten
Director, Office of Management and Budget

John D. Negroponte
Director of National Intelligence

Michael Chertoff
Secretary of Homeland Security

John R. Russack
Program Manager for Counterterrorism Information Sharing

THE WHITE HOUSE

WASHINGTON

October 21, 2005

Dear Ms. Baird:

Thank you for your thoughtful letter of September 7, 2005, in which you shared with the President insights and suggestions of the Markle Task Force as he prepares to issue guidelines and requirements pursuant to section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).

As you likely have heard by now, the priority response to Hurricane Katrina by many of the key information-sharing stakeholders temporarily delayed our efforts to meet the IRTPA's September 13 deliverable. We are now back on track, and expect the President to issue a directive shortly.

On behalf of the President, we are deeply grateful to you and the entire Markle Task Force for your abiding commitment to improving the U.S. Government's capacity to facilitate access to and sharing of terrorism information. We also share your sense of urgency about establishing an Information Sharing Environment (ISE) that will facilitate the flow of terrorism-related information within and beyond the Federal Government without infringing on information privacy rights or civil liberties.

As for your specific suggestions, please rest assured the Director of National Intelligence (DNI) fully appreciates his responsibility with respect to creating the ISE, and will ensure the Program Manager -- who is subject to the DNI's authority, direction and control -- receives the support he needs. In addition, the President's guidelines will be designed to set Government-wide policies and procedures, and will address conflicting authorities between and among agencies in the information-sharing context.

We appreciate your concern about the need to address Originator Controls (ORCON) and U.S. person data, among others, in the ISE context. Guidance on these matters will be forthcoming. The Privacy and Civil Liberties Oversight Board -- once its chair and vice chair are confirmed and it becomes operational --

promises to provide a valuable resource for the Program Manager, the Information Sharing Council, and participating departments and agencies in both the development and use of the ISE.

We have no plan to designate the Program Manager as chair of the Information Sharing Policy Coordination Committee (ISPCC). The ISPCC, like other PCC's, is a White House-based forum that neutrally addresses policy issues and disputes which, in this case, relate to terrorism information sharing and building the ISE. The Program Manager, who himself is a member of that body separate and apart from the O/DNI representative, is expected to raise issues and advocate positions before the ISPCC.

Thank you, again, for your ongoing commitment to this critical initiative and for your generous offer of further assistance. An identical letter has been sent to Mr. Barksdale.

Sincerely,

Stephen J. Hadley
Assistant to the President
for National Security Affairs

Frances Fragos Townsend
Assistant to the President
for Homeland Security and
Counterterrorism

Zoe Baird
Co-Chairman
Markle Task Force on National
Security in the Information Age
10 Rockefeller Plaza
16th Floor
New York, NY 10020-1903

[The statement of Mr. Crowell follows:]

PREPARED STATEMENT OF WILLIAM P. CROWELL

MARKLE TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE

Mr. Chairman, Ranking Member, Honorable Members of the Committee, thank you for the invitation to appear today. I appreciate the opportunity to speak on progress made towards building an Information Sharing Environment.

Key Task Force Recommendations

More than a year ago, the President issued Executive Orders to create an Information Sharing Environment (ISE) and in December 2004, Congress enacted the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 specifying the attributes of such an Information Sharing Environment. In particular, Section 1016 on Information Sharing tasks the President with creating an "information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties". The IRTPA also designates the new position of Program Manager to plan and oversee the implementation of the ISE. Responsible for terrorism information sharing across the Federal government, the Program Manager is tasked to develop policies, rules, and procedures to govern the operation of the ISE in consultation with the Information Sharing Council. On October 25th, 2005 the President signed Executive order 13388 creating the anticipated Information Sharing Council as required by the Act.

While there has been some progress, we still have a long way to go to implement this law. The government-wide direction and accountability anticipated in both the Executive Orders and the Act should today be a major priority for the DNI. Without effective information sharing, information collection remains stovepiped and the importance of information held by different agencies or at different levels of government cannot be understood.

My statement centers on the following five recommendations suggested by the Markle Task Force on National Security in the Information Age:

- Re-establish a greater sense of urgency to share information;
- Empower the ISE Program Manager;
- Translate law and executive orders into government-wide consistent guidelines;
- Adopt a Risk Management Approach to Information Sharing
- Focus on establishing trusted information sharing relationships, including those with state, local, tribal organizations and the private sector, rather than structural reorganization.

Perspective

I have had the privilege to participate as member in the Task Force on National Security in the Information Age since its creation in March 2001. The Task Force which is co-chaired by Zoë Baird and Jim Barksdale, is comprised of leading national security experts from the administrations of Presidents Carter, Reagan, Bush, Clinton and Bush, as well as widely recognized experts on technology and civil liberties, and was created to focus on how best to mobilize information and intelligence to improve security while protecting privacy and civil liberties.

My own background includes having been a former Deputy Director of Operations and then Deputy Director of the National Security Agency (NSA) during the intelligence draw-downs of the early 1990's. After retiring from NSA I became CEO of a public company in Silicon Valley that was focused on securing cyberspace for industry and government customers. After my company was acquired in early 2003 I became an independent consultant in security and intelligence systems and serve on a variety of boards of technology companies. My remarks today are based on an outside look at progress made by government.

The Markle Task Force has issued two reports: "Protecting America's Freedom in the Information Age" (October 2002) and "Creating a Trusted Information Network for Homeland Security" (December 2003). Both have stressed the importance of creating a decentralized network of information sharing and analysis that achieves security while at the same time protects our civil liberties. We need to create an Information Sharing Environment that fundamentally changes the way we think about the business of national and homeland security. It requires clear and understandable rules and business practices on collection and sharing of data that is permis-

sible and that which is prohibited. We believe that the Executive Branch and the Congress must both assume leadership for this task to succeed.

Creating an Information Sharing Environment

On September 6th of this year, Co-Chairmen Jim Barksdale and Zoë Baird sent a letter to the President on behalf of the Task Force with our thoughts on the progress of the Information Sharing Environment (ISE). The letter is attached and is available on Markle's website (*www.markle.org*), as is the response from the White House. In addition Zoë Baird testified to the House Intelligence Subcommittee on Oversight at an Open Hearing on the Office of the Director of National Intelligence on October 19, 2005. My remarks today largely parallel and mirror the letter and subsequent testimony.

Timeline—Greater Sense of Urgency Needed

Many first steps have been taken in the right direction, but much more needs to be done and the pace needs to be accelerated. We recognize the competing demands of an ongoing military engagement abroad and back-to-back catastrophic natural disasters, but getting information sharing right will pay dividends not only in preventing terrorist attacks, but in dealing with natural disasters as well. National and homeland security are based on many of the same concepts. It is time to stop applauding first steps and to raise our expectations for progress.

The nation must move to implement an effective ISE with much greater urgency. There are many initiatives that can be taken immediately, and many policies that must be adopted to empower government officials and provide assurance of privacy protections. The same sense of urgency and focused attention exercised by our military and intelligence men and women in the battlefield must be applied to reforming how government agencies work together to understand and prevent the threats to our nation.

Well-motivated people throughout the government are having a hard time adjusting to the new realities. In our letter to the President, we urged him to reiterate to Cabinet officers and all U.S. Government officers that they should interpret applicable laws and regulations to enable information sharing and not use old interpretations as an excuse to protect prior approaches. Any ambiguities as to authorities and lines of responsibility should be construed in favor of sharing and against turf battles. We still hear too many stories of departments and agencies using rigid interpretations of their authority prior to the change in the law in order to protect their turf. Constructive congressional oversight is needed here and the White House staff should itself take a more active role. The Intelligence Community should embrace rather than resist these changes and realize that change is not a rejection of the past, but a path to the future.

