AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

BUILDING THE INFORMATION SHARING ENVIRONMENT: ADDRESSING THE CHALLENGES OF IMPLEMENTATION

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

SECOND SESSION

MAY 10, 2006

Serial No. 109–75

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

36–987 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) 512–2104 Mail: Stop IDCC, 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

Page

STATEMENTS

The Honorable Rob Simmons, a Representative in Congress From the State of Nevada, and Chairman, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment 1
The Honorable Zoe Lofgren, a Representative in Congress From the State California, and Ranking Member, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment
Oral Statement 2
Prepared Statement 3
The Honorable Jim Gibbons, a Representative in Congress From the State Nevada 17
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island 19

WITNESS

Ambassador Ted McNamara, Information Sharing Program Manager, Officer of the Director of National Intelligence:
Oral Statement 1
Prepared Statement 9

FOR THE RECORD

The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas:
Prepared Statement 27

BUILDING THE INFORMATION SHARING ENVIRONMENT: ADDRESSING THE CHALLENGES OF IMPLEMENTATION

Wednesday, May 10, 2006

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 2:03 p.m., in Room 311, Cannon House Office Building, Hon. Rob Simmons [chairman of the subcommittee] presiding.

Present: Representatives Simmons, Gibbons, Thompson, Lofgren, and Langevin.

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

The subcommittee is meeting today to hear testimony on how the program manager of the Information Sharing Environment, or ISE, is addressing the challenges of implementing a government-wide information-sharing architecture. The development of the Information Sharing Environment, if properly planned and integrated, could turn out to be America's most important tool for preventing terrorism.

Terrorist threat information must be shared broadly, both within the federal government and with state, local, tribal and private sector partners in order to protect our country and the American people against attack. However, there are many challenges associated with creating that environment: incompatible policies, procedures and systems all across the homeland security information-sharing landscape.

The challenge for you, Ambassador McNamara, as the 9/11 Commission put it, is to "unify the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing system that transcends traditional government boundaries."

In my years of service as a CIA officer and as a military intelligence officer doing both collection and analysis, the impression I got in those days was that information was something to be collected and held and not shared widely or broadly, to be stovepiped to the national command authority and to others in order to protect sensitive methods and sources, point one, and point two, in order to get credit for the information collected.

So the culture of intelligence as I knew it many years ago was a culture that mitigated against information sharing. In a post–9/11 environment, I think America has learned and I think our government understands that we have to share information to be safe, but it is an awesome challenge that you face.

Although your tenure has just begun, the program manager was only given a brief 2-year mandate, time is running out. I would be interested in what you think you can accomplish and whether you believe the position needs to be extended or made permanent. As you well know, your job is vital to the security of our country, and I hope you will look to this committee and this subcommittee for any support you need to accomplish the task.

Now I would like to recognize the ranking member of the subcommittee, the gentlelady from California, Ms. Lofgren, for her opening statement.

Ms. LOFGREN. Thank you, Mr. Chairman.

I would ask unanimous consent to put my full statement in the record.

PREPARED OPENING STATEMENT FOR HON. ZOE LOFGREN

Good afternoon. I am pleased that we are turning our attention again to the Information Sharing Environment (ISE) and the obstacles that remain in the way of creating truly effective government-wide information sharing policies, procedures and practices.

We need the Program Manager to get this done as quickly and effectively as possible in order to help the Intelligence Community and State, local and tribal law enforcement share information that could thwart the next terrorist attack.

Accordingly, I'd like to welcome the new Program Manger, Ambassador McNamara, who has taken over these critical responsibilities from his predecessor, John Russack, who testified before this Subcommittee last November.

Mr. Russack's rather abrupt departure this past January came on the heels of his Information Sharing Environment ***Interim*** Implementation Plan—a plan that set new deadlines given the Program Manager's, and the Administration's, failure to complete the work within the time frames prescribed by Congress in the Intelligence Reform and Terrorism Prevention Act.

Much of the delay, it seems to me, came from three main factors: (1) a lack of personnel and other resources within the Program Manager's shop; (2) a lack of buy-in and cooperation from the wider Intelligence Community; and (3) a lack of urgency by the Administration.

The Markle Foundation in fact bemoaned this lack of urgency in correspondence it sent to the President on September 7, 2005, noting, "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."

Accordingly, I look forward to hearing from you, Ambassador, about what you have learned from your predecessor's experience as Program Manager—particularly (1) your assessment of the historical difficulties in getting the policies written and agreed to and to what extent you are facing those same difficulties (and with whom); (2) what lessons you will apply going forward as you take up the reins; and (3) what assurances you can give us that you will be able to meet the new deadlines set out in the Interim Information Sharing Plan we received in January.

I am also very interested in hearing about your reaction to the Government Accountability Office's recent report on information sharing, the progress made to date with the ISE, and the challenges that remain in developing appropriate policies for sharing terrorism-related and sensitive but unclassified information.

Because you are a direct report to the Director of National Intelligence, Ambassador, GAO invited the DNI to comment on its report before publication. Mr. Thompson and I were both disappointed by Mr. Negroponte's refusal to do so—apparently on the ground that GAO's "review of intelligence activities is beyond GAO's purview."

That is nonsense, Ambassador. GAO's review of your work did not involve evaluation of the conduct of actual intelligence activities. On the contrary, it focused narrowly "on the procedures in place to facilitate the sharing of a broad range of information across all levels of government."

Indeed, Guideline 1 of the President's own December 16, 2005 Memorandum for the Heads of Executive Departments and Agencies directs you and other agency heads to "develop and issue . . .common standards for preparing terrorism information for maximum distribution and access."

Those standards—which are now two months overdue—have nothing to do with "intelligence activities." They instead have everything to do with how to "sanitize" intelligence information into a format that can be shared with State, local, and tribal law enforcement.

The DNI's comments frankly would have been a valuable contribution to this Subcommittee's ability to conduct the oversight with which it has been tasked. Indeed, we rely on GAO, the Congressional Research Service, and our respective staffs to help us get the facts so we can make informed policy judgments.

The DNI's decision not to cooperate with GAO—and in other cases with CRS—leaves us with one hand tied behind our back.

Our staffs do good work, Ambassador, but we will be able to do our work even better by having the DNI's and your cooperation with GAO and CRS when they are tasked with reviewing and reporting on your progress. It is their detailed reporting, Ambassador that has informed our process since this Committee's inception and of other Members of Congress for decades.

I therefore look forward to hearing not only your views about the state of progress with the ISE but also your reaction to the GAO report, your thoughts on its recommendations, and how you might implement them as you move forward.

Thank you.

Mr. SIMMONS. Without objection, so ordered.

Ms. LOFGREN. I would just note that we are way behind on where we should be in this area. The last program manager rather abruptly departed, and we have not completed the task in the timeframes prescribed in the Intelligence Reform and Terrorism Prevention Act, as you know.

I think there were a number of issues, and perhaps more that I don't know of, but I am concerned that a lack of personnel and other resources contributed to the shortfalls, as well as the lack of buy-in and cooperation from the intelligence community.

I also think there has been a lack of urgency at the top on this task. As I am sure you know, the Marco Foundation weighed in on this last fall, bemoaning the lack of progress.

While we don't hold you accountable after 9 weeks for that lack of progress, I am looking forward to hearing from you about what you have learned from your predecessor's experience as a program manager, particularly your assessment of the difficulties in getting policies written and agreed to, and to what extend you are facing those same difficulties and with whom, what lessons you will apply going forward as you take up the reins, and what assurances you can give us that you will be able to meet the new deadlines set out in the interim information sharing plan we received in January, or if there are challenges that we can assist you in, that you let us know how we can help.

I am also very interested in the Government Accountability Office's recent report, which I am sure you have looked at. I am very disappointed—and I think ranking member, Mr. Thompson, has just arrived. We were both disappointed by Mr. Negroponte's refusal to comment on the report and felt that his objection was misplaced. We asked for comments not on the collection of intelligence, but on a far different issue, the common standards for preparing

information for distribution and access, not anything that should compromise his mission.

So we do think that it would be helpful to get that comment. We know that you report directly to him. Perhaps you can assist us with that as well. Our staffs do good work, but we will do even better work if we have the DNI's cooperation, and I expect yours, with the GAO and CRS when they are tasked with reviewing and reporting on progress in your office.

So I look forward to hearing not only your views about the state of progress with the IC, but also your reaction to the GAO report and your thoughts on its recommendations, and how you might implement them as they move forward.

Mr. Chairman, I will leave the remainder of my statement for the record, and I yield back.

