S. HRG. 107–912

SHOULD THE OFFICE OF HOMELAND SECURITY HAVE MORE POWER? A CASE STUDY IN INFORMATION SHARING

HEARING

BEFORE THE

SUBCOMMITTEE ON ADMINISTRATIVE OVERSIGHT AND THE COURTS

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

APRIL 17, 2002

Serial No. J–107–73

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

85–887 PDF WASHINGTON : 2003

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

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts	ORRIN G. HATCH, Utah
JOSEPH R. BIDEN, JR., Delaware	STROM THURMOND, South Carolina
HERBERT KOHL, Wisconsin	CHARLES E. GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ARLEN SPECTER, Pennsylvania
RUSSELL D. FEINGOLD, Wisconsin	JON KYL, Arizona
CHARLES E. SCHUMER, New York	MIKE DEWINE, Ohio
RICHARD J. DURBIN, Illinois	JEFF SESSIONS, Alabama
MARIA CANTWELL, Washington	SAM BROWNBACK, Kansas
JOHN EDWARDS, North Carolina	MITCH MCCONNELL, Kentucky

BRUCE A. COHEN, *Majority Chief Counsel and Staff Director*
SHARON PROST, *Minority Chief Counsel*
MAKAN DELRAHIM, *Minority Staff Director*

SUBCOMMITTEE ON ADMINISTRATIVE OVERSIGHT AND THE COURTS

CHARLES E. SCHUMER, New York, *Chairman*

PATRICK J. LEAHY, Vermont	JEFF SESSIONS, Alabama
EDWARD M. KENNEDY, Massachusetts	STROM THURMOND, South Carolina
RUSSELL D. FEINGOLD, Wisconsin	CHARLES E. GRASSLEY, Iowa
RICHARD J. DURBIN, Illinois	ARLEN SPECTER, Pennsylvania

BENJAMIN LAWSKY, *Majority Chief Counsel*
ED HADEN, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Schumer, Hon. Charles E., a U.S. Senator from the State of New York	1
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	69
Sessions, Hon. Jeff, a U.S. Senator from the State of Alabama	5

WITNESSES

Anderson, Philip, Senior Fellow and Director, Homeland Security Initiative, Center for Strategic and International Studies	46
Hastings, Scott O., Associate Commissioner for the Office of Information Resources Management, U.S. Immigration and Naturalization Service, Washington, D.C.	17
Hitch, Vance, Chief Information Officer, Justice Management Division, Department of Justice, Washington, D.C.	7
Jordan, Robert J., head of the Information Sharing Task Force, Federal Bureau of Investigation, Washington, D.C.	12
Light, Paul C., Brookings Institution, Washington, D.C.	53
Panetta, Hon. Leon E., Director, Panetta Institute, Monterey Bay, CA	35
Terwilliger, George J., III, Partner, White & Case, Washington, D.C.	42

SUBMISSION FOR THE RECORD

Department of Justice, Joseph Karpinski, Director, Congressional Relations and Public Affairs, letter	70

SHOULD THE OFFICE OF HOMELAND SECURITY HAVE MORE POWER? A CASE STUDY IN INFORMATION SHARING

WEDNESDAY, APRIL 17, 2002

UNITED STATES SENATE,
SUBCOMMITTEE ON ADMINISTRATIVE OVERSIGHT
AND THE COURTS,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:36 a.m., in Room SD–216, Dirksen Senate Office Building, Hon. Charles Schumer, Chairman of the subcommittee, presiding.

Present: Senators Schumer, Sessions, and Specter.

STATEMENT OF HON. CHARLES E. SCHUMER, A U.S. SENATOR FROM THE STATE OF NEW YORK

Chairman SCHUMER. Good morning, everybody. The hearing will come to order.

We have consulted with Senator Sessions' staff, and because of our timing issues and particularly a few of our witnesses have to catch planes, we are going to start now. We will probably have a quick vote at 10 o'clock, and so we are going to try to move things along as quickly as possible.

I want to thank all of our witnesses for coming to what I think is a very interesting and important hearing. I hope you will agree—all of you in the audience—after you hear what we have to say.

And here is Senator Sessions now. Jeff, I am just going to begin my opening statement, because we have some time constraints.

Since the events of September 11th, every local, State and Federal Government agency has been scrambling to repair the holes in our homeland defense that were revealed on that fateful day.

Our homeland defense situation is comparable to the story of the little Dutch boy who single-handedly tried to keep the floods from breaking through the dike and destroying Amsterdam. He was successful, but we have many more holes than that one little hole in the dike. All of them have to be plugged up rather quickly.

Try as we might, every time we plug one hole, another pops up. Whether it is the discovery of a terrorist with a shoe bomb who made it onto a plane, or sending student visas to known terrorists, we keep discovering hole after hole, and that translates into threat after threat and risk after risk.

That is something we clearly cannot afford in the post-9/11 world. Our world changes, and we have to adapt to it.

There are over 40 Federal agencies charged with law enforcement and intelligence gathering. Our safety relies in good part upon each and every one of them. When the left hand does not know what the right hand is doing, you have a problem. When you have 20 left hands and 20 right hands and none of them know what the other is doing, you have a potential disaster in the making.

That is what we are facing right now.

The backbone of homeland defense is good information sharing and coordination between Federal law enforcement and intelligence agencies. It is clear that we need some kind of body to coordinate government-wide policy on information sharing. We need an entity that can answer questions like: Where are we most vulnerable? Who can supply the right information about those vulnerabilities? Who needs to know about our weaknesses? And who is going to tell them?

These sound like simple, basic questions, but in a bureaucracy like ours, unless someone is keeping an eye on things, the answers get lost pretty quickly.

The Administration, in my judgment, was headed in the right direction when Tom Ridge was sworn in as the first Director of the Office of Homeland Security. Director Ridge was charged with developing and coordinating a comprehensive national strategy to strengthen protections against terrorist threats or attacks in the United States.

Though the idea is a good one, I am afraid that the consequences, intended or not, have resulted in OHS becoming a little bit akin to something like a toothless tiger.

Everybody has tremendous respect for Tom Ridge. I certainly do. We served in the House together, and he is an exemplary man and I am glad he is in that position.

But at this point in time, he does not have the tools or the power to get what needs to be done, and this hearing will just show one little aspect of that.

If OHS is meant to be more of a policymaking agency, then it needs to acquire the appropriate authority and be subject to congressional oversight.

We are not taking any sides on whether Mr. Ridge ought to testify here or not; that is not the issue. The issue is what the scope of his office ought to be as it relates to information sharing and other issues.

But OHS in this case needs to be able to prod or even direct the different Federal agencies into changing their management decisions and removing the blinders that stop agencies from thinking outside their own parameters. Each agency and bureau needs to think beyond its own functions, beyond its own databases, and work to connect to other departments.

It is very hard to do this on your own. I am not blaming any of the agencies here for not doing it on their own. I am not blaming anyone in the Administration or in the House or Senate that we did not do this before. This is a brave new world and nobody had the foresight to know what we had to do. But now we do know

what we have to do. And that is why we have to improve things and act.

Various proposals have been laid out on how this entity, a new entity, an agency that is responsible for making sure there is coordination of information, be structured. And I look forward to hearing from our witnesses today on what they think.

But whatever form it takes, I strongly believe that we need to empower one agency, one entity, to coordinate information sharing between and among the different Federal law enforcement and intelligence agencies for the purposes of homeland defense. Having an agency that coordinates information from different agencies is the first problem. Then having technology to help them do it is the second.

I have been told the technology exists to vastly improve our agencies' databases so appropriate agency officials can access information in real time, both within their own agencies and, just as importantly, with other State, Federal, and local agencies.

Before the recess, I introduced the idea of a supercomputer to coordinate Federal law enforcement intelligence gathering activities. While we would have to address the obvious privacy concerns in developing such an idea as this one, that is hardly beyond the pale. You can deal with privacy issues because you cannot just be Luddite and say do not make coordination better, do not have the best computers. You rather would have them, and then make sure that privacy concerns are protected as you use them.

Now, we might need three or four of these computers, each one for a separate security purpose. In a recent interview, Larry Ellison of Oracle blamed a lot of our security problems on fragmented data. He said, "We knew that Mohammed Atta was wanted. We just did not check the right database when he came into the country." And that sums up the problem as good as anybody can.

For the most part, we have the right information. We know who to go after. We just keep stumbling into our own bureaucracy.

About 6 weeks ago, I requested a complete list of the unclassified information databases used for law enforcement and intelligence purposes from 10 different law enforcement and intelligence agencies. I did not request what is in the databases, just what the databases are. I made follow-up call after follow-up call. I received the final lists only yesterday—6 weeks just to get a list of what the databases are, so we would know how to coordinate them.

What does that say about our organizational capabilities? I have been told that our intelligence community is light years ahead of our law enforcement community in terms of the organization of information sharing and its technology. Well, everyone has to be brought up to speed and maybe the intelligence agencies can share some of their wisdom and what they have done with our law enforcement agencies.

Intelligence gathering does not help if we do not have the law enforcement capability to deal with that information.

Finally, we have to look at the culture in our Federal agencies and put a stop to the rivalries that get in the way of protecting our country. It is a well-known fact that cultural differences between the different law enforcement and intelligence agencies hinder

proper information sharing. The CIA does not want to share with the FBI. The FBI does not want to share with the INS.

My message to all of these groups is: Get with it. We are in a new and different world, and those rivalries cause us to pay a real price or could cause us to pay a real price. This is not about a turf war between Federal agencies. It is about preventing terrorists from murdering innocent civilians. If you cannot see that, then you need to take a good, hard look and figure it out.

I very much look forward to hearing from our witnesses today from both inside and outside the government. And working together—this is not a partisan issue in any sense—we can repair our defenses and make our Nation a safer one.

Thank you.

[The prepared statement of Senator Schumer follows:]

STATEMENT OF HON. CHARLES E. SCHUMER,
A U.S. SENATOR FROM THE STATE OF NEW YORK

With over forty Federal agencies conducting homeland security-related law enforcement or intelligence gathering activities, and no one entity actually in charge of coordinating and directing all of them, the Courts Subcommittee today held a hearing to explore whether the Office of Homeland Security has the authority it needs. Schumer pointed to frequent terrorist threats that can and are slipping through the cracks and examined why major mistakes like granting student visas to terrorists occur and whether the Federal Government is doing enough to develop a supercomputer to coordinate homeland security activities.

The following is Schumer's statement from the hearing:

Since the events of September 11th, every local, State, and Federal Government agency has been scrambling to repair the holes in our homeland defense that were revealed on that fateful day.

Our homeland defense situation is comparable to that story of the little Dutch boy who singlehandedly tried to keep the floods from breaking through the dike and destroying Amsterdam. Though I think he was successful, we're having a much harder time defending our own.

Try as we might, every time we plug one hole, another one pops up. Whether it's the discovery of a terrorist with a shoe bomb who made it onto a plane or sending student visas to known terrorists, we keep discovering hole after hole, and that translates into threat after threat, risk after risk. That's something we clearly can't afford.