This process will take continuous commitment and persistence from the leadership and all stakeholders. The issues are tough. We are aware of several individual agency initiatives that show good promise. Some examples include:

—The FBI has developed the FBI Intelligence Information Report Dissemination System (FIDS); FBI officers are being trained and issuing more intelligence reports that are shared with the intelligence community;

—The National Counterterrorism Center (NCTC) is enhancing collaboration across the foreignintelligence/domestic information divide that was so detrimental to our efforts before 9/11.

Program Manager for Information Sharing

Now that the DNI has the administrative responsibility for the Program Manager, we believe he must assume the responsibility for the success of that office. The DNI must also recognize that the Information Sharing Environment extends beyond the Intelligence Community into the DHS, Federal law enforcement, and State and Local public safety arenas. Further, the Program Manager's office should immediately be staffed with the appropriate talent and given the resources needed to get the job done. More full-time government employees (FTE) positions must be provided. The Deputy Director of National Intelligence testified in July that they were striving to have the Program Manager's key leadership positions filled by mid-August. Obviously the priority response to Hurricane Katrina may have delayed the formation of the office, yet it is now mid-October and not much has changed.

New Guidelines and Policies

High-level direction and sweeping change is needed to remove any pre 9/11 confusion about information sharing. We have emphasized the immediate need for clear, new government-wide policies and guidelines for dramatically increasing information sharing, while protecting our civil liberties and protecting sensitive information. Regrettably, any confusion created about how to reconcile new legislation and executive orders with prior laws governing agencies and departments have not been re-

solved by the Department of Justice, the DNI or other responsible parties designated by the President. A single set of policies across the government, with some additional rules depending on agency-specific missions, should end confusion and interagency battles about whose rules apply in particular situations.

We believe the DNI's office must take responsibility for ensuring that the changes mandated in legislation and executive orders result in changes in practice. We assume that the President is looking to the DNI to exercise such responsibility.

These new guidelines should at a minimum include:

- Clear and enforceable rules and procedures that ensure information is accessed, shared, handled and retained in a manner that meets operational efficiency and security, while protecting our nation's privacy and civil liberties.
- Updated policies on the U.S. Persons rule: Since at least 1981, access to and sharing of intelligence information collected by U.S. Government agencies has been controlled by two factors: (1) whether information was collected within the territory of the United States or overseas; and (2) whether information involved a U.S. Person (U.S. Citizen or Permanent Resident Alien). These distinctions remain relevant for the *collection* of intelligence, but we believe they should no longer be the basis for controlling *access* to and *sharing* of intelligence information lawfully collected by the government. While there is broad recognition that these rules must change in the post 9/11 world, there also is justifiable concern that they be replaced with easily understandable rules that serve the same goal of protecting our civil liberties. In the next several months, our Task Force will propose a new approach to these issues that we believe can initiate a necessary dialogue about how to move beyond these outmoded rules while enhancing both civil liberties and operational success.
- New classification procedures: Executive Order 13356 specified that originator control (ORCON) be used very judiciously. Information sharing should not be impeded because of excessive classification rules that classify information according to sensitive intelligence collection sources and methods even when it could have been acquired by less sensitive means. Furthermore, we must work to extinguish the belief that those who collect information own it. The President clearly stated that standards be developed "requiring terrorism information be shared free of originator controls, including, for example, controls requiring the consent of the originating agency prior to the dissemination of the information outside any agency to which it has been made available, to the maximum extent permitted. . . ."
- Technical and organization mechanisms for policy compliance, oversight, and timely dispute resolution are needed to minimize and adjudicate failures to share information. There should also be a mechanism to turn disputes into policy. This will reduce risk aversion by government officials who might be concerned about the personal impact of wrong decisions in a new environment.
- A comprehensive and independent assessment of the value being created by the Information Sharing Environment.

A Risk Management Approach to Information Sharing

We realize that many in the Intelligence Community have concerns that the increased focus on information sharing creates a greater risk of damaging security breaches. What the Task Force has recommended—and I believe is critical—is that a distributed information sharing system like the ISE contain policy, procedural, and technical protections including robust access controls that reduce the risk of unwanted disclosure and promote trust. We are not advocating that all information be shared with everyone; we suggest that information must be accessible to those users who need it to successfully perform their assigned missions and are authorized to see it. This will require leadership by the DNI to determine legitimate user needs and innovative cross-agency teams of people working problems together.

Sophisticated technology exists to secure and protect information and we must take full advantage of it. However, the government must recognize that perfect information security is not possible and that the costs of seeking it are too high. There are security risks not only from information falling into the wrong hands, but also from information failing to find its way into the right hands. The risk of release and sharing should be balanced with the risk of not sharing. The government's current approach to protecting classified information does not recognize this risk from failing to share. As wrenching as it is, the government must move to a risk management approach to protecting classified information that balances the risks of failing to connect critical information and adopts flexible and creative mechanisms for mitigating risks on both sides. You cannot connect dots that you cannot access.

Privacy and Civil Liberties

As change in the intelligence community is being furthered, privacy and civil liberty interests must be considered consistently. Both the Congress and the Executive Branch must demonstrate that privacy is a priority. The Chairman and Vice Chairman of the Privacy and Civil Liberties Oversight Board in the Executive Office of the President have not been confirmed and the Board has never met. We hope the members have begun to be briefed so that, if confirmed, they are ready to assume their responsibilities immediately. It is critical that these oversight mechanisms established by law and executive order become operational immediately and get engaged as policies and guidelines are developed.

Furthermore, the position of the Chief Privacy Officer at the Department of Homeland Security must be filled again quickly.

Acquisition Procedures for New Information Technology

We cannot afford to lose the innovation race to the terrorists who are aggressively using technology like the Internet to connect and train recruits as well as plan and execute operations. Our government must be much more flexible and adaptive, taking full advantage of new technologies as they become available.

A Request for Information (RFI) was issued recently by the Program Manager seeking vendors to provide Electronic Directory Services (EDS) to "enable authorized participants to locate and access information, organizations, services and personnel in support of their respective mission requirements for terrorism information." We have recommended that a directory service is a critical element of an effective Information Sharing Environment, but it is not clear the Program Manager has the resources or authority to implement such a system. The technology is available to get this done, but it must be introduced quickly using an incremental approach. Attempting to seek a perfect solution will paralyze the effort—just as we have seen in other programs.

State, local, tribal and private sector

Our last concern has to do with an aspect of information sharing where very little progress has been made. Yes, it is true that more intelligence information is being shared with state and local officials and even with the private sector. However, the nature of the terrorist threat requires that we harness all resources available and, within guidelines that protect privacy and civil liberties, we develop two-way engagement with key organizations outside the federal government. Because terrorists are presumably living and working among us, some of the best intelligence may come from non-traditional and unclassified sources.

Meetings with state and local officials and the private sector have led us to believe that the federal government has not yet realized the value of information identified by state and local entities. A system to integrate this information has not been developed. Much more attention must be paid to this gap, because we as a government are ignoring a critical component of national security. This must be done jointly with the Department of Homeland Security because it is partly the reason why that department was created. We know this is one of the toughest challenges facing the federal government, but it must be done.