Mr. SIMMONS. I thank the lady for her comment.

I join her in a shared interest in getting some sort of comment on the GAO report. I think that, again, information sharing is something that traditionally was not focused upon by the intelligence community, but it certainly falls squarely within your domain.

I think that the DNI, as a newly created position, is designed to achieve coordination across traditional bureaucratic lines. So once again, the idea of comments on this report I think is important to us as we do our business.

That being said, we are pleased to have Ambassador McNamara with us here today. I welcome you. We had a chance to talk a week or so ago. You have an extensive background in national security and counterterrorism and have served eight presidents—my gosh, you don't look that old, but anyway—for the last 4 decades, including at the Department of State and the National Security Council.

Following 9/11, Ambassador McNamara was asked to return to government service as a senior adviser for counterterrorism and homeland security at the Department of State and was named program manager of the Information Sharing Environment in March of 2006.

Thank you, Mr. Ambassador, for being here. Your entire written statement will be inserted into the record. We would ask that you try to limit your oral testimony to about 5 minutes so that we can have an opportunity for questions.

Welcome. And you are recognized, sir.

STATEMENT OF AMBASSADOR TED McNAMARA, INFORMATION SHARING PROGRAM MANAGER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Ambassador MCNAMARA. Thank you, Mr. Chairman, and thank you, Ranking Member Lofgren. It is a great pleasure to testify before this subcommittee.

I recognize the committee's and the subcommittee's interest, attention, knowledge and background in this area. So I am particularly grateful for that attention and the commitment that the committee has shown and the subcommittee has shown on this important issue.

I see that my written statement is being entered into the record, so I will refrain from requesting that a second time.

I think that there is no more urgent issue, no more critical issue to our ongoing efforts to fight terrorism than improving our information sharing.

It has been 9 weeks to the day since President Bush designated me to serve as program manager for information sharing. I came back into government service this time, as I did the last time I came back in, because I believed that I was working on an issue of great national importance.

As the senior adviser at the State Department, I worked assiduously to make up for some of the problems that we saw in the immediate aftermath of 9/11. It happens that I am now coming back into government to try and work on a problem that came to the fore as a result of 9/11 that is still with us. I came back into government service to try and make a difference.

But after 9 weeks, I think you will understand that I have not quite tapped all of the different areas of this issue. It is an enormously complex one. But I do have some initial observations that I would like to make here before the subcommittee.

First of all, to clarify a bit what the program manager's office is and what it is not. We are a small office. We were established, as you know, under the IRTPA law, and placed under the office of the director of national intelligence. We are in the office of national intelligence, of the director of national intelligence, but we are not focused only on intelligence.

This office is responsible, as you noted, Ms. Lofgren, we are responsible for all terrorism information government-wide. I have broken this up into what I refer to as five communities of major importance in this effort.

First is law enforcement. And I don't mean "first" in the sense of more important than the others, just to list the five of them: law enforcement, defense, foreign affairs, homeland security, and intelligence. So we serve all five of those communities.

The next thing that we are doing is we are consulting government-wide and we will be advising and recommending to the president how to improve the information-sharing environment. The office is charged with managing and coordinating federal, state, local, tribal and private sector participation in that information-sharing environment for terrorism information.

What we do not do, and what we are not doing, is we are not replacing the operational agencies that implement the Information Sharing Environment. Maybe because of my background, I look at this more or less as an office that has some parallels with the National Security Council.

One of my very wise leaders in those years in the White House told me, we don't do the job here; we make sure the job gets done. We do what we have to do to make sure others do what they must do in order for the job to get done.

I kind of look at that as part of the approach that I take in this program management job, that with a very small staff—we are not quite at our 20, but we are very close to it, and expect to have a full staff, well, we have had larger numbers, and then some people have left and now some are coming in again. We will be at full strength I hope very shortly.

But even at full strength, there is no way without relying on the agencies to carry out their responsibilities, without relying on the state, local, tribal and private sector to do their share. There is no way that 20 people can get this job done alone.

We also will be relying on the Congress, as well as the executive branch, to help us to get the Information Sharing Environment up and running in a manner that is satisfactory to all.

The last point on this is that the office as I see it has not been told to start from scratch to build this. We are at war. There is a struggle going on, a protracted struggle against terrorism. What we need to do is to build on current capabilities, take the best that we do have, use it, and make it better, build on what we have, not tear it down and start from scratch.

The second point and observation, after this very brief period in the job, is that, since 9/11, a great deal of the sharing of national terrorism information at the federal level takes place within the environments of those five communities of interest that I mentioned, that is law enforcement, homeland security, defense, intelligence, and foreign affairs.

It is related to the very important missions and objectives of those communities. Those missions and objectives are important and need to be fulfilled. Increasingly, however, in order to accomplish those missions and those objectives, shared information across those communities is going to be required. That, I think, on the federal level is where most of the difficulty lives, in the sharing of information intercommunally, so to speak.

Within the communities, I think there is fairly good sharing of information, within each of those five communities. But inter-community, across the communities, I see where there is great need for and great possibilities for improvement.

A third observation: Given that the terrorist threat and other post-war challenges are as strong as they are, it is clear to me, and I think it is clear to senior officials in the executive branch, that the old ways of doing business are inadequate and have to be changed. We have to integrate. We have to share more. Not doing so was a failure that I think was correctly cited as a major defect by the 9/11 Commission.

So let me very briefly share with you some of my initial high priority items that I want to pay attention to in these first few weeks.

First is standardizing government-wide SBU procedures and practices around the entire federal government.

Secondly, I think we need to establish a network of state and urban area fusion centers. We have to create a national system that is effective and efficient in sharing information and empowering all levels of government to greater efforts and greater success in this protracted struggle.

Thirdly, we need to develop an information-sharing environment budget investment strategy.

Fourthly, we need to deploy the initial capabilities for an electronic directory of services, an EDS.

And fifthly, we need to develop guidelines to protect privacy and other legal rights for American citizens.

I don't want by saying to this to suggest that we have been inactive up to now. In fact, as I look at it, and I saw it immediately

after 9/11, within 3 weeks I was on duty at the State Department following the 9/11 events, I think we are much improved over what we were doing back then in terms of information sharing.

We have a National Counterterrorism Center, for example. We didn't have that back then. The National Counterterrorism Center is now being accepted by agencies and by the leadership of the executive branch as the focal point of our sharing of national intelligence and other information with respect to terrorism.

We have a Terrorist Screening Center that unites numerous databases that was quite clearly a problem during the period immediately before 9/11. Those databases existed, but were not united. They were not integrated and there was no one place to go to find out information about terrorists. The Terrorist Screening Center provides that capability now.

I think the fusion centers that have been set up by the states and urban regional authorities are important elements in solving the problem of sharing of terrorist information. I will have more to say about the fusion centers in just a moment.

I think the Department of Homeland Security is now up and running. It has Web-based portals and other tools that are great improvements over what we had in 2001. The Department of Justice law enforcement information-sharing program enhances sharing across law enforcement jurisdictional boundaries. We didn't have that before.

The director of national intelligence is transforming the data-sharing of the intelligence community in a way that is very, very helpful for the information-sharing environment. And the Department of Defense, in a step that I think could be an example for other large agencies, the DOD now has an information-sharing executive, something that would have been unheard of before 2001.

Let me take a moment or two to address one aspect taken from my written statement, which both of you have referred to, and which I think is central to our being able to resolve some of the major problems of information sharing. I think more must be done by all entities at all levels to create an information-sharing environment that is a truly national system, one that links state and urban fusion centers with each other, as well as with the federal government.

To do this, resources are going to be needed at all levels of government. It won't happen automatically and it will take an enormous amount of cooperation. I sense that there is a feeling both at the federal, state, and local levels that such cooperation is necessary and will be forthcoming.

I think what we are looking for is an integrated, federated approach that delineates responsibilities of the federal, state, local and tribal entities, as well as the private sector. The fusion centers are being created in order to truly share information that is useful and beneficial to all of the government entities involved. That federated approach, that system that is a national system, is my vision of what the future ISE ought to look like, in very broad terms.

State, local and tribal entities are critical partners in our nation's efforts in counterterrorism. They are consumers and producers of terrorist information. As consumers, they need the information to be brought to them in a more timely, more actionable, more concise

and usually unclassified form. It needs to be delivered efficiently. We are moving in that direction on all of those fronts, but I think we need to move faster and I intend to see that we do move faster.

As producers, assistance is needed so that they can bring together information at the state and the federal level that is useful to state and federal authorities and that effectively and efficiently moves the information through the system. That is another objective, I think, that we can aim for in this national system that I referred to.