There are over forty Federal agencies charged with law enforcement and intelligence gathering. Our safety relies, in some part, upon each and every one of them. When the left hand doesn't know what the right hand is doing, you've got a problem. When you have 20 left hands and 20 right hands and none of them knows what the other is, you've got a disaster in the making. And that's exactly what we're facing right now.

The backbone of homeland defense is good information sharing and coordination between Federal law enforcement and intelligence agencies. It's clear that we need some kind of body to coordinate governmentwide policy on information sharing. We need an entity that can answer questions like: Where are we most vulnerable? Who can supply the right information about those vulnerabilities? Who needs to know about our weaknesses? And who is going to tell them? These may sounds like simple, basic questions, but in a bureaucracy like ours, unless someone is keeping an eye on things, the answers get lost pretty quickly.

The Administration was headed in the right direction when Tom Ridge was sworn in as the first director of the Office of Homeland Security. Director Ridge was charged with developing and coordinating a comprehensive national strategy to strengthen protections against terrorist threats or attacks in the United States.

Everyone has tremendous respect for Tom Ridge, but he needs the power to carry out his mandate: protecting the American people. If OHS is meant to be more of a policymaking agency, then it needs to acquire the appropriate authority and be subject to Congressional oversight. OHS needs to be able to prod the different Federal agencies into changing their management decisions and remove the blinders that stop agencies from thinking outside their own parameters.

Each agency and bureau needs to think beyond its own functions, beyond its own databases, and work to connect to other departments. It's very hard to do this on

your own. That's why we need an agency who's responsible for making sure it happens.

Various proposals have been laid out for how this entity should be structured and I look forward to hearing from our witnesses today on what they think.

But whatever form it takes, I strongly believe that we need to empower one agency, one entity, to coordinate information-sharing between and among the different Federal law enforcement and intelligence agencies for the purposes of homeland defense.

Having an agency that coordinates information from different agencies is the first problem. Having the technology to help them do so is the second.

I've been told that the technology exists to vastly improve our agencies' databases so that the appropriate officials can access information in real time both within their own agencies and with other Federal, State, and local agencies. Before the recess, I introduced the idea of a supercomputer to coordinate Federal law enforcement intelligence-gathering activities. While we would have to address the obvious privacy concerns in developing an idea such as this one, it's not beyond the pale. We might need three or four of these computers, each one for a separate security purpose.

In a recent interview, Larry Ellison of Oracle blamed a lot of our security problems on fragmented data. "We knew that Mohammed Atta was wanted," he said. "We just didn't check the right database when he came into the country."

For the most part, we have the right information. We know who to go after. We just keep stumbling into our own bureaucracy. About 6 weeks ago, I requested a complete list of the unclassified information databases used for law enforcement and intelligence purposes from 10 different Federal law enforcement and intelligence agencies.

After making follow-up call after follow-up call, I received the final lists only yesterday. What does this say about our organizational capabilities?

I've been told that our intelligence community is light years ahead of our law enforcement community in terms of the organization of information-sharing and its technology. Everyone has to be brought up to speed. Intelligence gathering doesn't help if we don't have the law enforcement capabilities to deal with the information.

Finally, we have to look at the culture in our Federal agencies and put a stop to the stupid rivalries that get in the way of protecting our country.

It's a well known fact that cultural differences between the different law enforcement and intelligence agencies hinder proper information sharing. The CIA doesn't want to share with the FBI, the FBI doesn't want to share with INS. My message to all of them is this: grow up. This isn't about turf wars between Federal agencies. It's about preventing terrorists from murdering innocent civilians. If you can't see that, then you need to take a good, hard look and figure it out.

I look forward to hearing from our witnesses today, from both inside and outside the Government. Together, we can repair our defenses and make our Nation a safer one.

Chairman SCHUMER. Now let me call on my colleague and friend, Senator Sessions.

STATEMENT OF HON. JEFF SESSIONS, A U.S. SENATOR FROM THE STATE OF ALABAMA

Senator SESSIONS. Thank you, Senator Schumer, and thank you for your courtesy in working with us on putting this hearing together. We do not always work as well as we should in the Senate sometimes, but you have always been extremely courteous and open about what the purposes of a hearing would be and what you hoped to accomplish.

I believe it is an important issue. How we go about making sure that we have the right kind of unified information-sharing system is a critically important issue.

I have believed for some time that we have a number of problems there. DEA can do certain things. They do not input their intelligence information, but if there is a warrant or an arrest warrant for someone, they will flag it so that if that person is ever arrested, at least they would call the Drug Enforcement Administration,

then they would know that this person has been arrested, and they would not have to share their most sensitive intelligence information on the NCIC or some other system.

I believe we have to utilize the NCIC more. We have some 600,000-plus State and local law enforcement officers, and, for example, 12,000 FBI agents. So not to enlist them in this effort is a colossal error. They have got to be. They are out there every day making arrests, making stops for people. And it is just a tragedy if they make an arrest of a seriously wanted individual, to not know it and release them.

We have systems today that a person who has been stopped, you can put their thumb or finger on a machine, and it would tell their criminal history from the police officer's car. It is amazing.

So we have some capabilities here that we need to make sure that we are utilizing fully. I look forward to asking some questions about how our computer data systems are working, how they actually work today, because I am not sure I fully understand it. But there are gaps, and it is a good thing to talk about.

With regard to the homeland security organization, that is a matter of great complexity and importance. How we go about that, I do not know. I am not convinced we need to create a large, permanent Cabinet-level or even semi-Cabinet-level agency at this point. But we are going to have to decide how to do that, how we can improve our homeland security, so it will be good to talk about those issues, too.

Mr. Chairman, thank you.

Chairman SCHUMER. Thank you, Senator Sessions.

I want to just repay the compliment. We are from different parts of the country. We are different ideologically. But we work together well, and it is a tribute to Jeff. He is straightforward and fair, and I very much appreciate that all the time.

Now let's call on our witnesses and try to get right to the point here. I am going to ask each of the witnesses to really—their entire statements will be read into the record—but each witness to try and limit the testimony to 5 minutes and get to the point, so we can ask questions, because I think we are going to have a vote at 10 o'clock. As I say, we have some plane schedules from some of our future witnesses to catch. We could not put them on first, because the protocol is always that you guys go first. So I just ask your cooperation.

So let me introduce all three witnesses, and then we will have each of them testify.

Mr. Vance Hitch is the CIO, the Chief Information Officer, for the Department of Justice. He was appointed by Attorney General Ashcroft in March. He is leading the development of an IT, information technology, strategic plan that provides direction for the Department of Justice's future IT investments. Before coming to DoJ, Mr. Hitch was a senior partner with Accenture, where he developed the IT strategic plan for the State of Maryland, comprehensive reengineering and automation of the city of Philadelphia's records. He has worked with other agencies, such as the Department of State, the NSA, the CIA, and the DoD, to name a few initials, and multiple State and local governments.

Mr. Robert Jordan, our second witness, heads the information sharing task force for the FBI. He is the section chief in the Government and Civil Rights section. He is a 22-year-old veteran of the FBI and was most recently in Newark, New Jersey, where he supervised the white-collar crime and corruption program for that entire State. Before that, he was a supervisory special agent in San Diego, where he initiated a large-scale judicial corruption case.

Our third witness is Mr. Scott Hastings. He is the associate commissioner of the Office of Information Resource Management and the deputy chief information officer of the INS. As the associate commissioner, Mr. Hastings is responsible for the service's information technology programs, including all established ADP functions, telecommunications, and electronic enforcement technology programs.

He has considerable experience with outsourcing of government operations. In his current position, he is examining the role of Federal information technology organizations and their future configurations and structure.

Prior to this position, he was the assistant commissioner for the Office of Record Services at the INS, during which time he created a national records facility and centralized operation for holdings in excess of 25 million active files.

So you can see all three gentlemen are very accomplished in this field and in the government. We are lucky to have all three of you. Each of your statements will be read into the record. I am going to try to stick to the 5 minutes.

Mr. Hitch, you may proceed.

STATEMENT OF VANCE HITCH, CHIEF INFORMATION OFFICER, DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. HITCH. Thank you.

Mr. Chairman and Members of the Subcommittee, I am pleased to appear before you today to discuss information sharing, as you requested. I will take just a few minutes to briefly summarize my prepared statement.

Last month, the Attorney General appointed me as the chief information officer of the Department of Justice. In announcing my appointment, the Attorney General stated: A critical element in our battle against the terrorist threat is the effective use of information technology to share information across law enforcement.

To pursue this mission, my mandate, I believe, is very clear: Upgrade the department's information technology program to better enable core mission accomplishment and use information technology as a tool for collaboration among the Justice components and between Justice and other Federal agencies, as well as Federal, State and local law enforcement.

Improving and expanding the department's use of information technology is a key component of the Attorney General's wartime reorganization of the department, which he announced last November 8. Just last week, the Attorney General ordered the Justice components to take further actions to institutionalize the department's ongoing efforts to coordinate information relating to terrorism.

Specifically, he asked for four things. First, expand the information about known or suspected terrorists in existing law enforcement databases, such as the FBI's National Crime Information Center, or NCIC, the Department of State's TIPOFF system, and the Customs Service's Interagency Border Inspection System or IBIS. Number two, establish procedures to obtain on a regular basis identifying information on terrorists known to other countries. Three, establish a secure system for sharing information with State and local agencies. And four, standardize procedures for sharing sensitive information and implementing the information sharing provisions of the U.S. Patriot Act.

But even prior to 9/11, the department was involved in several efforts to improve information sharing. For example, the El Paso Intelligence Center, or EPIC, is an interagency center that provides tactical drug intelligence to Federal, State and local users. A telephone call, fax or teletype provides the requester real-time information access to EPIC from many Federal databases and EPIC's own internal system. The IDENT/IAFIS project is integrating the INS's IDENT system with the FBI's IAFIS fingerprint database. The integration project will increase the apprehension and effective prosecution of criminal aliens. Finally, the JABS, or the Joint Automated Booking System, is streamlining the identification and booking of persons in Federal custody. JABS enables the department's law enforcement components to share arrest information electronically and update the FBI's crime master file in a real-time mode.

In direct response to the deadly attacks on the World Trade Center and the Pentagon, the President directed the department also to create a foreign terrorist tracking task force, or FTTTF, a multiagency group that leverages expertise, information, and technology to identify, locate, remove or deny entry to foreign terrorists and their supporters.

Among the participating agencies are the CIA, the INS, FBI, State, Customs, Social Security and many members of the intelligence community.

The President also directed that the Attorney General and the Director of Central Intelligence ensure to the maximum extent permitted by law that the task force has access to all available information necessary to perform its mission. The task force is gathering and analyzing data contributed by participating agencies, using advanced techniques to mine the data, establish patterns, and calculate risk parameters. The results of these analyses are provided to the relevant agencies for appropriate enforcement action.

Although the task force is still in the early stages of its work, it offers an especially promising model for information sharing and collaboration associated with terrorism.

Despite these efforts, it is clear that more needs to be done. We must fundamentally rethink how information systems are designed, developed, and managed, so that information technology fosters rather than hinders collaboration.

This really means creating a Department of Justice information architecture, as well as infrastructure and the management approach that promotes both information sharing, as well as information security at the same time.