Recommendations

The Task Force will be announcing some proposals over the next months, but we offer a few specific recommendations to the Committee as you consider priority actions. These recommendations are in addition to the underlying point that the administration must get on with fully establishing and empowering the Program Manager.

- Government-wide guidelines to promote information sharing as called for in the Act and Executive Order should be established as soon as possible;
- The Program Manager should act quickly on the RFI issued to establish electronic directory services; this is a critical step toward better information sharing;
- Working with the Congress, the Executive branch should support the Program Manager in sponsoring some pilots which demonstrate information sharing between federal agencies, state, local, tribal and the private sector;
- Establish a panel of experts, primarily from industry, to review and advise the program manager, DNI, DoD, DHS, and Justice on architecture and system design (particularly important given the number of failed IT and information sharing programs between those four organizations);
- Congress should move quickly to act on key positions that are pending confirmation, and if they are not confirmed the President must quickly nominate others (the Privacy and Civil Liberties Oversight Board Chairman and Vice-Chairman have not been confirmed, and neither has a General Counsel to the

DNI, a particularly important position given the legal barriers and confusion cited by many as preventing implementation of the ISE);

Conclusion

Our nation has now reorganized the intelligence community as called for in many earlier reports. For this to address the significant challenges of the future, we must train government employees to work in new ways, develop our civil liberties guidance, sponsor research on new technologies and methods, and create systems that manage information in smarter and more cost-effective ways, while providing real security improvements and accountability. Any future intelligence failures will not rightly be blamed on legal constraints that prevent sensible information collection and sharing. The authorities to collect and share information exist; we must thoughtfully exercise them.

Finally, we must work toward improving our national security without eroding privacy and civil liberties. Our task force has expressed concern that if another major attack were to take place on our homeland, the immediate reaction could cause the pendulum to swing toward measures that impinge on our privacy and civil liberties in ways in which none of us would support given time for thoughtful consideration and debate. We have the opportunity now and we should seize it.

Thank you again for the invitation to appear before you, and I welcome any questions you may have.

Mr. SIMMONS. Thank you both for your testimony.

Normally, I would take my 5 minutes of questions at this point, but I see the distinguished vice chairman of the full committee has come in, and I suspect that it would be intelligent to extend to him the courtesy of taking my time, because I know how busy it is.

So the chairman yields to the distinguished vice chairman, the gentleman from Pennsylvania.

Mr. WELDON. I thank my good friend and chairman for yielding and for his leadership, along with the distinguished ranking member.

I thank our witnesses for coming in today and would like to say that this hearing is perhaps one of the most important subjects that we have to focus on relative to protecting the homeland from any emerging threats. And it is an issue that is not new to this Congress.

It was this Congress that created the Gilmore Commission and the four reports of the Gilmore Commission, chaired by former Governor Jim Gilmore, that issued three reports before 9/11. And in each of those reports, you will find references to this very issue.

So the Congress was in fact on the lead in the need for information sharing when it comes to information sharing, both vertically and horizontally, and the need to tear down the firewalls with the stovepipes of the 33 classified systems managed by 15 different agencies.

In fact, it as the Congress that had language in three successive bills, in 1999, 2000, and 2001, that mandated, at least from DOD's standpoint, where I sit as the vice chairman, that we push toward integration. Unfortunately, on November 4 of 1999, in spite of John Hamre encouraging such an initiative to create a national collaborative environment, the CIA and the FBI, after attending a meeting with John Hamre in my office, said publicly, "We don't need that capability."

Well, we have now learned some other important information that troubles me, and that is why I am here, Mr. Chairman, because we can't move forward unless we understand the lessons of the past. And I wish I didn't have to come to this hearing for this

purpose, but I am here for this purpose, because I have not yet received any responses.

Approximately June of this year, I learned the details of a top secret military program called, "Able Danger." My first contact was to call the staff director of the 9/11 Discourse Project to ask if they had looked at "Able Danger" because there was no mention of it at all, even a footnote in the 9/11 Commission report. My chief of staff got the response the next day that, "Well, we looked at it, but we decided not to go down that route," and they were the terms that were used, "not to go down that route."

I then met with Tim Roemer a week later and I said, "Tim, were you ever briefed on Able Danger?" He said, "No, Curt, never heard of it, never briefed." I said, "A top secret program that was ordered by the chairman of the Joint Chiefs of Staff, under the command of General Schoomacher at SOCOM and you were never briefed, and it was specifically against al-Qa'ida?" He said, "Never."

So I called John Lehman and had lunch with him, and John Lehman told me at lunch he had never been briefed either. And when I told him the details of "Able Danger," he was livid. I said, "What do I do, John?" He said, "You have got to pursue it."

So I went to the floor of the House and did a 45-minute speech. Of course, nobody pays attention to 45-minute speeches. During the month of July, I went to our committee chairs—Armed Services, Homeland Security, Intelligence, Oversight of Appropriations—and The New York Times picked the story up the first week of August with a front page story above the fold on Tuesday.

The response by the 9/11 Commission was that they denied that there was ever a briefing on "Able Danger." The New York Times ran a story the second day. And they said, "Well, there was a briefing but there was never a mention of Mohamed Atta." The New York Times ran a story a third day. The 9/11 Commission said, "Well, there was a brief, and, yes, Mohamed Atta's name was mentioned, but it wasn't until July, one week before our report was done, and we determined it wasn't historically significant." In fact, they used the terms, "historically insignificant."

Mr. Chairman, we have now determined, not through 9/11 Commission work, and I supported the 9/11 Commission with my vote and my voice, at least five professional employees of DOD have publicly stated that Mohamed Atta was identified before 9/11. And it wasn't just done by the Army's legal.

We now know, thanks to no help of the 9/11 Commission, that there was a separate massive data mining effort that was conducted down in Garland, Texas of the officers of the Raytheon Corporation, and guess who, Mr. Chairman, the head of that was? The 9/11 Commission doesn't have a clue because they never interviewed the guy. It was Sam Johnson's son, one of most dedicated members. And Sam Johnson's son, Dr. Bob Johnson, is now ready to testify, along with the other military folks, on the record, that he too identified Mohamed Atta before 9/11.

Now, we have two separate data mining operations that are ready to come public and testify. They both identified Mohamed Atta by name and in one case by photo before 9/11.

Now, this is not about a chart, as people have tried to say. In fact, we know there was 2.5 terabytes of data collected about al-

Qa'ida, specifically ordered by the chairman of the Joint Chiefs of Staff. Now, 2.5 terabytes of data is equal to one-fourth of all the printed material in the Library of Congress. That is historically insignificant, I might add.

And now we also know on the record, and the Senate Judiciary Committee has taken these statements and I have been there witnessing it, that there was an attempt made in September of 2000 to transfer information about the Brooklyn cell of al-Qa'ida to the FBI three times. The FBI employee who set up those meetings up will state that under oath, which he did to the Senate Judiciary Committee.

And you know what? Those meetings were canceled. Not one mention of this in the 9/11 Commission report. We now know that there was a 3-hour briefing providing for the chairman of the Joint Chiefs of Staff in January of 2001.

And now where do we see the response? We are here to talk about sharing information and public knowledge and accountability. We see this administration and the 9/11 Commission not willing to talk about it on the record.

Now, that is outrageous, Mr. Chairman, and I am not here to criticize just any Democrat, I am here to criticize this administration, which I supported. They have gagged the witnesses that will come forward.