Many state and urban governments have begun gathering, analyzing and sharing information, using the fusion centers that now exist. I think this is a very beneficial approach and I think it is one that we can usefully look at here at the federal government as benefiting us as well.

I strongly support fusion centers. I expect them to become central components of our national capability to gather, to analyze and to disseminate actionable information. As chair of the ISC, the Information Sharing Council, I intend to keep in close contact with state, local, tribal and private sector partners through regular meetings with them, and by inviting them to work closely with the Information Sharing Council in the coming months.

Let me wrap up with a few closing comments.

A critical question for implementing the Information Sharing Environment is how best to deliver capabilities today, while we continue with this protracted struggle, while at the same time addressing the myriad of policies, processes and technology differences among multiple organizations that must be done if we are to perform the disparate missions that those organizations perform.

These differences pose challenges to implementing an ISE. Those challenges, among others, are incompatible policies and procedures; classification problems; access by individuals that need access; vetting to grant clearances; security and privacy problems that have arisen. These and many more are going to have to be addressed.

To realize the ISE vision, these impediments are going to have to be dealt with, I think through adopting common policies, common processes, common data and technology standards and guidelines that will be set for all of the ISE participants.

A comprehensive and complex problem such as this needs a transformational effort. It is going to require time to fully implement. However, the information sharing is such an urgent national imperative that I believe it can and will be moved forward rapidly. That certainly will be my goal and that will be what I will do in this job. Much has been done, but much more needs to be done. We owe it to the American public to fix this problem.

Let me make two comments based on what you have both said in your opening comments.

First of all, I fully agree, Mr. Chairman, that the biggest problem is not technology. It is culture. You pointed out much more clearly than I could have that the culture has built up over many, many years, in fact decades. It was a culture that worked well for the Cold War. It is a culture that does not work well for the post–Cold War. It is time to change it.

To change the culture, it means changing people and institutions. That is the major problem I think I face. If we were pushing the

bounds of technology, I would have listed technology. I think the technology is the least of the problems of those three that I have listed.

With that, I will close and be delighted to answer and respond to any of your questions or comments.

[The statement of Ambassador McNamara follows:]

FOR THE RECORD

PREPARED STATEMENT OF AMBASSADOR THOMAS E. MCNAMARA

Introduction

I'm here this afternoon to provide you my plans for a terrorism information-sharing environment (ISE) in which terrorism information can be shared broadly, effectively and seamlessly to protect our nation. Our ability to share terrorism information across all levels of governments and the private sector is fundamental to the success of our efforts to defeat terrorism. Congress has provided us a legislative basis, the President has provided more specific guidance, and my predecessor has provided an interim implementation plan, the final that will be delivered to Congress in July 2006. Now it is time to begin building capabilities that make the ISE operational to the men and women who support the national effort to detect, prevent, respond to and recover from acts of terrorism, and to convey the sense of urgency with which the Information Sharing Environment (ISE) must be developed.

I want to say, up front, that I assumed the position of Program Manager for the ISE on March 15, 2006, approximately two months ago. I thank you for this opportunity to share with you my initial thoughts and reflections. In time, I look forward to sharing with you more developed and detailed thoughts and opinions. As you may know, the Program Manager has a responsibility to report this summer to the President and to the Congress on the implementation plan and guidelines. This is a short timeframe, but I take my responsibility seriously. I also owe it to the President, and to my other superiors and colleagues to listen to and work with them before coming before you and speaking on behalf of myself and them.

However, I know that I have a responsibility to the Congress. In the past, on the several occasions when I have held senior positions in government, I have had a policy of consulting and working closely with the Congress to keep you appropriately informed of my work. I intend to continue that policy in this position. I have already told my staff that we will offer regular briefings to Members and staff of the committees that exercise oversight responsibilities for the ISE and I am happy to report that we have already started that process.

Role of the Program Manager

As the Committee is aware, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) established the office of the Program Manager and designated by Presidential Directive to assist, in consultation the Information Sharing Council (ISC), in the development of polices, procedures, guidelines, rules and standards for the ISE at the Federal level, and to coordinate closely, in collaboration with the ISC, with State, local, and tribal governments and the private sector and relevant foreign partners, in the development and operation of the ISE. The Program Manager must also manage the development and implementation of that same environment by monitoring and assessing the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency, and policy compliance.

To do all this, the Office of the Program Manager is currently made up of about 15 Federal employees, plus contract support, and is situated within the Office of the Director of National Intelligence, although we are not an intelligence office. My authorities are government-wide with respect to overseeing development of the ISE. To be successful, the ISE must satisfy the needs of Federal, State, local, and tribal governments, and the private sector. Given the size of the office, you will appreciate that we do not operate as another bureaucratic layer that could impede progress and we do not substitute for responsibilities that each agency has to implement the ISE. We have limited time (two years) and a specific mandate. Each Federal agency, and State and local agencies, must take the responsibility for implementing the ISE. Our office will, however, do our best to oversee, manage, facilitate, and coordinate agency implementation of the ISE and information sharing mechanisms.

To advise me in this effort the IRTPA also established the ISC, which I chair, and which is composed of senior officials from 17 agencies and departments of the Federal government. To facilitate coordination with state, local, and tribal officials in

development of the ISE, we have established a State, Local and Tribal Subcommittee. It is my intention as chair of the ISC to keep in close contact with State, local, tribal, and private sector partners through regular meetings with them, and by inviting them to work closely with the ISC in the coming months.

To understand the complexity of the ISE one needs to realize that it affects the operations of a very large number of agencies of the Federal government. I divide those agencies into what I call five "communities." Those communities are: the intelligence community, the law enforcement community, the defense community, the homeland security community, and the foreign affairs community. Each community is a collection of departments and agencies with a specific focus on terrorism and terrorism related information. The development of the ISE will impact a large number of similar governmental entities at State, local, and tribal levels of government, and many entities in the private sector.

WHAT THE ISE MUST DO TO SUCCEED

The ISE must accomplish four key things. First, it must facilitate the establishment of a trusted partnership between all levels of government, the private sector and our foreign partners to mitigate the effects of terrorism against the territory, people and interests of the United States of America. The ISE, as we envision it, will enable the trusted, secure, and appropriate exchange of terrorism information, in the first instance, among those five communities, and also to and from State, local, and tribal governments, foreign allies, and the private sector, at all levels of security classifications.

Second, the ISE must promote an information sharing culture that eliminates information gaps between partners and facilitates the creation and sharing of validated, actionable information. We want to get the right information, to the right people, at the right time to ensure success within a system of rules established to protect the information privacy and other legal rights of Americans as well as sensitive sources and methods. I believe that right now the main problem is not too little information flow from the five federal community members to State and local ISE elements, but too much flow of uncoordinated information to the State and local levels. There is, also, too little flow of the right kinds of information in actionable form. Part of the cultural change we need is for all participants at all levels of government and the private sector to understand that the purpose of the ISE is to serve and satisfy consumers of information, who are at the same time all members of the ISE. In contrast, there is little information flow from the local and tribal levels to the State and Federal levels. This means that valuable information potentially is being wasted because it is not reaching the proper consumers.

Third, the ISE must function in a decentralized, distributed, and coordinated manner. In effect, we need to implement a federated ISE that incorporates the full cooperation and coordination of the Federal, State, local, tribal, and private sectors entities. This way ISE participants can be governed by an agreed set of common standards and practices that conform to mandated guidelines. Where these cannot be common, they must, at least, be compatible. Where necessary and consistent with proper information flow, these standards and guidelines must take into account the needs and desires of the constituent elements, including the security, where required, of the information in the ISE. The ISE should provide direct, continuous, online access to information that is readily available for analysis, investigations and operations without sacrificing privacy and security.

Finally, the ISE must be developed and deployed incrementally by leveraging existing information sharing capabilities and deploying centralized core functions and services to provide new capabilities and value-added business benefits to all ISE members. Only by building from what we now have functioning can we continue to share information effectively and uninterrupted.

ISE Implementation Approach

A critical question for implementing the ISE is how best to get it up and running while addressing the myriad policy, process and technology differences among multiple organizations tasked to perform disparate missions. These differences pose challenges and impediments which include: conflicting or incompatible policies, processes, and procedures for information classification, access vetting, security and privacy; incompatible or non-interoperable legacy systems and data formats; conflicting approaches to information sharing; and conflicting management structures for overseeing information sharing partners.