I am confident that the organizational and cultural roadblocks to information sharing are being remedied. We know that to succeed we must work together. Our long-term goal and one that technology can help make a reality is that the Department of Justice and members of the law enforcement community, whether State, Federal or local, be able to communicate and collaborate with one another fully, easily, and securely.

One of the Attorney General's top 10 management goals, which he announced in his initial reorganization letter, and one of his initial assignments to me, is the development of a comprehensive information technology plan for the department. We are working on this plan as we speak and expect to have it completed within the next several months.

Among the major goals of this plan are removing any technical barriers to information sharing, building a department-wide security infrastructure, and developing an enterprise architecture that ensures secure access to data by all authorized users, and promotes sharing and collaboration across organizational lines.

I can assure this Subcommittee that the Department of Justice is committed to moving away from the stovepipe systems and overcoming unnecessary obstacles to information sharing, and working closely with the Office of Homeland Security, the Federal agencies and others, to fully and securely share sensitive law enforcement information.

Again, thank you for the opportunity to discuss this matter of critical importance to the Justice Department and to all law enforcement. I would be pleased to respond to your questions.

[The prepared statement of Mr. Hitch follows:]

STATEMENT VANCE HITCH, CHIEF INFORMATION OFFICER, JUSTICE MANAGEMENT DIVISION, UNITED STATES DEPARTMENT OF JUSTICE

Mr. Chairman and Members of the Committee, I am pleased to appear before you today to discuss information sharing. I am both honored and grateful for this opportunity.

Last month, the Attorney General appointed me Chief Information Officer (CIO) for the Department of Justice. In announcing my appointment, the Attorney General stated: "A critical element in our battle against the terrorist threat is the effective use of information technology to share information across law enforcement." To pursue this mission, my mandate is clear: upgrade the Department's information technology program to better enable core mission accomplishment, and use information technology as a tool for collaboration among Justice components, between Justice and other Federal agencies, and among Federal, State, and local law enforcement.

In the aftermath of the September 11 terrorist attacks, it is clear that information sharing is critical to our Nation's safety. The Attorney General recognizes clearly that access to accurate and timely information is crucial to supporting the Department's critical law enforcement responsibilities, and especially in protecting against acts and threats of terrorism. Improving and expanding the Department's use of information technology are key components of the Attorney General's wartime reorganization of the Department, announced on November 8, 2001.

Just last week, the Attorney General directed key Justice components to take further actions to institutionalize the Department's ongoing efforts to coordinate information relating to terrorism. Specifically, he ordered the investigating components to establish procedures to provide, on a regular basis and in electronic format, the names, photographs and other identifying data of all known or suspected terrorists for inclusion in the State Department's TIPOFF system, the FBI's National Crime Information Center (NCIC), and the Customs Service's Interagency Border Inspection System (IBIS). He also ordered the Assistant Attorney General for Legal Policy to work with the components to draft for his consideration procedures, guidelines, and regulations to implement the information sharing provisions of the USA PATRIOT Act.

Historically, information systems have been developed and implemented to meet the particular business needs of a specific component organization. The result, as you know all too well, is a number of legacy stovepipe systems that impede cross component information sharing. However, even before 9/11, the Department was involved in several efforts to improve sharing or to consolidate systems. For example:

• **El Paso Intelligence Center (EPIC).** The Department of Justice established the El Paso Intelligence Center (EPIC) in 1974, staffed by representatives of the INS, the Customs Service, and the DEA, to provide a common information resource on drug movement and immigration violations. Today, EPIC has grown to include 15 Federal agencies, the Texas Department of Public Safety, and the Texas Air National Guard. In addition, EPIC maintains information sharing agreements with other Federal law enforcement agencies, the Royal Canadian Mounted Police and each of the 50 States and serves law enforcement agencies throughout the western hemisphere. A telephone call, fax, or teletype from any of these agencies provides the requestor real-time information accessed through EPIC from many different Federal data bases, plus EPIC's own internal database.

• **IDENT/IAFIS.** The IDENT/IAFIS project was established to integrate the INS IDENT system with the FBI's IAFIS. The integration project will directly enhance the Department's ability to meet its mission through increased apprehension and effective prosecution of criminal aliens. It is a major cross-cutting initiative and will provide improved INS identification services to determine whether a person they apprehend is the subject of a posted Want or Warrant or has a record in the FBI's Criminal Master File. Similarly, it will provide law enforcement agencies with all relevant immigration information as part of a criminal history response from a single FBI.

• **Joint Automated Booking System (JABS).** JABS is another major cross-cutting initiative involving the Bureau of Prisons, the U.S. Marshals Service, the INS, the FBI, and the DEA. JABS streamlines the identification and processing of Federal offenders by providing the means to electronically collect, store, and transmit photographic, fingerprint, and biographical data.

More recently, and in direct response to the deadly attacks on the World Trade Center and the Pentagon, the President directed the Department to create a Foreign Terrorist Tracking Task Force (FTTTF). This is a multi-agency Task Force that combines agency expertise, information and advanced technologies to identify, locate, and remove or deny entry to foreign terrorists and their supporters. There are several Federal agencies that are already participating (e.g., the FBI, the INS, the State Department, the Customs Service, the Social Security Administration, and elements of the Intelligence Community). These agencies are joint participants with a common mission of neutralizing the threat of terrorist aliens.

The President also directed that the Attorney General and the Director of Central Intelligence "ensure, to the maximum extent permitted by law, that the Task Force has access to all available information necessary to perform its mission." The Task Force is both gathering and analyzing data contributed by participating agencies, using advanced methods to mine the data, establish patterns, and calculate risk parameters. Results of these analyses are provided to the relevant agencies for appropriate enforcement action. Although the Task Force is still in the early stages of its work, it offers an especially promising model for information sharing and collaboration.

Despite these efforts, it is clear that more needs to be done. To meet the new threats and challenges we face today, we must fundamentally rethink how information systems are designed, developed and managed so that IT fosters, rather than hinders, collaboration. This means creating a DoJ information architecture, infrastructure, and management approach that promote both information sharing and information security.

It is important that we move forward on both the sharing and security fronts simultaneously. Sharing information depends in no small measure on our ability to assure that the information will be protected from unauthorized disclosure. A primary obstacle to sharing has been, and remains, concerns about the security of the information once it is outside the control of the agency that "owns" it.

The Department has a long ways to go, but I am confident we are headed in the right direction. I am convinced that organizational and cultural roadblocks to information sharing are being remedied. In part, this is because of executive branch and Congressional leadership; in part, it is because of the sheer magnitude and complexity of the threat. We know that to succeed we must work together. Our long-term goal—and one that technology can help make a reality—is that the Department of Justice and all members of the law enforcement community, whether Federal, State, or local, be able to communicate and collaborate with one another fully, easily, and securely.

One of the Attorney General's top ten management goals, and one of his initial assignments to me, is the development of a comprehensive Information Technology Plan for the Department. We are working on this Plan and expect to complete it within the next month. However, let me briefly outline the Plan's major themes and directions:

Information Sharing

There are three key technical barriers to information sharing within the Department of Justice: (1) insufficiently modernized office automation systems; (2) inadequate networking; and (3) applications and data stores that cannot be accessed by other components or agencies. Overcoming these barriers is a long-term effort, but progress has and is being made. For example, the components are in various stages of updating their office automation and networking infrastructures and, as mentioned earlier, there have been some, albeit limited, efforts to share information and integrate systems.

Critical areas in support of information sharing to be addressed in the plan include:

- Upgrading our telecommunications infrastructure to improve cross component access to intranet sites and other data stores, meet projected demands for bandwidth, and ensure wireless and remote access to the DoJ network;
- Accelerating the completion of component office automation upgrades; and
- Modernizing access methods, such as through Web-like interfaces, collaboration platforms, and systems consolidation.

I want to elaborate on the last point. Of great concern to this Committee is whether agencies are sharing information related to foreign nationals who want to enter this country, or are already here, and who may be threats to national security. One of the difficulties is that the INS has an array of heterogeneous systems that does not provide a full and complete picture of a foreign national's travel to and from the United States or critical events during his or her period of stay. For this reason, the Department is exploring with the Office of Homeland Security and affected agencies the creation of a consolidated database that would be organized by person rather than immigration event and would be accessible to all parties, including the State Department and the Customs Service.

Information Security

Information systems must be protected from inadvertent or deliberate disclosure of sensitive information to unauthorized users, from attacks on the infrastructure that deny services, and from attempts to alter or otherwise falsify information. Securing our information systems has rightfully become the focus of increasing scrutiny by the Congress and others.

We need to improve information security by building a long-term departmentwide security infrastructure that will ensure that information systems are secure from day one, rather than requiring continuous patches and fixes. In the meantime, we will take two immediate steps:

- First, we need to make sure that existing systems are as well protected as they should be by identifying vulnerabilities and taking corrective action. The Department is carefully monitoring and tracking component progress in this regard.
- Second, we need to build infrastructure-based capabilities, such as public key infrastructure, available for use throughout DoJ and scalable to the broader law enforcement and judicial communities.

IT Planning and Management

We also intend to strengthen the way we plan for and manage our IT investments. Here again, progress has been made but more work is needed. Among my priorities will be developing an enterprise architecture that is linked to investment management and provides a foundation for ensuring that IT systems meet mission requirements, identifies redundancies and opportunities for consolidation, and ensures cross component sharing of common assets, services, and solutions. It will be an architecture that ensures secure access to data by all authorized users and promotes sharing and collaboration across organizational lines. Relatedly, I will be emphasizing the development of Departmentwide standards and policies, as well as stronger oversight of priority initiatives.

This is an ambitious agenda, one that will take time, resources, and cooperation to implement fully. But I can assure this Committee that the Department of Justice is committed to moving away from stovepipe information systems, overcoming unnecessary obstacles to information sharing, and working closely with the Office of Homeland Security, Federal agencies, and others to fully and securely share sensitive law enforcement. We simply cannot afford to do otherwise.

Again, thank you for the opportunity to discuss this matter of critical importance to the Justice Department, and to all law enforcement. I would be pleased to respond to your questions at this time.

Chairman SCHUMER. Thank you, Mr. Hitch.

Mr. Jordan.

STATEMENT OF ROBERT J. JORDAN, CRIMINAL INVESTIGATIVE DIVISION, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, DC

Mr. JORDAN. Thank you. Good morning, Mr. Chairman and Senator Sessions.

My name is Bob Jordan and I serve as the head of the FBI's information sharing task force. With me today is Gene O'Leary, acting Assistant Director of the FBI's Information Resources Division, and Ken Ritchhart, Chief of the Data/Information Management Section of IRD.

We welcome this opportunity to meet with you today about the status of the FBI's information sharing initiatives within the bureau and with other government agencies for homeland defense purposes.

The FBI is an organization in change. Not only are we structurally different, but in very fundamental ways, Director Mueller has revamped our approaches to counterterrorism and prevention.

Since 9/11, we have seen massive shifts in our resource deployments. Our missions and priorities are being redefined to better reflect the post-9/11 realities. As an agency, we are committed to devoting whatever resources are necessary to meet our prevention mission and continue to sustain a dramatically enhanced worldwide counterterrorism effort.