Now, I sent a letter to the 9/11 Commission on August 10. I have yet to receive a response. This is November 8. Now, I got a letter congratulating me for my work on the frequency spectrum allocation issue but not a response to my letter about what is in fact the most important information prior to 9/11 that Louis Freeh, Louis Freeh, Mr. Chairman, on national TV 2 weeks ago, when he was questioned by Tim Russert, said, "That is the kind of tactical intelligence," meaning "Able Danger," that would make a difference in stopping a hijacking. We are very interested in what the 9/11 Commission didn't do with respect to "Able Danger." And that is Louis Freeh, FBI director when 9/11 occurred.

Mr. Chairman, there is something wrong here. There is something wrong. When we are supposed to be getting the facts for the 3,000 families, and I was with the families up in Harvard University with my good friend Jane Harman just a few weeks ago and they pleaded with me to get the information.

When we now know that there was information 2 days before the attack on the USS Cole that could have stopped the crew from the USS Cole from losing 17 of their sailors, and I had the captain of that ship in, Commander Kirk Lippold 2 weeks ago, who said, "If I would have had the information that they had, I wouldn't have taken my ship into port."

So I say, Mr. Chairman, "What is going on here?" We are talking about sharing information. Am I hearing it that no one really wants to share information? We want to spin things? Let the truth come out. Right now, the Defense Intelligence Agency is destroying the career of Lieutenant Colonel Tony Shaffer, and I am not going to allow that to happen. I haven't heard a peep out of the 9/11 Commission to ask for more information, not a response to my letter.

Mr. Chairman, I am a little bit upset, because we don't know the information about what happened prior to 9/11. This is not about a chart of one person. It is about 2.5 terabytes of data, collected by two separate data banks, neither of whom were talked to by the 9/11 Commission. It looks to me like a cover-up, Mr. Chairman. That is what it looks like.

And so I have two questions.

Mr. Hamilton, when can I expect a response to my letter of August 10, which was sent to you and Mr. Keane? And, number two, will you join in calling for a full and open hearing to allow all "Able Danger" people, and that is 6 individuals—there weren't 80 involved, there were 20 total, 6 are willing to come forward—are you willing to call for a public hearing, allowing them all to testify and also to have Dieter Snell testify under oath about his interview of Scott Philpot in July of 2004?

Thank you.

Mr. HAMILTON. Thank you very much, Mr. Weldon. First of all, with regard to the response, we are operating, as you may know, with a very skeleton staff. We no longer have the 80-some staff members that we had under the 9/11 Commission. We will respond to you, we should, and we will try to get a response promptly to you.

Secondly, we understand on the Commission that we were writing the first draft of history, if you would. We understand that information will be coming forth probably for the next century about what happened on 9/11, and we, in the Commission, must remain open to new information.

Now, let me tell you why we did what we did. The Commission based its report, first, on facts that were obtained by, supported by documentary evidence and, second, by witnesses who had direct firsthand knowledge of documents they produced and the events they described. Those persons that now make the claim about Atta's name on the chart cannot produce the chart. They did not do the analysis and they cannot reproduce the analysis.

Many serious questions have to be addressed to these people, and I think, so far as I personally am concerned, Mr. Weldon, I can't speak for all commissioners, I am perfectly willing to support a hearing with regard to these witnesses, because I think there are serious questions that need to be addressed to them.

We interviewed General Schoomacher. He was the Commander of the Special Operations Command at the time "Able Danger" was created. We interviewed General Hugh Shelton, who was chairman of the Joint Chiefs, Admiral Scott Frye, General Gregory Newbold, all successive directors of operations for the Joint Staff. We interviewed Brian Sheridan, the assistant secretary for special operations in low intensity conflict during the period that "Able Danger" was in existence.

We also interviewed several other senior and mid-level managers of the Special Operations and Low Intensity Conflict Program.

Despite direct questions for any information relevant to the 9/11 attacks, none of them mentioned such a chart. They mention nothing about identifying Mohamed Atta, even in response to questions about the "Able Danger" Program.

We interviewed Mr. Stephen Hadley for 3 hours. He responded to questions from the Joint Congressional Inquiry. He mentioned nothing about that chart, mentioned nothing about the name of Mohammed Atta (ph being on the chart.

We interviewed his boss at the time, Condoleezza Rice, for over 4 hours. She said nothing about a chart and mentioned nothing about the name of Mohamed Atta on the chart.

We interviewed her boss, President Bush, for nearly 3 hours. Neither he nor the vice president said anything about a chart or the name of Mohamed Atta on a chart. The White House has not confirmed the existence of the chart. There is, so far as I know, no evidence to document that such a chart ever existed.

Now, one other point I would make here, even if everything that you say is correct about Mohamed Atta, I don't think it would change the Commission's recommendations in any way. We documented in great detail many examples of the failure to share information, and we made that recommendation across the board, and action on those recommendations, we believe, is still necessary.

Now, I might point out that you, Mr. Weldon, in your book wrote, "On September 25, 2001, just 2 weeks after 9/11, I met in the White House with Stephen Hadley, the deputy national security advisor to the president. I presented him with a two by three chart I had been given in the aftermath of 9/11. The chart was developed in 1999 as part of a Defense Department initiative dubbed, "Able Danger." It diagramed the affiliations of al-Qa'ida and showed Mohamed Atta and the infamous Brooklyn cell." Hadley's response was, "I have to show this to the big man."

We have not yet seen that chart, and we are open to receiving it.

Mr. SIMMONS. Recovering my time, the chairman now recognizes the ranking member.

Ms. LOFGREN. Thank you, Mr. Chairman, and I would like to get back to questions on the testimony.

First, I would like to thank you both for being here, obviously, and for all that you do, and I would like to ask Mr. Crowell a couple of quick questions.

First, the Markle Foundation has called electronic directory services a critical step toward better information sharing, and, as you have referenced in your comments, it is important, both in terms of outlining what we need to collect but also what we don't need to collect, in terms of privacy and civil liberties.

What would be your best advice to Mr. Russack about how to establish the electronic directory services? I don't think it exists yet, unless I am wrong.

Mr. CROWELL. It doesn't exist yet. I believe he issued an RFI, a Request For Information, to industry regarding directory services.

What the Markle Foundation postulated was the need for directory services to be the pointers to information wherever it resided for several reasons. One was for policy reasons, in order to preserve the policy about how the information was used with the information when it actually got transferred. So that if there were privacy implications or if there were restrictions on the use, they would be part of the record that gets transferred.

The second was for freshness. One of the problems with transferring information among stovepipes in the U.S. federal government, in particular, is that the information has no—there is no way for the information to get updated. So if information is transferred that is either wrong or that is later changed, those changes don't follow the transfer of the information to other agencies.

But by using directory services and pointers to the information, as opposed to actually moving the information wholesale, there is an opportunity to, with technology, solve this problem of keeping the information accurate, fresh and updated by the people who actually have that responsibility.

Ms. LOFGREN. And also to make sure only those who need—that people get only what they are permitted to get.

Mr. CROWELL. That is exactly right. And also that you control things like can it be printed, can it be sent to further distribution lists and so on, which would go a long way toward increasing the trust that people have in the system that is going to be used to share.

Ms. LOFGREN. But do you envision—just thinking about this, and maybe this is incorrect—that the implementation of such a system might actually solve the need or go a long way toward solving the need of a government-wide consistent guidelines that you referenced in your testimony?

Mr. CROWELL. Well, it certainly would become a facilitator for moving consistent guidelines across organizational borders. It won't remove the need for someone to sit down and decide what some of those guidelines will be.