In many cases these differences have evolved over decades. It is not realistic to think that we can overcome them in a short period of time. But, we must proceed with intelligent, focused, and determined energy and dispatch. I believe this means that we must prioritize the many tasks before us. I am in the process of deciding

those priorities. In the past few weeks I have set several priorities—not all of those that need to be set, but several of the highest ones. Let me turn to those areas now.

To realize the ISE, the challenges mentioned above, must be addressed. Common policy, process, data and technology standards for terrorism information sharing must be implemented across all ISE agencies. The President's December 16, 2005, Memorandum entitled, *Guidelines and Requirements in Support of the Information Sharing Environment* (The President's Memorandum) established the ISE requirement to "implement common standards across all agencies regarding the acquisition, access, retention, production, use, management, and sharing of information." The comprehensive and complex nature of such a *transformational effort* will require significant time to fully implement. However, the ISE is an urgent national imperative that cannot wait for such an effort to be completed before enhanced information sharing is achieved. The key is to achieve initial operating capability for the ISE in the short term, and continue to build on existing capabilities, while the comprehensive, transformational effort proceeds in the longer term.

We have begun the work to assist in more clearly defining roles and responsibilities among departments and agencies by developing policies, business processes, and technologies to implement the ISE. There are already capabilities and initiatives underway to improve the Nation's ability to share terrorism information.

- The DNI has enabled the National Counterterrorism Center (NCTC) to step up to the Federal leadership role that the President and Congress have laid out. Admiral Scott Redd and his staff hold video teleconferences three times a day with analysts across the homeland security, law enforcement, intelligence, foreign policy, and defense communities. NCTC collects intelligence information and analysis from 28 different government networks which come into NCTC and post it on a single website where it is then accessible by individual agencies.
- The Terrorist Screening Center (TSC) used to receive terrorism information from NCTC via a computer disk. Today, the TSC receives this information directly from NCTC in controlled unclassified format and electronically. This has greatly enhanced the ability for TSC to efficiently produce the Terrorist Watch List and distribute it to local law enforcement partners.
- Fusion Centers have been established—or are in the process of being established in 42 states. Additionally, a growing number of localities—particularly major urban areas—are also establishing similar centers. State and local fusion centers are a critical component of the ISE because they can dramatically enhance efforts to gather, process and share locally generated information regarding potential terrorist threats and to integrate that information into the Federal efforts for counterterrorism. Federal law enforcement is working closely with these Fusion Centers.
- The Department of Homeland Security (DHS) offers a series of web-based portals and other tools that support information exchange, file sharing and chat services among State & local law enforcement, emergency operations centers, 53 major urban areas, local, state or regional intelligence fusion centers, and the private sector.
- Department of Justice's (DOJ) Law Enforcement Information Sharing Program (LEISP) implements a unified Department-wide technology architecture to enable DOJ partnerships with State, local, tribal and Federal law enforcement agencies, and identifies which IT investments to support. LEISP enhances DOJ's ability to share information across jurisdictional boundaries.

The Department of Defense (DOD) has recently designated a full time Information Sharing Executive; an initiative I intend to encourage other large agencies to follow. DOD has also continued to invest in the development of Global Information Grid (GIG). The GIG is being developed in concert with ODNI IC Enterprise Architecture (ICEA) to support all DOD, National Security, and related IC mission and functions in war and peace.

But, I freely admit that there are many areas where we need to do better. I intend to determine the highest priority areas and to devote the time, resources, and commitment to make near term and long-term improvements in these areas. Among the highest priority matters that need attention are the following: defining government-wide standards for Sensitive but Unclassified (SBU) information handling; assisting in the development of a national strategy that defines federal collaboration with State and local fusion centers; developing an ISE budget investment strategy; deploying of initial capabilities for Electronic Directory Services (EDS); and developing guidelines to protect the privacy and other legal rights of Americans.

Sensitive But Unclassified Information Efforts

The President's Memorandum contained specific direction related to the standardization of Sensitive But Unclassified (SBU) information. Specifically, Guideline 3 required each department and agency to inventory existing SBU procedures and their underlying authorities across the Federal government, and to assess the effectiveness of these procedures and provide this inventory and assessment to the Director of National Intelligence (DNI) for transmission to the Secretary of Homeland Security and the Attorney General. Guideline 3 further charged the Secretary of Homeland Security and the Attorney General, in coordination with the Secretaries of State, Defense, and Energy, and the DNI, with submitting recommendations for the standardization of such procedures for terrorism, law enforcement, and homeland security information. In response, an interagency working group led DHS and DOJ, working with my office, initiated a significant multi-agency effort to address these issues that I believe will lead to tangible improvements in the way SBU is marked and handled.

This working group completed the initial inventory task in March 2006, and is in the process of evaluating the results. The data collection also includes responses by agencies to the Government Accountability Office's (GAO) similar request, supplemental material volunteered by agencies, and publicly available data. The working group will use the analysis of the SBU inventory as well as review of related literature, including SBU reform proposals of concerned communities of interest, recommendations of the GAO, the Congressional Research Service (CRS), and a wide range of other legal, academic and policy sources to develop recommendations for submission to the President regarding the standardization of SBU procedures by June 2006.

Preliminary assessments indicate that there are no government-wide definitions, procedures, or training for designating information that may be SBU. Additionally, more than 60 different marking types are used across the Federal Government to identify SBU, including various designations within a single department. (It is important to note, seventeen of these markings are statutory.) Also, while different agencies may use the same marking to denote information that is to be handled as SBU, a chosen category of information is often defined differently from agency to agency, and agencies may impose different handling requirements. Some of these marking and handling procedures are not only inconsistent, but are contradictory.

Initial evaluation of the inventory data also suggests that different agencies rely on different authorities as a basis for developing marking and handling procedures. For example, some agencies rely on Freedom of Information Act (FOIA) exemptions to mark SBU information, while other agencies may apply markings to SBU data not necessarily subject to a FOIA exemption. Information characterized as SBU also can range in levels of sensitivity.

In coordination with my office, the Secretary of Homeland Security and the Attorney General will submit recommendations to the President in June on standardization of SBU procedures for terrorism, homeland security, and law enforcement information. The Guidelines also require that the DNI, in coordination with the Secretaries of State, the Treasury, Defense, Commerce, Energy, Homeland Security, Health and Human Services, and the Attorney General, and in consultation with all other heads of relevant executive departments and agencies, submit recommendations and standards applicable to all Federal controlled unclassified information by December 16, 2006. While many improvements can be achieved by Executive Branch actions alone, these recommendations may also involve recommendations for legislative changes.

The PM, in managing the development and implementation of the ISE, will closely coordinate all efforts under the President's guidelines to ensure progress, consistency, and effectiveness, and to ensure that all partners in the ISE benefit from the implementation.

State and Local Fusion Centers

State, local and tribal governments will continue to ensure that personnel responsible for protecting local communities from terrorist attacks have access to timely, credible, and actionable terrorism information. A number of State and local governments have sought to address this need for actionable information by establishing "information fusion centers." These centers coordinate the gathering, analysis and dissemination of law enforcement, public-safety and terrorism information. As I mentioned, Statewide fusion centers have been established, or are being established, in 42 states.

There is, however, no national strategy that defines federal collaboration with these centers. Each State and local fusion center has developed it own way of interfacing with the various Federal entities involved in terrorism prevention and re-

sponse efforts. Additionally, fusion centers rely on multiple channels to exchange terrorism information with the various Federal entities involved in investigatory, prevention, response, and recovery activities. It is one of my highest priorities to greatly improve this situation.

I strongly support the concept of fusion centers and I expect these centers to become critical components of our national capability to gather, analyze, and disseminate actionable information. State and local fusion centers across the nation should achieve a baseline level of capability. The Department of Justice Global Justice Information Sharing Initiative/Department of Homeland Security Advisory Council "Fusion Center Guidelines" were developed with Federal funds and through a collaborative process involving Federal, State, and local officials and may provide this useful baseline. I intend to help the collaborative process move forward by working with DHS, DOJ, DoD and others to develop an integrated Federal approach that describes how the various Federal entities (law enforcement, homeland security, defense) can interface with state and local Fusion Centers.

Guideline 2 of the President's Memorandum requires the Secretary of Homeland Security and the Attorney General, in consultation with the Secretaries of State, Defense, and Health and Human Services, and the DNI (which includes the Program Manager), to perform a comprehensive review of the authorities and responsibilities of executive departments and agencies regarding information sharing and to submit to the President a recommended framework for sharing information between and among executive departments and agencies and State, local, and tribal governments, law enforcement agencies and the private sector. This framework is to be submitted to the President through the Assistant to the President for Homeland Security-Counter Terrorism and the Assistant to the President for National Security in June 2006.