A substantial component of this approach is information sharing, not only at the Federal level, but also within the entire law enforcement and intelligence communities.

Over the last several years, much has improved, but this seemingly simple issue is actually a complex myriad of technology, legal, policy, and cultural issues. Since the tragic events of 9/11, this single issue which is critical to public safety is receiving the sustained high-level attention necessary to ensure that everything that can be done on every facet of the issue is being done.

In that regard, I am happy to say that the spirit of collaboration and willingness to exchange data has never been stronger or more pronounced than it is today. Many of the legal and policy impediments that kept us from more fully exchanging information in the past have been or are now being changed.

The Patriot Act has greatly improved our ability to exchange data with the intelligence community and across law enforcement. In addition, the Attorney General's recent directive to increase the coordination and sharing of information between the Department of Justice, the FBI, INS, the Marshals Service and the Foreign Terrorist Tracking Task Force on terrorist matters, and to establish secure means of working with State and local officials, are major milestones in improving our information-sharing and collaboration efforts.

Equally important, the difficult technology challenges we all face are on top of everybody's priority list. This is especially so at the

FBI. Under Director Mueller's leadership, the FBI on every front is hard at work, carrying out the Attorney General's information-sharing directive.

Within the FBI, Director Mueller has personally taken on the challenge of improving information sharing and has directed FBI executive management to develop every means necessary to share as much information as possible with other agencies, as well as State and local law enforcement. Years of experience have demonstrated that joint terrorism task forces, our JTTFs, have proven to be one of the most effective methods of unifying Federal, State and local law enforcement efforts to prevent and investigate terrorist activity by ensuring that all levels of law enforcement are fully benefiting from the information possessed by each.

There are currently 47 JTTFs. We are working expeditiously to establish JTTFs in each of the FBI's 56 field offices. In 1996, there were only 11 of these task forces. The creation of 21 new JTTFs this year is resulting in an expanded level of interaction and cooperation between the FBI and their Federal, State and local counterparts, as well as an enhanced flow of information between the participating law enforcement agencies.

Among the full-time Federal participants on JTTFs are the INS, the Marshals Service, Secret Service, the FAA, the Customs Service, ATF, the State Department, Postal Inspection Service, IRS, and the U.S. Park Police. State and local agencies are heavily represented.

The FBI has a long tradition of exchanging unclassified information with Federal, State and local law enforcement agencies on wants and warrants, fingerprint identification, forensic information, and watch lists. The last few years has seen dramatic increases in the exchanges of specific case-related information due in large part to the proliferation of task forces. Now we are improving our sharing of classified information, again through such mechanisms as the JTTFs.

Following the terrorist attacks of September 11, FBI headquarters compiled what became known as the Project Lookout Watch List. The project was successful in identifying a number of individuals potentially connected to the PENTTBOM investigation. Due to the success of this effort and in recognition of the need to maintain a centralized repository of names in the investigative interests related to terrorism investigations, Director Mueller instructed the establishment of a permanent terrorism watch list, TWL, to serve as the FBI's single integrated listing of individuals of investigative interest that will be accessible throughout the law enforcement intelligence communities.

We anticipate the full implementation of the TWL within the next 60 to 90 days, replacing the stopgap system now resident in NCIC. The TWL will consist of a compendium of names based on information identified through FBI and JTTF investigations, U.S. intelligence community reporting, and Department of Defense intelligence gathering, as well as information provided by cooperating foreign governments.

Director Mueller has undertaken several other initiatives that either directly or indirectly enhance the FBI's information sharing capacity. All of these efforts are designed around the recognition

that post-9/11, the FBI has adopted both a new focus and priorities that recognize the substantial investment being made in prevention.

A few examples include:

Director Mueller has recently named Louis Quijas, currently the Chief of Police of High Point, North Carolina, to be the FBI Assistant Director for Law Enforcement Coordination.

An Office of Intelligence is now part of the FBI's organizational structure.

The FBI has undertaken a major recruiting and hiring initiative to bring into the FBI private sector IT experts who can greatly assist in designing and managing our sizeable IT projects recently funded by Congress.

The FBI's future ability to deter and prevent crimes requires the use of current and relevant IT. We have several critical initiatives underway to upgrade our IT infrastructure and investigative applications, such as Trilogy program, data warehousing and data mining, and our information assurance initiative.

Funding these programs is essential to providing our investigators and analysts with improved IT resources and tools to support criminal and national security investigations, enabling improved and more expeditious data sharing and active collaboration.

That concludes my prepared remarks, Mr. Chairman. I will be happy to respond to any questions.

[The prepared statement of Mr. Jordan follows:]

STATEMENT OF ROBERT J. JORDAN, FEDERAL BUREAU OF INVESTIGATION

Good morning, Mr. Chairman and Members of the Subcommittee. My name is Bob Jordan and I serve as the head of the FBI's Information Sharing Task Force. With me today is Gene O'Leary, Acting Assistant Director of the FBI's Information Resources Division (IRD) and Ken Ritchhart, Chief of the Data/Information Management Section of IRD. We welcome this opportunity to meet with you today about the status of the FBI's information sharing initiatives within the Bureau and with other Government agencies for homeland defense purposes.

The FBI is an organization in change. Not only are we structurally different but, in very fundamental ways, Director Mueller has revamped our approaches to counterterrorism and prevention. Since 9/11, we have seen massive shifts in our resource deployments. Our missions and priorities are being redefined to better reflect the post-9/11 realities. As an agency, we are committed to devoting whatever resources are necessary to meet our prevention mission and continue to sustain a dramatically enhanced worldwide counterterrorism effort. A substantial component of this approach is information sharing, not only at the Federal level but also within the entire law enforcement and intelligence communities: Over the last several years much has improved, but this seemingly simple issue is actually a complex myriad of technology, legal, policy and cultural issues. Since the tragic events of September 11, this single issue, which is critical to public safety, is receiving the sustained, high-level attention necessary to ensure everything that can be done on every facet of the issue is being done.

In that regard, I am happy to say that the spirit of collaboration and willingness to exchange data has never been stronger or more pronounced than it is today. Many of the legal and policy impediments that kept us from more fully exchanging information in the past have been or are now being changed. The USA Patriot Act (Pub. L. 107–56) has greatly improved our ability to exchange data with the intelligence community and across law enforcement. In addition, the Attorney General's recent directive to increase the coordination and sharing of information between the DoJ, the FBI, the INS, the USMS, and the Foreign Terrorist Tracking Task Force (FTTTF) on terrorist matters and to establish secure means of working with State and local officials are major milestones in improving our information sharing and collaboration efforts. Equally important, the difficult technology challenges we all face are on the top of everyone's priority list. This is especially so at the FBI. Under

Director Mueller's leadership, the FBI, on every front, is hard at work carrying out the Attorney General's information-sharing directive.

Joint Terrorism Task Forces

Within the FBI, Director Mueller has personally taken on the challenge of improving information sharing and has directed FBI executive management to develop every means necessary to share as much information as possible with other agencies as well as with State and local law enforcement. Years of experience have demonstrated that Joint Terrorism Task Forces, JTTFs, have proven to be one of the most effective methods of unifying Federal, State and local law enforcement efforts to prevent and investigate terrorist activity by ensuring that all levels of law enforcement are fully benefiting from the information possessed by each.

There are currently 47 JTTFs. We are working expeditiously to establish JTTFs in each of the FBI's 56 field offices. In 1996, there were only 11 of these task forces. The creation of 21 new JTTFs this year is resulting in an expanded level of interaction and cooperation between FBI Special Agents and their Federal, State and local counterparts, as well as an enhanced flow of information between the participating law enforcement agencies.

Among the full-time Federal participants on JTTFs are the INS, the Marshal's Service, the Secret Service, the FAA, the Customs Service, the ATF, the State Department, the Postal Inspection Service, the IRS, and the U.S. Park Police. State and local agencies are heavily represented.

In addition to the JTTFs, the Regional Terrorism Task Force (RTTF) initiative serves as a viable means of accomplishing the benefits associated with information sharing without establishing a full-time JTTF. FBI Special Agents assigned to counterterrorism matters meet with their Federal, State and local counterparts in designated alternating locations on a semi-annual basis for common training, discussion of investigations, and to share and discuss intelligence. The design of this non-traditional terrorism task force provides the necessary mechanism and structure to direct counterterrorism resources toward localized terrorism problems within the United States. There are currently six RTTFs: the Inland Northwest, the South Central, the Southeastern, the Northeast Border, the Deep South and the Southwest RTTFs.

The FBI has a long tradition of exchanging unclassified information with Federal, State and local law enforcement agencies on wants and warrants, fingerprint identification, forensic information and watch lists. The last few years have seen dramatic increases in the exchange of specific case-related information due, in large part, to the proliferation of task forces. Now, we are improving our sharing of classified information again through such mechanisms as the JTTFs.

Terrorism Watch List

Following the terrorist attacks of September 11, 2001, FBI Headquarters compiled what became known as the "Project Lookout Watch List." The project was successful in identifying a number of individuals potentially connected to the PENTTBOM investigation. Due to the success of this effort and in recognition of the need to maintain a centralized repository of names of investigative interest related to terrorism investigations, Director Mueller instructed the establishment of a permanent Terrorism Watch List (TWL) to serve as the FBI's single, integrated listing of individuals of investigative interest that will be accessible throughout the law enforcement and intelligence communities. We anticipate the full implementation of the TWL within the next 60 to 90 days, replacing the stop-gap system now resident in NCIC. The TWL will consist of a compendium of names based on information identified through FBI and JTTF investigations, U.S. Intelligence Community reporting, and Department of Defense intelligence gathering, as well as information provided by cooperating foreign governments.

The TWL will be designed to assist both the intelligence and the law enforcement communities in their investigations of terrorist groups/individuals and, equally important, to alert officers or agents should a person of interest in a terrorism matter be encountered by another agency. TWL staff will coordinate with the FBI's Criminal Justice Information Services (CJIS) Division to ensure the utilization of appropriate NCIC files. This capability will provide all State and local law enforcement agencies ready access to this information. Information in the TWL will also be shared with U.S. Government agencies that operate comparable tracking systems. As I describe these new databases and our plans for sharing them, please remember that the FBI will by complying with the Privacy Act and the detailed regulations that govern our law enforcement, counterterrorism, and counterintelligence activities, which ensures proper protection for the rights of Americans in the use of the databases.

The TWL will be divided into three distinct categories. The first category will include the names of individuals for whom formal criminal charges or indictments have been issued (e.g., the 22 individuals on the Most Wanted Terrorist list). The second category will include the names of individuals of investigative interest to the FBI.

The third category of the TWL will include the names of individuals provided by the Intelligence Community and cooperating foreign governments.

Other FBI Initiatives

We have recently developed an FBI-wide and DoJ-wide capability to electronically share case information. Our Integrated Intelligence Information Application (IIIA) database is another example of major improvements in information sharing. It uses information derived from many different sources including the Department of State and INS. IIIA provides analytical support for Counterintelligence and Counterterrorism programs. It is a real-time collection system that houses over 33 million records. In the aftermath of 9/11 and PENTTBOM, IIIA has been asked to provide electronic search support to units within the FBI as well as to the critical FTTTF. To satisfy these requests, multiple programs have been written to standardize incoming data arriving in differing formats and to package the responses to accommodate the requesters' needs.