Ms. LOFGREN. Let me ask, if I could, just two quick questions that you mentioned in your testimony. One, the need for a dispute resolution mechanism as well as the lack of use of the streamlined systems we have for IT acquisition. We are woefully behind in very many parts of the government in our IT area.

Do you have advice for this committee and how we might promote changes in those two areas?

Mr. CROWELL. Well, on the first one, dispute resolution, the importance of that, particularly in the beginning of a change in the culture, is to try and move the inevitable disputes that will occur about whether information is too classified to be sent to particular users or whether it can be declassified or sanitized, to move those disputes quickly up to policy makers who in turn then can move the disputed policies back down as new policies and incorporate the disputes into the evolving policies and guidelines that would become important.

With regard to IT modernization, the best way I can phrase that is I won't mention the particular agency but I know of one agency where the analysts are prohibited from going home and doing any work from home, but they have better tools at home—

Ms. LOFGREN. Right.

Mr. CROWELL. —than they do at work. That is a pathetic situation. I mean, at home, I have access to blogs, to databases, to all kinds of information. Every day I get a terrorism report that is several megabytes in size from a private source that isn't even associated with the government, and I can use that information to review

what is happening worldwide, with a little Googling, on a very positive basis.

And that kind of technology is not expensive, but it is not being deployed very rapidly in some cases because of security concerns and security constraints and other cases, just because it opens up the process too much.

Ms. LOFGREN. Let me follow up with Mr. Hamilton on that point. It has been a frustration to me. I have been on the Judiciary Committee for 11 years and we have yet to have an oversight hearing on the FBI. Thinking about just the technology aspect of the FBI and the Trilogy Program, which we found out in March of this year, after $157 million, basically was scrapped.

As far as I know, and, Mr. Hamilton, you may know from your service on the 9/11 Commission, we still don't have a comprehensive or working solution for sharing information internally within the FBI.

And my question is, how are they going to be partners in information sharing across agencies as well as out into our private sector and local and state government allies if they can't even share information internally? Can you give us any information on that?

Maybe we should have a hearing on that since Judiciary apparently doesn't want to exert their jurisdiction. We have concurrent and might be able to move this forward.

Maybe the Commission didn't go too heavily into that, but if you can give us an wisdom, it would be much appreciated.

Mr. HAMILTON. Congressman Lofgren, I, among other things, now serve on an Advisory Board to the director of the FBI, and they are, I believe, finally, seized this issue, and they recognize the failure of their past efforts, I might say costly failure, but I do believe that they are now trying very hard to improve the information systems within the FBI.

Now, I don't think they are there yet, by a long shot. They have brought in a lot of highly trained technical people to deal with this problem, and I think there is a very strong emphasis on it now to improve it.

So your oversight here is terribly important because of all the changes that are necessary in the FBI, and you appreciate the director's trying to change the whole culture of the institution, from law enforcement to—

Ms. LOFGREN. Well, I am an admirer, actually, of the director, but I have to note that we have got a problem here.

Mr. HAMILTON. Well, the question is, can he do it, and can he change the culture, and I have no doubt at all about, number one, his ability, nor, number two, his intent. He is a top flight person, but it is a formidable challenge, and I just think you and all of us need to bear down on the FBI, make sure we are fully supportive of what they are trying to do, because that change is critical.

If you change the FBI's focus from law enforcement to prevention of terrorism, what that means is that intelligence becomes the area of the FBI's work that drives the entire FBI, because it is intelligence that tells you about possible terrorist activity. So the intelligence effort and the information sharing and the information technology involved in that intelligence effort is just crucial in order for the FBI to carry out its new function well.

Ms. LOFGREN. I see my time has expired.

Thank you, Mr. Chairman.

Mr. SIMMONS. Thank you.

The chair now recognizes the gentleman from Pennsylvania with the hope that he can yield me some of his time.

Mr. WELDON. I will, Mr. Chairman. Thank you. I just want to respond to some of Mr. Hamilton's comments, just for the record. And, again, we are trying to spin instead of getting to the facts.

Mr. Hamilton, I have had respect for you, we served together for a number of years. I have never criticized you publicly. But I am absolutely outraged at what is happening here in the lack of aggressiveness in wanting to get to the bottom of this story.

You brought up the fact, alluding that somehow Steve Hadley didn't acknowledge. Well, why don't you talk to Chairman Dan Burton who chaired the Government Operations Oversight Committee, who went with me to that meeting? Why don't you talk to Chris Shays, the chairman of the Government Operations Oversight Committee for National Security, who went with me to that meeting? There were three of us in the room with Hadley, not one.

If you have a problem with what Hadley said, you ought to—he told me he was misquoted. The fact was—and it is not about a chart. Don't try to spin this about a chart. We have a 23-year Navy veteran who has risked his entire career to tell the truth, that in January of 2000 he identified Mohamed Atta and three terrorists. He had to seek you out to give you that information in July of 2004, and this was the response of the person who debriefed him who I want to put under oath, Dieter Snell.

After he was questioned, he said to—and this is a direct quote from Commander Scott Philpot. He said, after Scott gave him the information, Dieter Snell said, "What do you want us to do with this information? We go to print in 10 days." Is that the legacy of the 9/11 Commission, that we go to print in 10 days; therefore, we don't even mention "Able Danger" as a footnote in your book? This was not ordered by some Johnny Come Lately off the street.

And you say you interviewed Schoomacher, you interviewed—you didn't question him about "Able Danger" in detail. I talked to them. You didn't question the people that were involved in the operation of "Able Danger." Talk to Scott Philpot, as I have 20 times, who has risked his career. You have never talked to him personally. You have never talked to Tony Shaffer personally, who is having his career destroyed right now.

You didn't play this kind of role when you were in Congress. You were aggressive at oversight. And I am not going to sit by while a man's career is destroyed because we don't want them to be able to tell the truth. And it is going to embarrass this administration, the Bush administration, but I don't care.

That was the job of the 9/11 Commission. I voted for it, I supported it. I tried to meet with you all. Tom Keane gave me a 5-minute phone call. I hand delivered information at the hearing when George Tenet was at the witness stand and the questions were never asked. We gave a packet of follow up. You never proceeded to interview me. It is not about me. It is about the 3,000 families that had their lives ruined and the 17 sailors on the Cole.

We are going to get to the bottom of this, Lee, I will guarantee you, and there is going to be egg on the faces of people when the truth comes out, because in the end, the truth provides the justice.

I yield you the rest of my time.

Mr. HAMILTON. Mr. Chairman, I think I should have the opportunity to respond to that.

Mr. SIMMONS. Absolutely.

Mr. HAMILTON. Mr. Weldon, we want that truth to come out, and I don't wan to try to block the truth, and I will stand with you to try to get the truth out. Now, we are not trying to spin the chart. Where—

Mr. WELDON. It is not about a chart.

Mr. HAMILTON. Where is the chart?

Mr. WELDON. The chart was destroyed, I guess, by Hadley. It is not about a chart. It never was about a chart.

Mr. HAMILTON. Well, it was in your book.

Mr. WELDON. My book mentions it in one sentence.

Mr. SIMMONS. Would the gentleman—

Mr. HAMILTON. And when those people met with our investigators in Afghanistan, they talked about a chart with Mohamed Atta's name on it.

Mr. WELDON. Come to my office, I will show you a chart.

Mr. HAMILTON. With Mohamed Atta's name on it, I would like to do that. Look, that is a very—

Mr. SIMMONS. Reclaiming my time, the gentleman at the witness table is recognized by the chair.