ISE Budget

In March of this year, OMB issued a budget data request (BDR) in support of the Information Sharing Environment. This request provided to my office information on the inventory of systems, programs and architectures that support terrorism information sharing. The BDR requested corresponding FY06 and FY07 budget information for those systems, programs, and architectures.

My office will use this data to develop an investment strategy for the ISE to shape future budget decisions through the identification of gaps and opportunities to better enable terrorism information sharing. Such mechanisms could include system modification and/or enhancement, as appropriate; new investments and acquisitions; and strategic leveraging of existing programmatic resources.

Electronic Directory Services (EDS)

On March 31, 2006, we released the initial capability for the ISE electronic directory services (EDS) within a classified environment—something that has not existed before. The approach to EDS is incremental, starting first at the federal level to provide directory services information within a classified environment; and then eventually creating the capability at the SBU level. This first delivery of the EDS provides contact information for Counterterrorism related watch centers, and is similar to a telephone book?s "Blue Pages" listing. These Blue Pages are available to anyone who has access to the Sensitive Compartmented Information (SCI) and SECRET security domains. The Blue Pages reflect agreements and cooperation among the Information Sharing Council members; in particular, the Office of the Director of National Intelligence (ODNI), who is hosting the Blue Pages in the SCI security domain, and the Department of Homeland Security (DHS), who is hosting the SECRET security domain Blue Pages.

My staff has a strong sense of urgency to deliver full EDS-People and Organization (EDS–PO) capabilities defined as a set of registries that share a common, trusted, and up-to-date view of people and organization information, which includes identification of necessary attributes and standardized metadata on people and organizations, to assist in locating people and resources with relevant knowledge about intelligence and terrorism information. Current efforts are focused on White and Yellow Pages and are defined below:

White Pages Concept—Name, personal attributes and at least one method of contact for named personnel. Additional contact information may include phone numbers, email addresses and postal addresses. For urgent needs, an alternate 24/7 method of contact may be included. Attributes may include such information as skill set, clearance level and areas of expertise. For certain users, some attributes may not be viewable or searchable.

Yellow Pages Concept—Organization and contact information, which may include description of roles and responsibilities and organization charts. For urgent needs, an alternate 24/7 method of contact will be included. These may include a pointer

to the organization directory. For certain users, some organization attributes may not be viewable or searchable. The EDS–PO Implementation Plan developed in February 2006 calls for implementing the Blue Pages on the Sensitive But Unclassified (SBU) domain by end of July 2006. Due to lack of cohesive and centralized governance structure of the SBU domain, the solution for SBU Blue Pages is more complex than the SCI or SECRET domains. As a result, the SBU Blue Pages data will be a subset of that available on the SCI and SECRET Blue Pages.

By the end of October 2006 we plan to increase existing ODNI White Page capability at the SCI and SECRET domains to include non-IC information. Also planned for October 2006 is the initial iteration of Yellow Pages at the SCI and SECRET domains. Currently, the implementation team is working with the Departments and Agencies to identify the cost of making appropriate content available to the right users.

Guiding Principles

Creating a culture of information sharing within the various departments and agencies of government will require us to assign dedicated personnel and resources; reduce disincentives to sharing; and to hold our senior managers and officials accountable for improved and increased sharing of information. And it will require a great deal more. I have established the following principles to guide the efforts of each of the entities engaged in developing the ISE.

- We will deploy a decentralized, distributed and coordinated model so that the handling of terrorism information in the ISE will take place directly among users, using a web-enabled, network model accessible to each of the stakeholders in information sharing.
- We are working to develop and use common standards and best practices to promote maximum distribution and access to terrorism information, including the appropriate method for government-wide adoption and implementation of these standards.
- We will deploy the ISE on the premise of information "access" by using the concept of "shared information space". In this model, information is a community asset—not the property of a particular agency. We will ensure security and privacy safeguards are in place to protect sources and methods while ensuring the privacy and other legal rights of Americans are protected.
- We will operate on the basis of "risk management" not "risk avoidance" to balance the risk of inappropriate disclosure of information against the risks associated with inadequate information sharing. This is the approach used now within most departments and agencies, and it should be used within the ISE.
- I want to build trust through auditing, performance evaluation, accountability and transparency. Achieving that end will require significant training and education as well as strict enforcement of policies and processes relating to the handling of information that is shared.
- Finally, we are striving to facilitate easier user access to terrorism information for users faced with a wide variety of systems and tools and by different policies, procedures and access controls. I want to simplify ISE access for users regardless of their point of entry into the environment through the deployment of open standards and technologies and appropriate policies related to user access.

I want to thank the Members of this committee for your continued support and dedication to this important issue and look forward to working with you on building an enduring capability for information sharing for this Nation. I welcome and look forward to your questions.

Mr. SIMMONS. I thank you, Ambassador.

I have some questions, and then we will go back and forth to the members.

My question is a follow-on to what you just mentioned, and what I mentioned in my opening statement, the issue of culture. When we talk about the five communities, we could just as easily talk about the five bureaucracies, if you will: intelligence, law enforcement, defense, homeland security and foreign affairs.

Many country teams overseas have four of those five communities at the country team table. As somebody who served on country teams, as I am sure you have, you know that everybody gathers, and you know that everybody listens to the ambassador and they all smile at each other, and they all plan to be at the cocktail

parties, but not necessarily a lot of sharing unless there is really strong leadership at the table.

To those four, we add the fifth, which is homeland security, and we have a new dimension here, which is the non-federal dimension. The homeland security dimension goes to state, local and tribal. So you are not just dealing at a federal level. You have other levels of government. One could argue that law enforcement goes to state and local, potentially, through state police and municipal police, for example.

One could argue the defense community also has a state component through guard and reserve, principally through the guard. So there are multiple dimensions here, multiple bureaucracies, and multiple tasks at a vertical and a horizontal level.

With your 20 people, what tools do you have? What carrots and sticks do you have to ensure that this complicated, I think of it like a lion tamer, almost in a circus, you know. What kind of a whip can you crack? What kind of incentive can you provide to ensure that these people are sharing, and in a productive fashion?

Do you have the tools necessary to get the job done? Can you enforce the rules, if you will, or provide incentives for those who cooperate and punishments for those who don't?

Ambassador MCNAMARA. Well, let me start by saying I understand the country teams concept. I think what I am talking about here when I talk about that national system that needs to be set up for information sharing is a kind of country team. It just happens that it is our country here back home, rather than our country as projected overseas.

Indeed, all five communities are present in that country team, if I may note. The country team that is now part of, or the element of the country team that is now part of homeland security includes the Coast Guard, the Bureau of Customs, and other elements that are present overseas in many of our embassies, Transportation Security, et cetera.

Do I have the tools? I do have the tools. I do not have tools to enforce the rules. I have tools to recommend the rules, and the president will make the rules, and I will be enforcing his rules. But when he makes the rules, that also means that every member of the Cabinet and sub–Cabinet level and on down is to obey those rules also.

What tools I have are calling attention to those who don't follow whatever the rules are, as the rules are established. Number two, I have the ability to recommend budgetary changes. I have the ability to go to the OMB and to the president with a budget strategy for information sharing. That means that I do not have to pass my recommendations through any particular agency in order to get them heard at the highest levels.

If I might address in a little bit more detail the relationship with the DNI, I do report to the DNI on matters that directly relate to the intelligence community. But the legislative mandate that I operate government-wide means that I must also operate in those communities which are not under the direct authority of the director of national intelligence. He and I have discussed this and we understand perfectly well that I go through him sometimes, and other times go in another path.

As for support, thus far in a very short time that I have been here, I have spoken with almost all of the Cabinet-and sub–Cabinet-level officials in the major agencies that I am working with. By that, I mean Homeland Security, DNI, Defense, Justice, FBI and others. In fact, in some cases I have seen them several times since I started.

I expect to work at that level and to continue to dialogue at that level in order to get what I believe to be my job done. That, I think, will be a significant factor in how well and also how fast we move forward.

Mr. SIMMONS. Thanks very much.

The chair recognizes the ranking member, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman.

And thank you, Ambassador, for being here with us today.

As you probably know, the National Governors Association last month surveyed state homeland security directors and found that 60 percent of them were either somewhat or completely dissatisfied with the specificity of intel information they were receiving from the federal government. So I have specific questions.

We have heard now for several years, obviously not from you, about the culture and dialoguing and the like. But I am one for setting protocols and rules, and then you can get some enforcement.