Director Mueller has undertaken several other initiatives that either directly or indirectly enhance the FBI's information sharing capacity. All of these efforts are designed around the recognition that post-9/11, the FBI has adopted both a new focus and priorities that recognize the substantial investment being made in prevention. A few examples include:

- Director Mueller has named Louis Quijas, currently Chief of Police of High Point, North Carolina, to be FBI Assistant Director for Law Enforcement Coordination. Chief Quijas has as his single mission fully exploiting State and local law enforcement support through enhanced information sharing and ensuring that State and local law enforcement have a strong voice within the FBI as we work on terrorism, prevention and major investigations.
- An Office of Intelligence is now part of the FBI's organizational structure. This office has as part of its mission not only to ensure the vigorous and fluid flow of information within the FBI but also to ensure that intelligence goes elsewhere within the law enforcement and intelligence communities in every instance when it is appropriate to do so.
- The FBI has undertaken a major recruiting and hiring initiative to bring into the FBI private sector IT experts who can greatly assist in designing and managing the sizable IT projects recently funded by Congress. These projects, such as Trilogy, are vital to any robust information sharing program.
- A Records Management Division has been established, headed by an outside records expert, to put in place the "information management" policies and mechanisms critical to effective sharing programs.
- The FBI is detailing personnel to other agencies, and vice versa, to ensure that information both is both shared and understood within both agencies. These efforts are critical to programs like the National Infrastructure Protection Center (NIPC), the Counterterrorism Center at CIA, and others.

Information Security

One equity we must balance with our desire to share information as freely as possible is the need for the security of information. As recently detailed in Judge William Webster's report, we must keep in mind that we are keepers of information that is highly classified and controlled by "need to know" principles. Access to highly confidential information will be in accordance with the FBI's broad, new security policies. Access control mechanisms, such as identification and authentication will provide accountability for those individuals having a need to know restricted information. In addition, audits of this access will be routinely conducted. The lives of agents, informants and innocent victims often rest upon the safekeeping of their information. The need for information security must be balanced by the driving need of the criminal investigator to be able to follow any and all avenues in an investigation.

The Webster Commission report accurately points out that the FBI's information technology (IT) recapitalization effort, Trilogy, includes funding for only the foundational elements of Information Assurance (IA). At rollout, Trilogy will provide more security than the FBI's current IT backbone. The goal, however, is to develop the IA Program to be on par with other world-class information systems security efforts. Significant coordination has taken place between the Trilogy Program and personnel assigned to the IA Program to ensure that the Trilogy security architec-

ture will support the utilization of the future IA technologies we plan to employ. So, while Trilogy and related applications will give the FBI a vastly increased capability to use, analyze, exploit and share information collected in investigations, it will be designed and deployed in a manner that addresses the shortcomings apparent in the Hanssen matter.

Challenges

Today, information sharing is technologically feasible. Advances in information technology have made it possible to link the information systems of agencies that are operating with different hardware and software. The improvements in information sharing that are at the heart of these initiatives, however, require that agencies participating in integration initiatives come together and agree upon a governance structure to manage decisionmaking in an integrated environment. Federal, State and Local law enforcement must address the considerable challenge of developing a formalized organizational framework within which participating agencies will share responsibility for making and executing overarching decisions on such issues as budgeting, hardware and software purchases, and the development of policies, procedures, and protocols that effect the operational integrity of the information sharing system. Our systems were originally designed to comply with a complex set of regulations restricting what can and cannot be shared amongst Federal, State and local agencies. We are committed to redesigning our systems and making whatever changes are necessary to ensure the effective and efficient exchange of information within the law enforcement community.

At the same time, we still need to further improve our ability to share information between our own applications and our own multitude of databases. Our Data Warehousing project will provide us with the capability to finally combine information from all our applications into a coherent whole and provide advanced data mining, analytical and visualization tools. We are also working with the Office of Homeland Security on improving horizontal information sharing, developing common data standards, and improving collaboration capabilities.

The FBI's future ability to deter and prevent crimes requires the use of current, and relevant IT. We have several critical initiatives underway to upgrade the FBI IT infrastructure and investigative applications such as the Trilogy Program; Data Warehousing & Data Mining; our Collaboration Initiative; and our Information Assurance initiative. Funding these programs is essential to provide our investigators and analysts with improved IT resources and tools to support criminal and national security investigations, enabling improved and more expeditious data sharing and active collaboration.

That concludes my prepared remarks, Mr. Chairman. I will be happy to respond to any questions you may have.

Chairman SCHUMER. Thank you, Mr. Jordan. I want to thank both witnesses. I know you condensed your testimony.

Mr. Hastings. I presume you will do the same thing.

STATEMENT OF SCOTT O. HASTINGS, DEPUTY ASSOCIATE COMMISSIONER FOR INFORMATION RESOURCES, IMMIGRATION AND NATURALIZATION SERVICE, WASHINGTON, DC

Mr. HASTINGS. I will certainly do that.

I appreciate the opportunity to appear today to discuss this issue. In any discussion about moving Federal agencies to a more effective information-sharing environment, technical solutions need to be only a part.

The Department of Justice approach and the approach of the Office of Homeland Security are similar: build a solid planning requirements base before identifying technical solutions, at the same time implementing tactical interim successes that make sense to support the immediate threats. Business needs and objectives that may be expressed in enterprise architectures must be established.

Following that process, decide the information that is required by the operation and how to deliver it, identify technology alternatives to deliver that information, create utilities that support that process, and invest.

Finally, select, control, and manage those utilities, and then create knowledge-management capability.

The INS is clearly one of the core agencies that requires enhanced information-sharing capabilities. The data we collect are crucial to the law enforcement and intelligence communities, who are now integrating their functions to combat the threat of terrorism. Consequently, we are deeply involved in efforts to overcome the barriers to appropriate and secure exchange of data, and equally important to convert that data to useful information that supports clear operational objectives.

The Office of Homeland Security, in conjunction with OMB, is overseeing initiatives that provide information sharing between Federal agencies horizontally, and then promote agencies vertically to State and local governments, as well as selected private industries. INS is a working partner in those efforts.

Attorney General Ashcroft has made the prevention of terrorist activities an overriding priority in the Department of Justice and its components. With this goal in mind, he directed us to review and strengthen our policies and procedures to ensure that information sharing and analysis and coordination of activities with other Federal agencies, as well as our State and local partners, to combat terrorism.

This mandate, coupled with new legislation, such as the USA Patriot Act, has provided us with greater authority to share information as appropriate. We are implementing technical linkages as we speak with other Federal agencies to integrate the data required to support the act.

We have also been directed by the Attorney General to step up our efforts to coordinate information activities in the common effort to prevent and disrupt terrorism, and we are full participants in the departmental efforts to improve data sharing.

Federal agencies maintain a number of databases that provide real-time information to officials at U.S. diplomatic posts abroad, offices at ports of entry, and the interior law enforcement officials. We work closely with agencies to prevent terrorists from entering the United States, to deny them entry across our borders, and to detect and apprehend those already in the country, and to gather intelligence on the plans and activities of terrorist conspiracies.

We provide, in electronic format, biographic, biometric, and associated data for inclusion in several external agency databases to better identify these terrorists.

For many years, INS has taken steps to enhance the exchange of information through greater cooperation amongst the law enforcement community. An example of this is the law enforcement support center, available 24 hours a day, 7 days a week, to provide State law enforcement with data and information from INS databases. We also verify immigration status for State and local benefit granting agencies, some employers and some State drivers license bureaus.

Finally, we are working internationally to develop better ways of sharing information that will support enforcement intelligence operations. The U.S. government recently signed agreements with the governments of Canada and Mexico to further these initiatives.

I cannot overemphasize the commitment of INS and the other Federal agencies to work together to achieve a more supportive and comprehensive information support environment. In each of these, we need to be sensitive to the legal limitations on sharing information, security and privacy concerns, and who are the appropriate users of the information.

With all the initiatives, there are no quick fixes, technological or otherwise, to problems we face. We must work with advanced technology to improve our systems. But technology alone cannot solve our problems.

In order to leverage our resources and maximize our capabilities, technology must be coupled with strong intelligence information-gathering distribution systems. This will require seamless cooperation amongst the agencies involved. It is crucial we focus on the efforts exemplified by DoJ, the Department of Justice, and the Homeland Security Office that solidify the planning and administrative structures that are required, while continuing to support the immediate requirements levied every day by ongoing intelligence and enforcement operations. In this way, the INS can help ensure a more dependable outcome that takes advantage of the wealth of technology solutions that already exist, but that may be embedded within individual agencies. Without these structures, we will be unable to interlace these solutions together in a meaningful way.

Thank you for the opportunity to testify.

[The prepared statement of Mr. Hastings follows:]

STATEMENT OF SCOTT O. HASTINGS, ASSOCIATE COMMISSIONER FOR THE OFFICE OF INFORMATION RESOURCES MANAGEMENT, U.S. IMMIGRATION & NATURALIZATION SERVICE, WASHINGTON, D.C.

Mr. Chairman and Members of the Committee, I appreciate the opportunity to appear before you to discuss the important issue of how technology and information can best support our efforts to reduce the threat of foreign terrorist activity.

The Immigration and Naturalization Service (INS) is clearly one of the core agencies that will require enhanced information sharing capabilities. The data we collect are crucial to the law enforcement and intelligence communities that are now integrating their functions to combat the threat of terrorism. The INS will need to take advantage of additional external sources of data to support our enforcement and intelligence functions.

Consequently, we are involved deeply in efforts to overcome barriers to the appropriate and secure exchange of data and, equally important, to convert that data to useful information that supports clear operational objectives. The Office of Homeland Security, in conjunction with the Office of Management and Budget, is coordinating agency initiatives that promote information sharing among Federal agencies horizontally, and then from those agencies, vertically, to State and local governments as well as selected private industries. INS is a working partner in those efforts.

Attorney General Ashcroft has made the prevention of terrorist activities an overriding priority of the Department of Justice and its components. With this goal in mind, he directed us to review and strengthen our policies and procedures to ensure information sharing and analysis and coordination of activities with other Federal agencies, as well as our State and local partners, to combat terrorism. This mandate, coupled with new legislation such as the USA PATRIOT Act of 2001, has provided us with greater authority to share information with Federal officials to assist in the performance of their duties. We are implementing the technical linkages with other Federal agencies to integrate data required to support this Act.

The Attorney General has also directed Department of Justice components to step up our efforts to coordinate information and activities in the common effort to prevent and disrupt terrorism. We are participating in Department efforts to improve data sharing.