Mr. HAMILTON. Well, I am not sure it benefits us here to go further, but I will say that that chart is an enormously important piece of information.

We did not have any information, Mr. Weldon, that prior to 9/11 that the government knew the name of Mohamed Atta. Now, when our investigators talked to your people—well, the people you have identified today, when they talked to those people in Afghanistan, they said there was a chart with Mohamed Atta's name on it.

Now, at that point in the investigation, which this was in the year 2003, we certainly knew the name of Mohamed Atta, and anybody in a meeting that heard the name of Mohamed Atta, that would have been like ringing a fire bell. None of our three investigators, the White House lawyer did not recall a chart, did not recall mention of Mohamed Atta.

Now, if the chart exists, let's see it, and we will give it due weight.

And let me join you in saying that we don't want to destroy anybody's career. We want to get the information. Just give us the documentary information.

Mr. SIMMONS. The chair now recognizes the gentlelady from Texas, Ms. Jackson-Lee.

Ms. JACKSON-LEE. I thank the chairman very much.

And I apologize, was delayed with some other meetings, Mr. Hamilton and Mr. Crowell, and would have gotten here sooner if I had known how much excitement you all were having in this hearing.

[Laughter.]

But let me thank you for your service and the previous witness who is now going to be our new Manager of Intelligence and important, I think, position in our Department.

If I might, I will make a statement that will look for solutions, and that is that I do think that we are still making a journey toward securing the homeland. There is much debate as to whether or not we are any more secure today than we were on September 10. I think the 9/11 Commission report has been a great road map and directive, and we have put in place many very positive aspects, and I think that puts us in a step in the right direction.

But I have several points that I would like to bring up, and I would engage Mr. Crowell as well on these questions.

First of all, with respect to the Information Sharing Manager, do you think that we have an effective position that can generate intelligence down to our federal, state and local sharing, meaning that we can generate or translate information down into the state and local jurisdictions and whether they can translate? Do we have an appropriate vehicle for that and they can translate information to us?

Use as a backdrop, and I don't want to be coy, but use as a backdrop the recent incident with New York. I have a great respect for Commissioner Kelly, I know him well, but I am hoping that it was not tainted by politics and local elections. Did we do that right and is that an example of sharing information in the right way? If you are taking notes, I would appreciate it, because I would like to be able to—on the questions, I would like to be able to finish my questions and then yield to both of you.

In particular, Mr. Hamilton, I know your great work, and we worked very closely, so many of us, around the 9/11 report. I was pleased to have been on the Select Committee, the committee before this one on Homeland Security and sort of worked closely with the work that you all were doing.

But maybe we should have hearings. Ms. Lofgren has said something very insightful and also indicting and that is that there have not been oversight hearings over the FBI. I know the chairman of this committee is very astute about these issues. And maybe we should have, moving aside the recent occurrences of politics and in and out indictments and other types of activities.

I have always said that the American people need to have the ultimate truth. I think it would be appropriate to hold hearings anew—and they have always said, "Well, they belong in the Intelligence Committee;" I think it is appropriate in the Homeland Security Committee—on the trail of intelligence that led us to the state of war.

The reason why I say that is it is more woven around the question of terrorism. And, therefore, if it is woven around that question, then that is the jurisdiction of the Homeland Security. Let us track the trail and all the pieces that might not have been addressed by the 9/11 Commission, your task was monumental, and I think the work that you did we will be forever grateful that we got a road map. But we are now seeing the missing links.

Should we not convene hearings, oversight hearings, transparent hearings that will engage representatives from the White House, engage the proponents of information to find out how the trail of

information either gave us information about those terrorists that might be engaged or did not?

And I yield to the gentleman for what was a very lengthy questioning, but I think you can detail about three of them. There are about three questions. One happened to be longer than the others.

Mr. HAMILTON. Let me begin to respond, and then Mr. Crowell will pick it up.

First of all, with regard to Mr. Russack's job as the Program Manager, it has been said several times here it is an enormously important job. He becomes now the key official in implementing information sharing, which is the key aspect of better intelligence with regard to counterterrorism. There is nothing this committee can do that would be more important, I believe, than to stay on top of the progress that he is making and maybe not making and try to provide guidance to him.

And to the extent that you have hearings to that effect, then I would certainly applaud them.

You have to make sure he has the authority that he needs, and if he doesn't have it, you should give it to him. You have to make sure he has the resources and the personnel that he needs, and if he doesn't have it, you should make sure he has it. And you have to keep your focus on this particular office, I believe, to see that if functions. And if this office does not function, then your counterterrorism effort is going to be severely hampered.

Now, with regard to the New York situation, I know there has been some controversy about that. The positive side of it is that information was shared from the DHS to the city of New York. And on October 6, the New York Police Department reacted to information that came to them from the FBI, and that information suggested that their system, their transportation was at risk of being attacked in the next few days.

The DHS gave a different interpretation to that information than the New York officials did, but keep in mind they have got very different responsibilities. If you are the mayor of that city and you have this information coming to you, you are going to act in such a way that will protect the city.

You also have to keep in mind that the information here keeps developing. You don't get a finished product at 10 o'clock in the morning. What you get is an initial intelligence assessment, which is refined over a period of many hours, but the mayor has to act right away if he is going to protect the system. So you would have a very different perspective here.

I believe that the New York mayor and the New York Police Department acted responsibly based on the information that was given to them, but it is a dynamic situation, and I can understand why the DHS people had a different interpretation of the information than the mayor did.

All of this has to say is that we have got to work harder to get this right.

Ms. JACKSON-LEE. That is right.

Mr. HAMILTON. So that there is a consistent message flowing from Washington to the local officials as the situation develops. And we all know it is a crisis situation, and it is very, very hard to do.

Ms. JACKSON-LEE. Would you just—I know he has to answer—would you also comment on further hearings to sort of determine whether or not we had some faulty intelligence leading us to where we were in terms of the war? And not so much the war but interpreting whether there were terrorist threats that would lead us to go to war. Whether further hearings would be appropriate.

Mr. HAMILTON. That is really outside the mandate of the 9/11 Commission. We did not look at the Iraq war. We acted on the basis of the statutory mandate you gave us, and that told us to do two things: To tell the story of 9/11 as accurately as we could, and, number two, to make recommendations to the American people on how to better protect themselves from a terrorist attack. We did not have the statutory authority to look into the questions of the war. That is an all together different?

Ms. JACKSON-LEE. If you had it, you obviously would have pursued it. If we have it, do you think we should pursue it?

Mr. HAMILTON. That is a judgment you have to make. And as a person testifying on behalf of the 9/11 Commission, I can't really comment on that.

Ms. JACKSON-LEE. And I appreciate your consistency with your testimony.

Mr. Crowell?

Mr. CROWELL. I certainly agree with all of the comments that Mr. Hamilton made with regard to the information sharing environment. I would add, though, that his job is not really framed around the notion that he will have a responsibility for interpreting or moving information form any of the players—federal, state, local—but, rather, that he will assist in the development of the policies, the guidelines, technology, the systems, the training, the environment, if you will, that will allow that to happen within the agencies that have that responsibility today.

In that regard, without the necessary resources and without the necessary oversight to see that he is getting the resources and doing the job, I think we run some risk that this very tough job won't get done.

So I would applaud any efforts by the committee to continue to review what he is doing and what he has to work with in order to get it done. I know he will put a personal effort into it. Will he get the support that he needs from everyone?

With regard to the New York City thing, there is not much that I really can add since I am not currently involved in any reviews that relate to that. And it is certainly not something that Markle looked at.