So first, the president directed in December of last year that the DNI, and I think through your office, would come up with standards to convert classified terrorism information into a sanitized format that could then be shared with state, local and tribal enforcement. I think the deadline was mid–March. We didn't make it. We have a new deadline of June 14.

Are we going to make that deadline? Where are you on it? If not, what can we do to help you make that deadline?

Ambassador MCNAMARA. I expect to make the deadline. I would be less than candid with you if I said I was absolutely certain at this point, after only 9 weeks on the job, that I have in effect gathered in all of the information I need in order to make that report. But by June, I intend to make that report.

That report will include recommendations with respect to classified information, and I think even more importantly, what to do about the unclassified, but controlled information.

Ms. LOFGREN. That is my second question, because, as you know, the GAO identified 56 different sensitive but unclassified designations across the government, and identified that there are no government-wide policies and procedures for making those designations. I think your office is to develop those procedures. In the absence of that, each agency is kind of ad-hoc'ing it.

We learned from the GAO that there is no review process, and further that there is apparently no legal standard that has been developed for this either, which means that ultimately the sensitive information is going to end up being published unless we have some legal hook for keeping that from happening.

So I am wondering, I am sure you have read the GAO report, the deadline for that is December of this year, but I am hopeful that we can get something done prior to that time. What are your thoughts on that? Where are you? Do you have the resources necessary to do that? And how can we help?

Ambassador MCNAMARA. I think we can meet that deadline, and I hope we can come in early. I intend to make some recommendations in June. That, as I listed in my top priorities, that was one of them.

A couple of comments. Here is another example of how we are working against the culture. It is a culture that was quite an effective and useful culture when it was working during the Cold War.

Ms. LOFGREN. If I may, I don't think we are disagreeing on the culture issues, but if we don't have any policies, then it is very hard to insist that they be adhered to.

Ambassador MCNAMARA. That is right.

Ms. LOFGREN. There is no argument on the culture, but you have to have some rules that you ask people to obey.

Ambassador MCNAMARA. And that is what I intend to make recommendations on in June, and then again in December. Specifically, I think what has happened is indeed we have since the GAO report was written continued to get information with respect to the SBU problem, and 56 is a low number. We are well above that now, and I expect the number will go up in the coming weeks as more information becomes available to us.

I think what we have to do, and for this I was referring back to the Cold War, we thought the classified information during the Cold War, national security information needed to be classified, and we created a rational system which we then propagated throughout the federal government, and we insisted that everybody observe that system.

In the post–Cold War period, it seems to me, that during the Cold War we said, with respect to nonclassified matter, do whatever you want with it. We are not interested; that is not a danger; that is not a problem; do what you will. So for 50 years those 56 or 60 or 70 systems got built up.

Now comes the time, I think, to set up a system which in some respects would mimic what we have been doing in classified information, and that we will restrict the use of the SBU to certain categories that need to be controlled, and there are some legislatively mandated, and in some cases via regulation, truly do need to be controlled.

But the great majority of the information which is now controlled can be put in a simple unclassified, uncontrolled category, it seems to me. And that is the system that we are trying to put together, a rational limited set of categories that, like the system that we have for classified national security information, can be applied to controllable information, but leave most of it as fully unclassified.

Ms. LOFGREN. My time has expired. I appreciate the chairman's indulgence. We will do a second round, and I will ask some further questions.

Mr. SIMMONS. The distinguished gentleman from Nevada, a member of our Intelligence Committee.

Mr. GIBBONS. Thank you, Mr. Chairman.

Ambassador McNamara, welcome. Thank you for your service, and I especially thank you for voluntarily coming back into government and trying to put your arms around a very difficult issue.

As I look out there, and I look at all of the agencies, and certainly can understand the inability of some agencies to work well

with others, I am aware that there is a degree of mistrust between various organizational agencies within the federal government.

You are telling us that already we have intra-agency cooperation that is fairly good. I still see this mistrust out there, though, on information sharing, either because it is going to jeopardize the source or method by which we receive that information, or it will jeopardize the utilization of that information in, for example, the prosecution of a case.

What can we do to bridge that mistrust so that we can get this information out there without giving the sense that we are forcing somebody to sacrifice either the prosecution of a terrorist or result in the loss of a source or a method by which the information is generated? What needs to take place to build that bridge?

Ambassador MCNAMARA. Again, after 9 weeks, I hesitate to give you a full answer to that, but I think I see, based on prior experience, a way out of this conundrum. And that is that we now practice a system of information sharing within agencies that is called "risk management." That is to say, you understand what the nature of the information is, how sensitive it is, and then you manage that information according to certain risk criteria. Within agencies, that has been done now for many years, a decade or more, depending upon the agency.

What is interesting is that the risk management approach is not practiced between agencies very much. Occasionally it is, and on a limited basis. Instead, what is practiced interagency is risk avoidance. That is to say, if there is any risk, no sharing. It seems to me to be irrational and illogical to practice risk management within an agency of many tens of thousands of employees, and not risk management with respect to other agencies where the clearances and the process of vetting the employees is very similar, and in some cases identical.

So I think the way to get from where we are now in sharing information among the various federal agencies, and indeed by extension down to the state level, is to change the culture of risk avoidance, a zero-risk approach, and consider what we are doing within agencies, within the CIA, within the Department of Defense, within the Department of Homeland Security, within the Federal Bureau of Investigation, and practice risk management.

Mr. GIBBONS. Now, in your position, are you comfortable that that can take place? Because it reminds me of what my mother told me when I was a young boy about changing the way I did things. She said, "Jim, change is not a difficult thing if you are willing to let go of the old way you do things." I am sure that there are some institutional problems within those various agencies that will make this a challenge, and I am sure we see that even today.

My time is about to run out. I wanted to ask you one final question here. We talked about state fusion centers. I think, along with you, they are very, very important to the future of our intelligence network nationwide.

What gives you the comfort of knowing that when we have 50 state fusion centers up and running, that we are going to be able to have the same bridged sharing of that information among those 50 states and in many territories that would also be sharing in those as well?

Are we doing things today to set the proper stage so that these states when they begin to set that up—and I know my state is looking at doing one, modeled after what California has done. I want to make sure that the federal government is playing an active role in making sure that we are all interoperable, so to speak, for that information sharing.

Ambassador MCNAMARA. I think the answer, Congressman, is that yes we have started down that path. Indeed, the Department of Justice and the Department of Homeland Security jointly have put out guidelines for those fusion centers.

Those guidelines are quite extensive, and they are guidelines; they are not rules. They are no "you must do," because cookie-cutter approaches are not going to work with 50 states, and indeed more than 50 states because you have cities such as New York, Los Angeles, Chicago and others that wish to see urban regions and urban areas united in a fusion center.

Those guidelines, and I have read them, and experts that put them together, both from the federal, state and local governments around the country, believe those guidelines are adequate to set up a system, a national system, indeed, of such fusion centers that would integrate the fusion centers effectively.

The 42 that are now up, most of them, particularly the larger ones, are following the guidelines. We believe that most of those that are in the planning stages are using the guidelines as their planning tool for setting up those centers. Once again, the federal government can't dictate to the states and there are local conditions and variations that need to be addressed at the state level and below.

But that, I think, is a very important tool and, again, that did not exist a year ago. It exists now, and in fact we hope very, very shortly to have that published. I am pushing very hard to get that published as soon as possible. It has been informally distributed, so the publication will simply sort of put a final mark of approval on the document itself.

There are other ways also I think that we have been able to help through grant programs with the various states that are setting them up. I would point out that in some cases states are making decisions as to whether they want just a single state fusion center, or whether they should join with some neighboring states to set up a fusion center for that group of states. In other instances, we are going to find fusion centers will be multiple within a state, California being a prime example, as is New York.

Mr. GIBBONS. Mr. Ambassador, my time has expired. I want to thank you again for your presence here today.

Mr. Chairman, thank you.

Mr. SIMMONS. I thank the gentleman.

The chair recognizes the distinguished gentleman from Rhode Island, Mr. Langevin, a member of the Armed Services Committee.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Ambassador, I want to thank you for being here today and for your testimony. I know you have a tough job on your hands. We look forward to working with you.

With respect to information and intelligence, the most important thing, I am sure you would agree, is to make sure that those who

need the information have the information that they need to do their jobs. That often means people on the frontlines, law enforcement most especially.

So far, I can tell you that most state and local law enforcement entities have not been impressed with the level of communication they have had with the federal government, the Department of Homeland Security in particular.

So I guess I would like to start with the question of, has there been a general agreement reached in terms of your understanding of the type of infrastructure that will be used to share information?