Federal agencies maintain a number of databases that provide realtime information to officials at U.S. diplomatic outposts abroad, officers at ports-of-entry, and in-

terior law enforcement officials (e.g., the State Department's TIPOFF program). We work closely with these agencies to prevent terrorists from entering the United States, to deny them entry across our borders, to detect and apprehend those already in the country, and to gather intelligence on the plans and activities of terrorist conspiracies. We provide in electronic format biographic, biometric, and associated data for inclusion in several external agency databases to better identify suspected terrorists. For example, through the Interagency Border Inspection System (IBIS), the primary automated screening tool used by both the INS and U.S. Customs Service at ports-of-entry, access is provided to many databases, including the FBI National Crime Information Center (NCIC). NCIC is the Nation's principal law enforcement automated information sharing tool. It provides on-the-street access to information to over 650,000 U.S. local, State, and Federal law enforcement officers.

Additionally, the INS works to share information through the Integrated Automated Fingerprint Identification System (IAFIS) and other appropriate law enforcement databases to assist in detecting and locating foreign terrorists.

We have successfully integrated wants and warrants from the NCIC and the FBI into our own IDENT system. Through this joint endeavor, since August 15, 2001, we have identified a total of 891 individual aliens at the border who were wanted on outstanding criminal charges. With the expansion of IDENT to INS offices in the interior, we have been better able to identify criminal aliens residing in the United States.

On October 30, 2001, the President directed the Department of Justice to establish the Foreign Terrorist Tracking Task Force (FTTTF). The mission of the FTTTF is to keep foreign terrorists and their supporters out of the United States by providing critical and timely information to border control and interior enforcement agencies and officials. To do so requires electronic access to large sets of data, including the most sensitive material from law enforcement and intelligence sources. The INS works closely with the FTTTF to discern patterns and probabilities of terrorist activities and to ensure that data is properly shared.

For many years, the INS has taken steps to enhance the exchange of information through greater cooperation amongst the law enforcement community. An example of this is the Law Enforcement Support Center available 24 hours a day, 7 days a week to provide State law enforcement with data and information from INS databases. We also verify immigration status for State and local benefit granting agencies, some employers, and some State driver's license bureaus.

Finally, we are working internationally to develop better ways of sharing information that will support enforcement and intelligence operations. The U.S. Government recently signed agreements with the governments of Canada and Mexico to further these initiatives.

I cannot over-emphasize the commitment of the INS and other Federal agencies and other participants to work together to achieve a more supportive and comprehensive information support environment.

In each of these data sharing initiatives we must be sensitive to the Privacy Act and other relevant legal limitations on sharing information. When making information available to other entities, security, privacy concerns and appropriate user access are primary considerations for us. We have created a standing reviewing body to ensure all these issues are addressed with each type of data-sharing request.

All of our efforts to better share data need to take place in a sound planning and investment management process in order to succeed. Prior to September 11, the INS was developing mid- to long-range plans in response to growth in both its mission responsibilities and information sharing. Specifically, the INS has long-term plans to guide and align infrastructure and technology to accomplish this mission. The INS has undertaken several major initiatives to improve the planning and integration of its information technology environment, including an INS Enterprise Architecture Plan, a technology architecture, strategic information technology plans, and a 5-year records management plan. One goal of these plans is to ensure enhanced data sharing that is secure, accurate, and timely, and that meets the enterprise's operational objectives, not individual and "stove-piped" business functions. Other goals of these plans include:

Additional agent support equipment and technology enhancements and expanded access to biometric identification systems, such as a mobile IDENT system.

Implementation of automated access to the National Crime Information Center Interstate Identification Index (NCIC III) through the Advance Passenger Information System to enable primary inspectors at ports-of-entry receiving Advance Passenger Information to identify, prior to admission, aliens with criminal histories.

Improved system checks for the adjudication of applications at INS Service Centers and District Offices.

Improved accessibility to all Department of State visa data and photographs in electronic form at ports-of-entry so that visa information will be available at the time of actual inspection.

Expanded implementation of alternative inspection systems to facilitate admission of low-risk travelers while focusing on high-risk travelers. Deployment of the Student Exchange Visitor Information System, an Internet-based system that provides tracking and monitoring functionality on non-immigrant students and exchange visitors. Implementation of an entry and exit data system that will record the arrivals and departures of foreign nationals visiting the United States.

Continued cooperation with the State Department to replace old border crossing cards with the new biometric border crossing card and deploy card readers to our ports-of-entry.

Even with each of these initiatives, there is no quick fix, technological or otherwise, to the problems we face. We must work with advanced technology and improve our systems. But technology alone cannot solve our problems. In order to leverage our resources and maximize our capabilities, technology must be coupled with a strong intelligence and information-gathering and distribution system. This will require seamless cooperation among the many Federal agencies involved.

The most compelling progress in this arena has been the formalization of the planning and management processes needed to achieve the necessary level of information sharing among Federal, State, and local entities. These structures will bring discipline to the development and application of technology and will ensure that the INS defines what our operational objectives should be, identifies the data and the data sources needed to support those objectives, and applies the appropriate technology solutions to deliver that information.

It is crucial that we focus on the efforts exemplified by the Department of Justice and the Homeland Security Office that solidify the planning and administrative structure, while continuing to support immediate requirements levied every day by ongoing intelligence and enforcement operations. In this way, the INS will ensure a more dependable outcome that takes advantage of the wealth of technology solutions that already exist, but that may be embedded within individual agencies. Without these structures, we will be unable to interlace those solutions together in a meaningful way.

Thank you for the opportunity to testify before the Committee this morning. I welcome your questions.

Chairman SCHUMER. Thank you, Mr. Hastings.

As you can probably see, we had a vote called. Senator Sessions has gone to vote, so we do not have to interrupt, because we know the deadlines.

So I am going to begin asking questions. The minute Senator Sessions gets back, I will break my questioning. He will ask questions. I will go vote, and then we will resume in that way.

And however Arlen wants to fit into this will be fine with me in any way.

I guess the first question I have is a preliminary one. You have all outlined some ambitious plans for information sharing and all of that, which obviously requires more dollars in terms of both hardware, machinery, computers, et cetera, as well as more personnel.

First, how much would each of you estimate it will cost to eventually do this over the period of years? I guess Mr. Hitch would probably know this for all of Justice, and then just Mr. Jordan and Mr. Hastings, in your respective agencies.

And second, is lack of money a problem at all? I would presume it is not at this point in time.

Mr. Hitch.

Mr. HITCH. Yes, sir. Right now, we do not have definitive estimates to respond to your question. However, I would say, the way I have been talking about this to my counterparts in Justice, is we need to view this as the Defense Department would a new aircraft

carrier. It is a big effort to implement the kind of systems that are going to be necessary to protect our citizens. The number is—

Chairman SCHUMER. It is in the billions, you would say?

Mr. HITCH. It is probably in the billions, yes.

Chairman SCHUMER. That is within the Justice Department.

Senator SPECTER. Mr. Chairman, could I just say a word?

Chairman SCHUMER. Please.

Senator SPECTER. I am going to be departing in a moment for the vote, but I just wanted to thank you for scheduling this hearing.

I believe the issue of homeland security is one of enormous importance. It cuts across many of our Committee lines. It is my hope that we will see some legislation in the field that will strengthen the operation, make it a Cabinet officer.

And I think that a hearing like this is very constructive toward finding out what we ought to be doing.

Thank you, Mr. Chairman.

Chairman SCHUMER. Thank you, Senator Specter.

Do you expect that you will have all the dollars that you need to do this? You have been told by the Attorney General or others to make the best system and do not let finances get in the way?

Mr. HITCH. At this point, finances have not gotten in the way. I think the U.S. Patriot Act was really a landmark piece of legislation in helping us along that way. It provided a lot of seed money for a lot of things to get under way that we currently have under way. I think ongoing support is going to be necessary, but I think we have got enough to get us going in the right direction, to do the best we can without regard to that issue.

Chairman SCHUMER. Right.

Mr. Jordan, how much do you think it will cost and do you have the resources you need to do what you need to do in the FBI?

Mr. JORDAN. We have a budget request for fiscal year 2003 in this area of approximately $411 million. With that, we would have what we need.

Chairman SCHUMER. And has the Administration put that in its budget?

Mr. JORDAN. That is correct. It has.

Chairman SCHUMER. It will continue to be at about that level over the next several years, by the way, Mr. Jordan.

Mr. JORDAN. That is my understanding.

Chairman SCHUMER. Okay, Mr. Hastings.

Mr. HASTINGS. We received specific funding for specific projects in the counterterrorism supplemental. We have a 2003 budget request, which I do not have the details in front of me, but there are some large efforts that we have yet to put dollars to. The exit-entry system alone will be a significant investment, and it is really very difficult to predict at this point.

I know that the department will be helping us orchestrate and integrating these requests to ensure that we are not duplicating efforts, and we are making the best use of the funds from a departmental standpoint.

Chairman SCHUMER. Is yours in the hundreds of millions for this year?

Mr. HASTINGS. I would say so.

Chairman SCHUMER. Yes, okay.

Well, Jeff is not here, and I think we have about a minute or two left to vote. So what I am going to do is just call a brief recess. I will run vote and come right back.

But if Senator Sessions comes, we will let him start his questioning, and then I will resume mine when he finishes.

We are calling a short recess.

[Recess.]

Senator SESSIONS. If you do not mind, we will get started again. Senator Schumer told me to go ahead and get started with some questions that I might have.

I would just like to ask some fundamental questions that sort of go to where we are in terms of information sharing.

My personal view is the National Crime Information Center, the NCIC, is accessible by police officers in their vehicles anywhere in America, by police departments and sheriff's departments. It is secure in the sense that anybody that leaks that information is subject to a criminal penalty. But it is not secure, not greatly secure, in terms of the intelligence community, I am sure, because so many thousands of people have access to it and could obtain access to it in any police department surreptitiously to run any name that they would like to run.

So it has tremendous potential to help local law enforcement be the eyes and ears and hands of our effort to maintain security in our country, but it has some difficulties, too.

Mr. Hastings, with regard to INS, let me ask you a few simple questions. If an individual who comes here overstays his visa or is otherwise declared to be illegally in the United States, is that information made available to local law enforcement through the NCIC? Is any of that information placed in NCIC, which is the primary information center for law enforcement throughout America?

Mr. HASTINGS. The information would be available through our LESC, which is available 24 by 7 to law enforcement communities. We can provide that on a case-by-base basis.

And we also have begun including absconder information, where folks have gone through deportation proceedings and are still known to be in the country.

Senator SESSIONS. Prior to September 11, that was not the case. Is that correct?

Mr. HASTINGS. That is correct.

Senator SESSIONS. So prior to September 11, we did not have any database accessible to local law enforcement to identify people who they may be apprehending for some minor offense, but that would tell them that person was an illegal entrant or overstayer in the United States.

Mr. HASTINGS. By accessing the LESC, it would be the—

Senator SESSIONS. Now let's pursue the changes you have made. What is the LESC?

Mr. HASTINGS. The Law Enforcement Support Center. I am sorry for the acronym.

Senator SESSIONS. Is that available to a local police officer?

Mr. HASTINGS. Yes, it is.

Senator SESSIONS. And is it, therefore, part of the NCIC? Or does he have to do a double access?

Mr. HASTINGS. The LESC will access a multiplicity of data sources to provide information that we have according to the query that is generated by the local law enforcement.