I just would say that in the case of information sharing, the principal concern is to make sure that the people who have responsibility for taking action, in this case New York City, have all the information. I have no way of judging whether or not they had all the information or not, but the whole purpose of this effort to develop the information sharing environment is to make sure they know whether or not they got all the information and that there is an audit, if you will, of the process that gets that information to them.

Clearly, your question on the hearings with regard to the trail of information are well outside of my responsibilities in the Markle

Foundation or the Markle's current focus, so I won't make any comment on that.

Ms. JACKSON-LEE. Thank you.

I thank Mr. Chairman. I will just self-testify and would think that both Mr. Crowell and Mr. Hamilton, as good Americans, would want us to find out the truth. And so any appropriate hearings that would help us do so in this whole chain of intelligence sharing as well as the allegations that surround us might be helpful in this committee, so I hope maybe we will look into that.

And I yield back, and I thank the chairman and the ranking member.

Mr. SIMMONS. Thank you for your comments on the issue of sharing information. Again, we have had some substantial inquiries into that issue, and I think it is fair to say that sometimes two groups of people can have the same information but draw different conclusions. And in particular, sometimes a trained intelligence analyst will be able to make an assessment based on more information that might place the source of information in question, whereas a non-trained individual might interpret more information as being a better and better source, if that makes sense. And that is why two groups looking at the same information can draw divergent conclusions.

And so the information sharing system has to be sufficiently sophisticated that it takes into account the various backgrounds of the people involved.

That being said, if our witnesses could bear with us for just a few more minutes, we might do a second round, if that is agreeable. I don't know what your time constraints are. Is that agreeable? Thank you very much.

Asking my questions, Mr. Hamilton, a few years ago, in the eighties, we had a lot of excitement here on Capitol Hill focused around the Boland amendment and something called Iran–Contra. I happened to be on the Senate side at the time in a staff position. I believe you were actively involved in oversight on the House side. And what we discovered in that situation was that there was a culture of secrecy that even extended from the intelligence community to the oversight agencies of Congress.

Fast forward 20 years into the post-9/11 situation. That culture of secrecy has broken down somewhat. Information sharing is a buzzword on everybody's lips. But, as you have said, it is still a question of changing the culture.

And how optimistic are you that we can actually change this culture or do we in fact need to add additional sources of information to the equation, namely open sources of intelligence, which are not as highly protected by the secrecy system and the secret bureaucracies and which lend themselves to sharing?

Mr. HAMILTON. Mr. Chairman, I am glad you didn't press me on Iran–Contra. That is too far back for me to remember very well.

Mr. SIMMONS. I won't press you on anything. I just want your opinion.

Mr. HAMILTON. Well, I think?

Mr. SIMMONS. You have been pressed enough today.

Mr. HAMILTON. Yes. I think you have got it very well analyzed, and no one can say at this point in time whether you are going to be able to break down that culture.

I think the important thing to recognize is that the need to know principle, which, as you know from your background, is sacrosanct in the intelligence community, or has been for many years, probably served us very well for many years and was kind of the abiding principle during the Cold War period.

But as you suggest in your question, times have changed an awful lot now, and that principle must not be relinquished but it has to be balanced against the principle of need to share so that you have both principles operating. Sometimes need to know is going to prevail, sometimes need to share.

I think Mr. Crowell put it very well in his testimony when he identified the risk of failing to share. The concentration has always been on the risk of elite or the risk of information getting to the wrong person. That is a real risk. You don't want to deny that. But what we found, I think, over and over again was that the risk is greater in terrorism of failing to share information.

Look, the govern develops, as you well know, millions of bytes of data every minute, all kinds of languages, and we collect mountains of data, which 99.999 percent of it is irrelevant. The task is to pick out those nuggets and to put them together to analyze, collect them and you don't get intelligence information that says, "We are going to hit the World Trade Towers at 9 o'clock on Tuesday morning." You get all kinds of hints, and so putting that all together is difficult. Information sharing is critical.

I am reasonably optimistic that if you give us enough time, we can put it together.

And your final comment about open sources is critically important. Here, again, the intelligence community, as you may know better than the rest of us, has had a kind of disdain for open sources.

If you look back on 9/11 and you trace what happened in the World Trade Towers and the embassy bombings and the USS Cole and the Fatwas from Osama bin Laden, everything was public—everything. We all knew it, we just didn't get it. And so open sources are just as valuable as the secret sources, I believe, and I like your emphasis on adding information from open sources. I think it is critically important.

Mr. SIMMONS. Thank you.

Mr. Crowell, you work for the National Security Agency, or NSA, which at one point was referred to as NSA, "No Such Agency." Twenty years ago when James Bamford did his book, "The Puzzle Palace," Director Lincoln Faurer tried to prevent publication because it was the first book ever written on, "No Such Agency." So this is an organization with quite a reputation for secrecy, even the cables dating back to the Gulf of Tonkin incident have only just recently been disclosed.

How can "No Such Agency" involve itself in information sharing in any useful way?

Mr. CROWELL. Well, I will go back to the earlier comments I made about leadership and its importance in all of this, and I think that if you examine some of the records of the past, you will see

that information has willingly been surrendered by agencies like NSA and others as a contribution to history. I cite, for example, the release of the VENONA papers in 1995.

During my tenure as deputy director, 25 million records were declassified and sent to the archives for use by the American public and by scholars who would study what really happened and return all of that investment to the American people.

So it can be done. It is a matter of culture, not just of secrecy but it is a matter of having a commitment to history and to the importance of information and understanding that history.

You know, during the Cold War, the need to know principle worked primarily because we had a very focused enemy, and we in fact did know who needed to know. I mean, I knew by name the individuals who were responsible for Soviet long-range air and the military officers who were going to respond to any of those threats and attacks. And I talked to them on a regular basis.

This is a different world. It is no longer one in which I would be able to personally divine who needs to know about an arrest of Mohamed Atta on a Virginia roadway. I mean, it is just a different kind of situation.

You talked about analysis and how people can come to different conclusions. I used to tell my young analysts that any two pieces of information would not give you any conclusion. As a matter of fact, I can draw an infinite number of circles through two points on a board. But with three, I begin now to define something that I can say with certainty but maybe one of those thoughts is misplaced, and so the more information I get, the more important it is.

I believe that we are missing a point about terrorism as it relates to how we go after these targets. Now, I am talking well beyond my Markle experience. You are drawing upon my other experience. Terrorism has a process. That process includes target selection, planning, recruitment, training and then execution or command control.

The earlier we can get into that process, the most chance we have of preventing terrorism. And I, for one, do not want to have a system that is just going to forensically document what they did to us. I would prefer to put our efforts into this whole plethora of processes that they are going to be involved in. And that is why members of the Markle Task Force began focusing on information sharing very, very early in our process of deliberation on what needed to be done to make things better.

So the experience of the people in Markle who have served previous presidents and previous administrations in intelligence positions, in law enforcement positions that led us to believe that this new world is not about need to know, it is about sharing information that allows us to know more and come to conclusions earlier in the game. Rather long answer but important question.

Mr. SIMMONS. Very discrete.

The chair recognizes the gentlelady from California.

Ms. LOFGREN. Thank you, Mr. Chairman. I think this has been a very helpful hearing and just a couple of further questions.

Mr. Crowell, you mentioned in your initial testimony that there was an issue relative to involving law enforcement so long as Mr.

Russack reporting to the DNI. Do you have a proposed solution to that?