Law enforcement, to be honest with you, doesn't want to reinvent the wheel. By way of example, the regional information sharing network, RISSNET, is something that law enforcement is very comfortable with. They use it all the time for sharing basically law enforcement intelligence.

Many in the law enforcement community feel that there should just be a component added for sharing terrorism-related information within RISSNET. Obviously, Homeland Security may feel differently. I have raised this with Charlie Allen, by the way, and to his credit he dispatched his deputy up to RISSNET to actually see this in operation and how it is in terms of what law enforcement is familiar with, and how they work now.

But could you answer the question of, is there general agreement on how we are going to share this information, particularly with those on the frontlines who need it most, particularly law enforcement?

Ambassador MCNAMARA. I think there is an understanding of what is necessary in order to create that national system that I was talking about. The complexity of the systems, particularly at the local level, are a major obstacle to getting a single, if you will, pipeline in place.

I think in the end, we are probably going to do something of what you suggested. Rather than creating new lines, use those that we now have, but expand their use so that we don't have to create something new.

What we can do is build on the ones that are out there. And there are things like RISSNET and there are networks within the Department of Defense, within the Department of Justice itself, as opposed to the FBI, and also in Homeland Security that can be usefully expanded so that they can handle more and better information.

I think a major problem is in packaging the information. I was surprised, one of the many surprises when I came to this position was my impression that the information flow from the federal government to the state and local governments was insufficient. That is, it was inadequate. I found out that it was not inadequate in volume. It was inadequate and insufficient in quality and in the manner in which it was packaged.

What we need to bring to this issue is an understanding of, and I think it is understood within the intelligence community better than it is in some other communities, of managing it so that the consumers of the information can benefit from it, so that sending out information, as we have done in the past, in which we didn't take into account that the local police chief needs that packaged in

a way that he can use. It has to be actionable. It has to be something that is relevant to his situation.

I heard the story of a police chief from a major city, after the London bombings, who said that he got no useful information about the London bombings from the federal government. He had about 3 or 4 hours at most to decide what he was going to do about the commuters who were going to be using buses and subway systems in his city for the morning rush hour.

What he was looking for was information that would tell him what can he put out to the public and how should he react to the London bombings in a way that would make the community feel more comfortable about going to work in the morning. He got that by getting on a telephone and phoning four other chiefs of police in four other major cities, and the five of them came up with an effective recommended way of handling the morning rush hour problem.

I think if we had a national system such as I am talking about, if wouldn't have to be ad-hocced at 5 o'clock or 4 o'clock in the morning. It would be a system that would come online and it wouldn't be necessarily the chiefs of police that would be the first ones to communicate with each other.

There would be a communications system that would go into emergency mode among the fusion centers, and the information would be gotten out not just to five police chiefs, although that was certainly a benefit, but maybe to 55 or 155 or 255, because the system would work for the benefit of all.

I think that is what we are talking about. We are talking about setting up a limited number of pipelines with information that will be packaged in a way that is useful to the consumer, which means we have to go to those police chiefs. We have to go to those state homeland security officers and get them to tell us what is useful to them.

And then I think we need to use the NCTC, the National Counterterrorism Center, as a major focus of our effort to package the information so that it is useful to those at the state and local level. That, it seems to me, means bringing state and local people up here to Washington to work with us so that we will get out of the product that we have here in Washington something that can be used either in an emergency situation such as after the London bombing, or that can be used for, let's say, investigations, protection of infrastructure, managing public fears, managing the difficulties of a particular sector in the private sector.

All of that needs to be packaged in a way that is useful for the consumer, and the consumer is the person at the other end of the line. It is not the analysts sitting in Washington writing out what is a perfectly good piece of paper, useful to people here in Washington, but of no use to that police chief who has to make a decision about what to do before the commuters go to work at 6 in the morning.

It is a very long answer to a short question, but that is my understanding of where we need to go and how we need to do it.

Mr. LANGEVIN. It is obviously an important subject. I like what I am hearing, and obviously you are identifying the problem. I hope you will follow through with working very closely with law enforce-

ment people on the frontlines who are going to ultimately be the end-users of this information they need. It is so important to involve them from the get-go, and listen to them to hear what is going to be most helpful.

So I know my time is expired. If we do a second round, I had additional questions.

Thank you, Mr. Chairman.

Mr. SIMMONS. I thank the gentleman. We will do a second round.

I appreciate the comments on the fusion centers. I agree completely that that is a tremendously useful tool to facilitate information sharing. But I would like to go back for a few minutes to the sensitive but unclassified issue.

You are absolutely correct. During the Cold War, a security system was established of confidential, secret and top secret, and then various compartments, based on sensitive methods of collection that were pretty much at the top secret level, but simply a top secret clearance didn't give you access to those compartments. You had to be signed in and signed out.

So I have traditionally looked at the classification system as three parts: confidential, secret and top secret. We have this unofficial use only; we have law enforcement sensitive; we have various other caveats that really aren't classifications. They are controls.

Ambassador MCNAMARA. Controls, right.

Mr. SIMMONS. I suspect that you could spend the rest of your life trying to figure out a system to get everybody happy to accommodate all of these different controls.

Somewhat hypothetically, but I will ask the question anyway, why don't we clear the deck? Let's take all of those SBUs and just wipe them out. Start with a clean slate, and then ask ourselves, which ones absolutely have to be added back and in what fashion?

Now, law enforcement is sensitive. It has been around for a long time. As Mr. Langevin said, people don't like to reinvent the wheel, et cetera, et cetera. Okay, so that should be added back. Perhaps that should be added back as something that is classified confidential. I don't know.

But it seems to me that, again, you could spend the rest of your life working this problem and never reach a completely satisfactory conclusion, and in the meantime other critically important initiatives such as, you know, we have to share, folks; we have to figure out how to share; we have to make sure the guys in the fusion center and the police officers in the municipalities have actionable intelligence. We have to make sure that pipeline is working.

So if we were to take the SBUs and just clean the slate, how many would we count as being really critical to add back in some form or another? Has anybody on your staff taken a look at this? Has anybody tried to address this problem from that standpoint, of erasing and adding back, as opposed to trying to accommodate what we have?

Ambassador MCNAMARA. Let me make one comment about the "wipe it out and start over again." If we assume that we were to wipe it out, and let's say it took 6 months to start it up and get it working again, or even if it only took 6 weeks, the question arises as to whether or not all that information that rightly was controlled?

Mr. SIMMONS. If I could interrupt for just a second. I understand. It is like an academic exercise. We have all this stuff on the chalkboard, and we erase it all, and then we ask the class, okay, who is upset at what we just did? Who absolutely cannot deal with the fact that we have erased everything of the chalkboard? Who absolutely insists that we have to add their SBU back to the slate?

Ambassador MCNAMARA. That is part of the process that we are going through right now, is determining what is essential to control, and if so, if it is essential to be controlled, under what rational set of categories, what legislative mandate, or government-wide regulation should it be controlled under?

It varies. We are not at that point of actually setting up the final list of categories, but my initial observations would be that certainly no more than a half-dozen or so categories would probably do the job. And then you would determine, depending upon the level of sensitivity, whether or not something that is now personal health information, for example, which under various privacy laws must be controlled, or whether it is proprietary information, again under other laws must be controlled.

It has nothing to do with national security. In fact, the federal government doesn't really have an interest in itself of doing the controlling. It is that proprietary information needs to be controlled because of other interests.

So setting up those categories and then, you might way, wipe it out, but then inserting those categories that definitely require under legislation or government-wide regulation, require controls, that they be put in the proper category of control. And that the rest of it I would think would just become unclassified, with no control mechanism.

Mr. SIMMONS. I think that would be a very useful exercise for you to pursue between now and June.

Ambassador MCNAMARA. I am pursuing it. I will pursue it beyond June if necessary until I get it done. I have until the end of the year, according to the rule. I would be delighted to get it done by June. July, I would be less delighted, but more delighted than September or October.

Mr. SIMMONS. Before the August vacation.

The ranking member?

Ambassador MCNAMARA. I will do my best.

Ms. LOFGREN. On that same point, and perhaps we are honing in on this because we had such a useful workshop with the GAO on this very subject. As you are describing the process, you are using, you are getting a reading, you are getting the temperature from various agencies. I am wondering what, other than just their druthers, what kind of objective criteria that you are proposing to them?

I assume that in this process, you will get buy-in from across the federal agencies. But have we reached out? I mean, one of the things that I thought was interesting in the GAO exchange was that it is not all clear that we have any legal basis, in some cases, for actually keeping this information private. So if we don't set up objective standards that will withstand scrutiny, it doesn't matter how we define these things, we will not succeed in protecting them from an assault.