Senator SESSIONS. Let me get that straight. I just want to know what it is like for the police officer out there trying to do his duty. He stops someone. Does that officer have to run two different systems from his vehicle or from the police station where he may have taken a person for some maybe minor crime? Or will one access to the general NCIC kick out a hit for that individual? Do you know?

Mr. HASTINGS. If he runs NCIC, and we have put information such as the absconder in that database, he will have access to that. He might want to make a further inquiry to determine whether or not we have additional information on this individual, in which case that is when he would contact our Law Enforcement Support Center.

Senator SESSIONS. With regard to absconder information and so forth, what if a person is eligible to stay in the country one year and they overstay and they are here 18 months. Is that going to be normally in your system under your current policy today?

Mr. HASTINGS. In the NCIC?

Senator SESSIONS. Yes.

Mr. HASTINGS. Not at this point.

Senator SESSIONS. So who would go in that system, then? You say you will put some of the absconders or others in there. How do you determine who will go in the system made available to local law enforcement?

Mr. HASTINGS. Sir, you are getting into an area—I am the technologist, and I am really not able to give you the policy decisions behind how we make the decisions. I know that information is reviewed before it goes into the NCIC to make sure it is appropriate to go there.

We can certainly follow up with a detailed explanation of what types of information at this point we put in there and how it is done, if I can defer that to a follow-up.

Senator SESSIONS. All right. That is very important to me.

Mr. HASTINGS. We will make sure you get that information.

Senator SESSIONS. What we have done in this country with regard to illegal immigration, we have said the words, and we have passed generalized statutes that deal with immigration. But when it gets down to the grassroots level where it actually succeeds or does not succeed, we have created roadblocks and problems that have eviscerated the capability of enforcing our statutes.

Well, I guess, Mr. Hastings, I will ask you. Maybe some of the others would comment. What happens if a police officer in Hagerstown stops a person that he identifies as being an illegal alien, but has not violated any serious Federal crimes? Do you know what that officer does, Mr. Hastings, with the person he has apprehended, who he determines to be illegally here?

Mr. HASTINGS. I suspect that will be a case-by-case decision on their part.

Again, sir, I would want to defer to our operations and investigations folks to give you the specifics on that.

Senator SESSIONS. That may not your area of responsibility.

Mr. Hitch, would you like to opine on that question?

Mr. HITCH. Sir, I would have to defer to the INS on exactly how it works today. What I have been working on is the future vision of how this would work. Certainly, our objective is to do exactly what you are talking about, to have a tiered system where that police officer would know exactly what the situation for that person is. The top tier would be the 10 most-wanted terrorists, but along the line there would be the people who are on an overstay situation, with specific directions, action codes to tell the police officer how to react to that situation.

Senator SESSIONS. We are going to get to the bottom of that question pretty soon.

Mr. Jordan, what is your view on it?

Mr. JORDAN. Currently, right now, there is a stopgap system in place, wherein absconder information can be accessed through NCIC, and it is currently dependent on INS putting that information into the absconder file.

Senator SESSIONS. Will the FBI accept any INS information indicating illegal aliens and absconder information that they wish to put in it? Or does the FBI refuse to accept—would have to approve that? Or do you object to receiving such information?

Mr. JORDAN. My understanding is that absconder information, where the person has been adjudged to be an absconder, that that information we will enter, if it is provided to us by INS.

As I said in my opening statement, we have a terrorism watch list, which is being integrated into NCIC. And it will be fully implemented within this next 60 to 90 days, to bridge the gap that I think you are making reference to.

Senator SESSIONS. Well, I just want the American people to know something. What the American people need to know is that all over America, when a police officer or sheriff's deputy stops someone, unless they have some high degree of notoriety, that is illegally in this country, they turn them loose. They do not even bother to call INS, from what I understand, because INS has no interest in it. They will not come and pick them up and process them, because they say they are too busy.

And so we have these rules that people think are working, but actually out there on the ground, they are not working.

So it makes a mockery, really, of the immigration laws in America.

So let's go back. You say absconder information; that deals with a circumstance, if I am not in error, in which a full court hearing has been held and an individual has been declared to be illegal and has been ordered to remove himself from the country and fails to do so, but absconds and hides in the United States.

Mr. JORDAN. That is correct.

Senator SESSIONS. Those are very, very few. That would be less than 1 percent of the people here illegally, would it not, Mr. Jordan?

Mr. JORDAN. I would not know the numbers, but it is certainly a distinction between someone who just overstays and someone adjudged to be an absconder.

Senator SESSIONS. Well, I think it is going to be exceedingly small, probably less than one-tenth of 1 percent, but I may be in error about that.

Overwhelmingly, the people that are here illegally have not been taken to court and been officially declared to be illegal. This is when they have contested it in some fashion or maybe got in trouble and there was an official court hearing.

I have information, Mr. Hastings, that there are some 321,000 people who have been ordered deported, but only 2,000 names have been put in NCIC. What would you say about that?

Mr. HASTINGS. I am not sure of those statistics. I believe that those cases are being reviewed. There are procedures that need to be followed before we enter individuals into NCIC, to make sure it is appropriate that they are there. Again, I will include the exact statistics in the follow-up that I can give you on where we stand in terms of how many have actually been entered.

Senator SESSIONS. Well, that is the information I have. Certainly, prior to September 11, that is what the circumstances were, if not worse than that, which just indicates to me that we are not serious about this.

There are people who say, well, we cannot do anything about people who are here illegally. It is just hopeless. One reason it is hopeless is because we are not taking the steps necessary to see that we enforce the law.

To me, as a Federal prosecutor for 15 years enforcing the law and prosecuting a number of immigration cases, America has got to enforce the law fairly. It is just not right to have somebody who patiently waits their turn to come into the United States, and to have their slot, their spot, taken by somebody who is here illegally and who cuts the corners and goes around it.

So I just think that in the course of all this it will help us in security. It will help us also just in maintaining the rule of law in this country.

With regard to approval for a person, let's say from Iran, who would like to come to the United States, what does the American embassy in Iran, what kind of information do they have as they evaluate whether or not that person is a potential good person to trust to come into the country? Do they have access to your computer system?

Mr. HASTINGS. They do not have direct access to our computer systems. There are databases that they utilize—TIPOFF is one—to inform the decision-making. We are working with them to include, again, additional information and make that available. We are working aggressively with a Department of State initiative to establish a collaboration zone to enhance the data sharing and information available to those decisions made before these individuals reach our shores.

Senator SESSIONS. Well, what if an individual that has been approved for admission into the United States from Iran, and I just say that because there are some people in that country that would be dangerous, although normally I think most Iranians reject all terrorism and that kind of thing, but let's just say some country that we know has an indigenous terrorist network that perhaps may be trying to operate there illegally, and that after they have been approved for entry into the United States it is discovered by the consulate that they may be connected to al Qaeda, what is

done? Are they taking any action to identify or apprehend that person?

Mr. HASTINGS. Is State Department taking any action?

Senator SESSIONS. Yes. Would they contact INS and say, "The person that we approved for entry we now think may be dangerous."

Mr. HASTINGS. I cannot testify to specific steps the State Department takes. I do know that information that is being developed cooperatively between intelligence and enforcement agencies is that there is an effort to include that in the inspectional access, the systems that we use as the inspections, to determine whether or not that information can be communicated at the point of inspection. I am not sure what the procedure is at State Department in a case like that.

Chairman SCHUMER. I just had a follow-up here, related to Jeff's question, which I think is on the money.

Right now, and I would ask this of Mr. Hastings and Mr. Hitch, right now if, say, the FBI Counterterrorism Bureau suspects somebody of being a terrorist, and they would be on this list that I think Mr. Jordan mentioned, what you called TWL, and they apply for a visa in any country—they are a foreign national—does that show up on the INS computers right now?

Mr. Jordan.

Mr. JORDAN. Right now, the State Department, when they receive an application for a visa, prior to them approving it, they send that information on the application to the FBI, and we process that through our databases to include databases that have information about terrorism.

Chairman SCHUMER. So every single person who applies for any kind of visa would go through your TWL list?

Mr. JORDAN. Yes. That is going on right now.

Chairman SCHUMER. Through the State Department.

Mr. JORDAN. Right. That is correct.

Mr. HASTINGS. And the INS gets access to it. A Border Patrol or somebody at a port of entry would have access to the IBIS system, which contains the same information. These are coordinated databases that would contain information about——

Chairman SCHUMER. Right. That is what I was asking. So at the border, you would have exactly that information.

Mr. HASTINGS. Yes.

Chairman SCHUMER. So right now we could say that every person on this list—we do not know if we have everybody who might be a terrorist on this list—but anyone we have on this list would be known immediately as they apply to come into the country by both the State Department and the INS, whether it is at the border or in the embassies. Is that fair to say?

Mr. HITCH. I think that is fair to say that that is certainly the intent, and in the post-9/11 world, the Attorney General specifically asked for a review of all those procedures to make sure that if there was anything that could be done, it was done. He followed up just this past week to institutionalize all those procedures to make sure that that is happening.

Chairman SCHUMER. And what is the answer? I know he wants to make sure.

Mr. HITCH. The answer is yes.

Chairman SCHUMER. Yes, okay. And you both agree with that? Sorry, Jeff.

Chairman SESSIONS. What about where there is a visa waiver in our relationship with a country? Many countries have that.

First, if you know how many we have a visa waiver system with? And does this procedure you have just described work in those cases? Do they check?

Mr. HITCH. The visa waiver countries, there are a lot of them. There are something like 29 or 30.

Mr. HASTINGS. Twenty-eight countries.

Mr. HITCH. Twenty-eight visa waiver countries. Those countries basically what they have is a speedy process of getting into the United States based on treaties that have been negotiated. Those procedures do not apply to them. They can come if they have a passport.

So I think that is an area that, for our future look at what we are doing, what we are planning to do is to tighten up on those visa waiver people also, because that is a significant hole in our security.

However, that is going to require renegotiation of those agreements.

Mr. HASTINGS. We do have access to advance passenger information, and we are utilizing that in the inspectional process. And by the fall, we will have that fully integrated in that IBIS environment as well, again, as an interim step, knowing that we have still have an entry-exit system in a very large scope to be planned and developed over the next several years. These are the interim measures that we have taken.

Chairman SCHUMER. But you are basically saying that your system at the borders is a lot better than your system internally in the country. I mean, the kind of thing we read about with the two people, the two terrorists who posthumously got the approval of their visas, shows that things are not in good shape. What you are leading us to believe is that, if they were coming into the country at this point in time, not 9/11, and they were on some kind of list—that is a different issue, how good our lists are—that they would have been blocked.

Mr. HASTINGS. I think that is safe to say. As a matter of fact in those cases, at the point of inspection and the point of adjudication, there was no reason to believe in any of the data that was available in our databases that there was a record that these folks were of interest.

Chairman SCHUMER. Right. Okay.

Senator SESSIONS. The shoe bomber came in the country through another country that we have a visa waiver system for. Mr. Hitch, would our system today catch that or not? Or would that be a weakness in our system today?

Mr. HITCH. I believe that is a weakness in our system today that we are fully aware of and trying to figure out ways to best fill it.

As I mentioned before, the long-term answer is some renegotiation of the visa waiver agreements. I think the passenger manifests that were mentioned by Mr. Hastings are a step in the right direction.