Mr. CROWELL. Well, there are two possible paths that you can go down. One is that you accept the fact that he is now in the DNI's Office and the president and those involved in the cabinet in other departments come to some agreement about how they are going to cooperate at a high level with the DNI in meeting the needs across the entire government.

The other possibility, of course, is to either reassign him or dual hat him so that he has a reporting chain that gets him closer to these other organizations that must be supported, specifically the Department of Homeland Security and the law enforcement activities of Justice and FBI.

Mr. HAMILTON. Ms. Lofgren, if I may interject, I think this problem of information sharing with state and local authorities is a formidable problem. I know you have been in touch with your state and local officials and they really complain a lot.

Ms. LOFGREN. Yes, they do.

Mr. HAMILTON. And it is a question of building a relationship and building confidence. And it is a two-way relationship. I mean, the DHS and the DNI and all the rest of them have to pay attention to these local officials and the information they are gathering with regard to terrorism. But they also have to impart the information. These relationships cannot be quickly developed. They have to be developed over time. Confidence is the key, building the confidence in those relationships.

And, of course, it is a very formidable problem for the federal authorities because they are dealing with so many municipalities and states across the country. It cannot be expected to be done quickly.

Ms. LOFGREN. And the level of expertise varies widely among the groups.

Mr. HAMILTON. That is exactly right. There are some municipalities that have expertise that matches that federal government and maybe even exceeds it in areas, and there are others that are very rudimentary.

Ms. LOFGREN. I wonder, Mr. Crowell, you mentioned—or maybe you didn't—the Markle Foundation, in any case, suggests, I believe, in the letter to the president that Mr. Russack should chair both the Information Sharing Council and the Information Sharing Policy Coordinating Committee. Is that because there is a lack of coordination between the two bodies? Why is that suggestion being made?

Mr. CROWELL. I am not really an expert on how those two organizations function today, and they are just standing up, but I think it is because the Policy Coordinating Committee in fact is able to set guidelines and policies across the entire federal structure, and it is not just a coordinating body.

Ms. LOFGREN. I see.

A final question for Mr. Hamilton. I have followed for several years now the National Infrastructure Protection Plan, and it is late, we had a November 2 deadline for public comment, and I guess the final plan is supposed to be released in February of next year.

Have you had an opportunity to review the draft plan? And if so, do you have any thoughts for us on it?

Mr. HAMILTON. I have not seen the draft plan but I do have some thoughts.

Ms. LOFGREN. All right.

Mr. HAMILTON. Look, it is a question of priorities. You have got thousands and thousands of targets out here, 85 percent of them in the private sector. What do you decide to protect and what do you decide what not to protect? And the secretary in his confirmation hearing spoke about making hard choices. Well, that is exactly right.

And I understand and you understand how difficult it is to make these choices, because if you choose to protect this chemical plant and not protect this one over here, and then this one over here is the one that is hit, you look pretty bad, you have made the wrong guess.

Therefore, policymakers are very reluctant to make the hard choices on priorities. What I think you have to force the policy people to do is to make those choices as best they can. Otherwise, you are trying to protect everything and you will protect nothing very well. So I think the policymaker has an exceedingly tough job here, but it is a job that a policymaker must do. He has got to decide what infrastructure needs protecting.

A chemical plant in southern Indiana is not going to cause the kind of damage if it is attacked than a chemical plant in the heart of New York City. You have got to make the choice.

Ms. LOFGREN. If I can, I realize my time is up, I understand what you are saying, and it is hard to disagree with that. I think, though, we are far from even that situation where we are mixing in supermarkets and a miniature golf course, in the case of my district, with infrastructure in telecommunications. It is simply never been included.

Mr. HAMILTON. You have to make these judgments on the basis of the best intelligence you have and on the risks that are involved, the vulnerabilities that are involved and the consequences that are involved.

Ms. LOFGREN. Well, I do want to state for the record, because I did ask, that there is nothing to base the miniature golf course inclusion. People should not be fearful of playing miniature golf in the 16th Congressional District.

And with that, I would like to thank both of these witnesses for their excellent testimony. It has been very helpful.

Mr. SIMMONS. I thank the ranking member for all of her assistance and participation.

We have been joined again by the gentlelady from Texas. Did she have a final comment that she wished to make?

Ms. JACKSON-LEE. I wanted to pose the question regarding the October 20 report, Mr. Hamilton, from the Public Discourse Project. The project noted various impediments to the operations of the Privacy and Civil Liberties Oversight Board. Whenever I think of intelligence, I am always concerned about—or the gathering of intelligence, privacy and civil liberties, and of course the board was a creature of the Intelligence Reform Act.

I would like to get your sense of what the ongoing problems with the board that you may be aware of and what role should the board play with regard to information sharing issues we are examining today. Sharing suggests questions dealing with privacy and civil liberties, and I hope that we could track, deface and secure our civil liberties. And what should Congress be doing to address the shortcomings of the 9/11 Public Disclosure Project that has been identified with the board?

Mr. HAMILTON. I think it is very important to recognize that when you have an elaborate counterterrorism strategy, you are greatly expanding the role of government. You are spending a lot more money, you are hiring a lot more people, and government is becoming much more intrusive.

Now, all of those things may be necessary in the current climate, and apparently most people think they are, because we are doing it. But what we said was that in this environment—and I appreciate very much your question—you have to set up a Privacy and Civil Liberties Board that has power to look into these things across government, not just the FBI, not just the CIA but all across the government.

The Congress obviously agreed with that. You put that into the law that was passed.

Now, our concern at this point is that we don't see much urgency here. The president has named the members of the board. The nominees for the chair and the vice chair of the board have not yet been confirmed by the Senate. So far as I know, there is no funding available, no meetings have been held, no staff has been named, no work has been outlined, and no work has begun, no office has been established. So this is, incidentally, 10 months now after the establishment of the board by statute. So I think there is a real urgency here to get a board in place that is a robust board to protect privacy and civil liberties.

Ms. JACKSON-LEE. Let me thank you very much. That is a very forceful response.

And, Mr. Crowell, let me acknowledge and thank you for your testimony. Didn't know if you wanted to comment on that. If you desire to do so, be happy to receive your comments.

Mr. CROWELL. Well, as I mentioned earlier, the Markle Foundation has always considered privacy to be a major part of our entire study. We believe very strongly that wit the right mechanisms, an oversight board, the right policies, guidelines and some technology to help audit and enforce those policies, that we do not have to compromise our right to privacy in order to attain a higher degree of security in this fight on terrorism.

Ms. JACKSON-LEE. Then let me thank both of you for your testimony.

Let me thank the chairman and the ranking member, and may I pile on to both your plates possibly an oversight hearing regarding this board, why it hasn't been energized, if you will. We don't have confirmation rights or privileges, as the Senate does, but it would be important to ask the administration and others why we have not moved forward and whether or not we can help expedite—when I say, "we," they can help expedite and encourage the confirmation of their appointees and as well establishing, as Mr. Ham-

ilton said, an office, a mission, resources and staff I think might be a good parallel to the work we are doing on this committee.

And with that, I thank them, and I yield back.

Mr. SIMMONS. Thank you very much.

Thank you, gentlemen, both for your long and very distinguished careers in service to the United States of America. Thank you for bringing the distilled wisdom of those careers as well as your recent activities to the table to benefit this subcommittee and this Congress. We thank you both very much.

The hearing is now adjourned.

[Whereupon, at 4:20 p.m., the subcommittee was adjourned.]