Can you shed any light on those questions?

Ambassador MCNAMARA. Again, a tentative observation at the start. I don't pretend to be an expert in this. I have begun in the last 2 weeks to get more and more involved in this, so therefore that means in the first 6 or 7 weeks, I was busy with other things.

There are instances where it is very clear. There are 17, in fact, that are required by law, by a legal mandate. There appear to be others that are equally meritorious, but there was never a problem, and so no law was passed. In other words, in 17 cases, something happened and the Congress said, that should not have happened; we will fix it with a law.

But there were other cases where agencies did things on their own in order to control something that should have been controlled, and therefore no problems ever arose. If we were to wipe that out, we would find problems arising. That is one of the reasons why I am a little bit cautious.

Ms. LOFGREN. If I can clarify. I am not suggesting, because I don't know in fact—I don't think either one of us knows all of the things that are being kept confidential. I am not necessarily assuming those judgments are wrong, because I don't even know what those judgments are.

All I am suggesting is there needs to be a framework for that decision making, and there needs to be a legal basis for enforcing that decision, or else ultimately this scheme will fail.

Ambassador MCNAMARA. Or come back to the Congress to create the legal basis, and that is one of the options that is open to us; that is, to set up the framework, apply what law is currently available, see where it falls short, and possibly come back up. There is much, quite frankly, that has no legal basis and doesn't deserve any legal basis. We should be getting that stuff out.

Ms. LOFGREN. In some cases, when in doubt, stamp it confidential.

Ambassador MCNAMARA. That is right, or otherwise control. That gets back to this thing about risk management versus risk aversion. This is another area where the process has been risk aversion. Does that look like it might cause a problem? On goes the control stamp.

Ms. LOFGREN. A final question. In a free society, we have more actors than just the government. We have a free press. We have the citizenry at large. Have you built into your work-plan outreach into advocates for the press or for civil liberties? Not that they should see the information, but that they should evaluate the standards and get their input up front?

Ambassador MCNAMARA. Honestly, I don't know what the answer to that is. I hope the answer is yes, but I haven't asked it. I will go back and ask it. And if it is not yes, I will try and make it yes.

Ms. LOFGREN. Thank you.

Mr. SIMMONS. The gentleman from Rhode Island?

Mr. LANGEVIN. Thank you, Mr. Chairman.

Ambassador, are you familiar with the term "electronic discovery"?

Ambassador MCNAMARA. Electronic discovery?

Mr. LANGEVIN. Electronic discovery. Basically, it is a relatively new technology or concept, you might say, and basically it allows us to take massive amounts of data and organize it into a understandable and usable format. They are using it, for example, on some of the highest profile criminal cases right now in the corporate world that you have read about in the newspaper.

I would think that this would be something that would be very useful in organizing this intelligence information and then being able to disseminate it into usable type where you have a format. And so maybe at some point we can talk a little bit more about that if you are not familiar with the concept.

Ambassador MCNAMARA. I have heard of it, and I have heard it in these last few weeks mentioned. It is also data-mining, is another—

Mr. LANGEVIN. It is data-mining, but it is also organizing one you have mined it—

Ambassador MCNAMARA. Once you mined it, right.

Mr. LANGEVIN. —to organize into a useful form.

Ambassador MCNAMARA. I am not that familiar with all the details, but I understand that there are both privacy concerns, as well as security concerns that are involved in how one goes about managing, if you will, the data-mining and the electronic discovery.

Mr. LANGEVIN. Sure. I welcome the opportunity to talk more about that.

Ambassador MCNAMARA. I would like to. I will try and get myself more informed on it also.

Mr. LANGEVIN. The other thing is, I would like to ask you, the Department of Homeland Security right now has a clear mandate to be the point of contact between federal government, state, local and tribal law enforcement agencies in terms of information sharing. Accordingly, I would think that the department would have a lot of say about the policies that you are developing for this vertical type of information sharing.

What is the precise role of the Department of Homeland Security in the work that you are doing to advance the information sharing environment? And what support is Charlie Allen, the chief intelligence officer, providing to you specifically?

Ambassador MCNAMARA. The answer is that I recognize that the Department of Homeland Security is basically the lead agency in many of these areas, and that it has a primary responsibility under the law to move information to the state, local, tribal and private sector.

I have worked very, very closely with them. I have met with Secretary Chertoff, Deputy Secretary Jackson, with Assistant Secretary Allen, whom I have known and worked with before over a period of 20 to 25 years. He is a good friend of mine, as well as being a colleague that I have now come to work with one more time after being out of government. I have also worked with and met with Assistant Secretary Stew Baker and others in the Homeland Security Department.

I think their role is going to be central in this national system that I am talking about. My initial observation is that the three chief, if you will, largest players in this are going to be the Department of Homeland Security, the Department of Justice, including

the FBI, and the Department of Defense. Those are the three majors. Then there are other departments, but to focus in on Homeland Security, I think they will play a central role, and they should and will expect to fulfill their legislative mandate in that regard.

When I make my recommendations with respect to what I think ought to be done, I will be taking that into account.

Mr. LANGEVIN. Thank you, Ambassador. I look forward to working with you further.

Ambassador MCNAMARA. Likewise.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Mr. SIMMONS. I thank the gentleman.

Are there any other questions from the members of the committee present?

Ms. LOFGREN. I said I didn't have a question. This really isn't one, but I am hopeful that we can get, at least in writing, periodic progress reports on where we are on these two pressing questions on classified-to-distributable information and the SBU issue.

Ambassador MCNAMARA. If I may add a comment. As I said in my written statement, and probably should have in my oral, but I was trying to keep it very compressed, it has been my policy over many years to work carefully and closely with the Congress and to keep them informed, whether I was working in political-military affairs or terrorism, to keep the Congress informed.

I think that is doubly the case on this particular issue. I have already told my staff that I want regular contact with members and staff. We have already been meeting periodically with House members on the House side and on the Senate side. I intend to do that. And anytime we are not doing enough, please give me a call and let me know and we will do enough.

Ms. LOFGREN. Okay.

Mr. SIMMONS. Mr. Ambassador, thank you for your testimony.

And thanks to the members for their questions.

Members of the committee may have some additional questions for you, and will ask you to respond to these questions in writing. The hearing record will be held open for 10 days.

I think it is fair to say, Mr. Ambassador, we want you to succeed in what we understand to be a complex and difficult, perhaps even overwhelming task. I would suggest to you that the GAO report should be considered a useful tool. It is a tool for us, of course, and it could be a useful tool for you as well, if properly utilized. I think you know what I mean by that.

We look forward to keeping in touch with you. Thank you for your past service and for coming back to the government once again to rise to the challenge that we face.

Homeland security is something that is incredibly important to all of us, and all you have to do is look at some of the pictures on the wall to see the consequences of our failure. We never want that to happen to our country and our loved ones again.

I thank the members.

Without objection, the committee stands adjourned.

[Whereupon, at 3:15 p.m., the subcommittee was adjourned.]

FOR THE RECORD

PREPARED STATEMENT OF SHEILA JACKSON-LEE

Thank you Mr. Chairman and members of the Subcommittee. I thank the witness for testifying today. I speak to today on the challenges of implementation on building the Information Sharing Environment (ISE). According to the Intelligence Reform and Terrorism Prevention Act, Congress intended the ISE as a method to "provide and facilitate the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." However, the advance of ISE has been very slow due to lack of resources and a lack of commitment from the Intelligence Community.

The Government Accountability Office (GAO) released a very critical report detailing slow progress of ISE. The report goes on to describe that the Department of Homeland Security and other agencies presently use 56 different sensitive but unclassified designations to protect information that they deem critical to their mission.

The GAO's report goes on to note that the Director of National Intelligence (DNI) refused to comment on the report deeming it a "review of intelligence activities" that was "beyond the GAO's purview." In fact, GAO's report was solely a study of the development of government wide information sharing policies and procedures which did not involve evaluation of the conduct of actual intelligence activities. Instead of there being government wide policies and procedures governing information sharing, each agency determines for itself what designations and associated policies should apply to their sensitive information. Even with agencies, more than half of the agencies the GAO examined reported challenges in sharing such information because they do not have a formal policies and procedures on the matter. It is clear that there seems to be a disconnect and lack of communication between intelligence agencies internally and externally. Today, I look forward to learning how Ambassador McNamara will go about setting realistic policies and procedure that intelligences will be able to disseminate and follow.

I look forward to hearing the witness and learning how we can better protect this nation. Thank you Mr. Chairman.