But unless we had some reason to suspect him, the passenger manifests would not have shown up anything.

Mr. HASTINGS. Mr. Hitch is correct in that. I do want to articulate that, in that case, we would check the advance passenger information against what we have in our databases. The question would be, would there be information in those databases that would have suggested that this individual was someone we should be looking for?

Chairman SCHUMER. As I remember, he was an American citizen, right? The shoe bomber?

Mr. HASTINGS. I think he was a British citizen.

He was traveling on a British passport.

Chairman SCHUMER. A British passport.

Mr. HITCH. I do believe that that is a weakness that has to be plugged up. The visa waiver issue has to be plugged up from a policy standpoint.

Senator SESSIONS. Just one more.

Mr. Jordan, with regard to the National Crime Information Center, let's say an individual came here from the United Kingdom. There is no evidence that they pose any threat to America, but under our new system that INS is going to be putting together, I trust he is identified as an overstayer or is identified as a person that otherwise has violated the terms of his entry and is therefore illegally entering here. Does the FBI have any objection to entering all of those people's names into the system?

Mr. JORDAN. Give me one minute, Senator?

Our NCIC system is managed by an oversight panel that is staffed by local chiefs, who work with us in establishing what goes in and what does not go in NCIC files. One of the things we want to make sure is that the information is relevant and useful and mature enough to be disseminated.

Senator SESSIONS. Has the FBI opposed that information coming in? Or is it INS that has no desire to put it in?

Mr. JORDAN. I do not know that sitting here this morning, Senator, I can answer that question.

Senator SESSIONS. Well, the answer I guess fundamentally is, it is not going in. And it is either that the INS is not putting it in or there has been an objection from NCIC to receiving it. If it overwhelmed the computer system, I could understand that. Otherwise, I think it should be in there for whatever value it can provide to a local officer.

I think we, ultimately, if we have any respect for law in America, if we have any respect for fairness and justice, will try to make sure that people who are here illegally are not allowed to continue in that status. And to do so, we have to enlist the local law enforcement, and they have to be able to access it on the computer.

I do not mean to belabor that. That may be a subject for a different hearing, because you are the technicians, you are not the policymakers on this deal.

Thank you, Mr. Chairman.

Chairman SCHUMER. Thank you, Senator Sessions.

I have so many questions, but we are going to move it along. This was all helpful.

Just one final question on this level, Mr. Hastings. I remember back in 1993 when the outcry occurred because the sheik came in through Khartoum, I believe it was, and there was not a computer. I take it every one of our embassies has a computer now, whether INS or State Department. There are no just handwritten lists. And what we are talking about is available in any point of access.

Mr. HASTINGS. I know that our staff overseas has access to computers. Again, I am not sure where the State Department is, but I assume that is correct.

Chairman SCHUMER. Do you know, Mr. Hitch?

Mr. HITCH. I cannot speak for the State Department.

Chairman SCHUMER. Right. OK.

Let me ask you, Mr. Hitch, a couple of questions.

Do you have the authority to order all the various agencies in the Justice Department to do things so that their computers are in greater sync or so that their coordination is in greater sync? How does that work?

Let's say you go to the FBI and then you go to the INS—both Justice Department components—and they have good reason, each of them, to say, "No, no, no, they have to do it my way, or I cannot do it." Each agency says that. Do you have the ability to order them to develop a system to coordinate?

Mr. HITCH. I believe I do, sir. But that is a new position. I have only been around for a month, but in my discussions with the Attorney General when I accepted the position, I made it clear that I thought that was necessary in order to be successful.

Chairman SCHUMER. Right. OK. And so your authority——

Mr. HITCH. And he has asked me to define an organization to make that happen.

Chairman SCHUMER. I see. Good.

Now, what if the same problem occurs from without your agency? In other words, Justice to State or CIA to Justice or DIA to Justice. What happens? What will happen if, say, we need information from DIA or NSA and they, "We are not giving it to any of your Justice Department components," and you say you need it? How does that work?

Mr. HITCH. Well, the way it is working right now, and I can speak from experience on this, even though it is short, is we approach the department directly, and we are participating in what are called these policy coordination committee meetings of the homeland security, associated with a lot of different topics. On this one, it would probably be called horizontal sharing, which is the sharing of information among Federal agencies. On a regular basis, we would discuss those issues and come to resolution of those issues.

Chairman SCHUMER. And someone from the Homeland Security Office is there?

Mr. HITCH. Yes.

Chairman SCHUMER. OK. What if there is an impasse? You may not have had that yet in your short history.

Mr. HITCH. There has not been an impasse in my short history. Basically, I asked that same question and was told that we will work it out, and basically Homeland Security will help us broker the agreement.

Chairman SCHUMER. Okay. So we do not know, but at this point, you have not come across it. I take it neither of you have either, where someone outside of the Justice Department purview, you feel you need certain information from them, and you cannot get it. Because of their own internal reasons, they will not give it to you. I am sure that has happened in the past.

Is that correct, Mr. Jordan? You do not have to give me any specifics, but I am sure it has, right?

Mr. JORDAN. That is correct.

Chairman SCHUMER. And how about now? Is it better?

Mr. JORDAN. Our Director has told us that we are going to share information unless there is a specific or legal reason not to. That has been a sea-change for us at the FBI.

Chairman SCHUMER. Yes. And how about the other agencies sharing it with you, intelligence agencies in particular?

Mr. JORDAN. It is a tremendous change there. I can tell you that in my position as the chief of the corruption section, I brief up all the cases that we have in the presence of CIA and DEA personnel that are assigned to FBI headquarters. They sit in without any reservation on all those kinds of briefings.

Chairman SCHUMER. Mr. Hitch, which agency in your purview needs the most help in terms of bringing its computers up to date, its entry and all of that? Which one is the furthest behind where you want them to be?

Mr. HITCH. Within Justice?

Chairman SCHUMER. Yes.

Mr. HITCH. Obviously, the two largest agencies and the two at the center of this issue are here at the table with me, and so I am looking very closely at both of those and trying to get involved very deeply in all the projects associated with this topic.

Chairman SCHUMER. When we hear that there are mess-ups at the INS, the people in the INS are often quoted in the press saying, "Well, what do you expect? Our computer system is so backward that it doesn't work. It doesn't do what we need." You hear that sometimes from FBI, too, although I think there have been greater efforts to update the FBI computers.

Again, this is not to blame anybody here. We are all new to this.

Would it be fair to say that INS is considerably behind most of the others?

Mr. HITCH. I think INS needs a lot of improvement in terms of its computer system. I think it is fair to say that.

Comparing it to others, I have a difficult time doing that at this point, based on my short tenure.

But I am trying to work with them to improve what they have.

Chairman SCHUMER. I have one final question for all of you. I have more questions that I will submit in writing.

But there has been talk of one sort of supercomputer, where all the information is almost automatically shared. You would have to have privacy safeguards. But, again, that is who manipulates the computer, not what the computer says.

What do you think of that idea? I would ask each of you, given your experience in this, what you think of that idea? What do you think of the idea of the fellow from Oracle who came in and said,

"You just let me do it. I will do it for free, and I will have you all coordinated in no time."

Easier said than done, obviously. When you are worth $10 billion, you can——

Mr. HITCH. Having been in this business for 28 years so far, I certainly respect Larry Ellison. However, it is easier said than done.

From my perspective, I am trying to understand what the business issues are and what the impediments to doing what we want to do are. I do not think it is technology.

We are looking into all different alternatives—supercomputers, data mining. We are looking into distributed databases. We are looking at all the options. And I do not feel that that is the obstacle at this point.

Chairman SCHUMER. But I do think, and you tell me what you think of this, right now there is an era of cooperation because of 9/11. The way the world works, the way bureaucracy works, if, God willing, there is no new terrorist incident a year from now, that could fade back into the old bureaucratic mentalities, unless a system is in place that ensures that sharing. If you believe, as I know the President does and I do, that this terrorism is going to be with us for decades—it is not an al Qaeda phenomena; it is a technology phenomena that we have to deal with.

It would be good to have a system in place that makes sure that there is no slide-back. Do you buy that?

Mr. HITCH. Absolutely. Absolutely.

Chairman SCHUMER. And do you think we will have one in a year or two?

Mr. HITCH. I think putting in place the long-term solution to these issues is going to take more than a year or two. I would couch the problem a little differently than you have. As opposed to the technical solution being a supercomputer, I think the real solution—as a couple of us, Scott and I, mentioned—is looking at enterprise architecture, because that is really where you design into the systems the ability to share information, making sure that you do not have redundancies, making sure that the business functions that are related get related in the system. That is the real answer.

So my long-term approach is to make sure that we are doing that kind of an approach to building systems at the Justice Department.

Obviously, in the shorter term, we have to look to what I would call patches, things to physically integrate information that was not previously in the same database.

Chairman SCHUMER. And have you in the short time that you have been there had disagreements among your component agencies about how to solve some of these problems?

Mr. HITCH. I would not call them major disagreements. I would call them heated discussions about approaches.

I have been involved very significantly in this entry-exit system that is being developed at the INS. I would say we have come up with a collaborative effort that I am pretty proud of.

Chairman SCHUMER. Okay, thank you.

I want to thank the entire panel for being here, and I would ask unanimous consent the record be held open for approximately a

week so others might submit written questions or some of us might, but it was very helpful.

Senator SESSIONS. Mr. Chairman, can I ask one thing?

Chairman SCHUMER. Please.

Senator SESSIONS. Regional Organized Crime, they have a database system too, don't they, Mr. Jordan? The Regional Organized Crime group?

Mr. JORDAN. Yes.

Senator SESSIONS. State systems have data systems.

I really think that we have to do better about getting it all in one system.

You listed, Mr. Hitch, here a number—EPIC and IDENT and JABS. There are a lot of them out there, and how you make this come together in a coherent way is real important.

These systems are sources of power for the individual entities. They create them. They work at them. They put their information in them. They tend to be very jealous of them.

So we want you to know we are behind you in trying to work that out. I think that is fair to say.

Chairman SCHUMER. One hundred percent.

Senator SESSIONS. They have some legitimate concerns, but for the most part, unifying this system is going to be good for America.

Mr. Hastings, with regard to the two individuals—I will just say it this way. You will hear from the people at the top echelons of the Department of Justice and INS and Customs and State and all that; they are looking at this level up here. I do not think they understand or have given nearly enough thought to the grassroots level where you have got two terrorists stopped for speeding in Maryland. They were on those planes that killed American citizens.

Had that information been in the system available to those local police officers when they ran NCIC, which they invariably do when they stop somebody, there would have been a hit, would it not, Mr. Hitch?

Mr. HITCH. Yes.

Senator SESSIONS. And, Mr. Hastings, I know there are policies now, with regard to what you can put in the system and you cannot put in the system. Let's say you have an individual that has been approved properly to come into the United States, and somewhere along the way the embassy or State Department or another agency determines that that person has connections to al Qaeda. You find out that they have overstayed in the United States, but they have committed no provable crime at that point. Can you put in the system legally today, according to our rules and regulations, that information, so any police officer stopping them would know to hold them?

Mr. HASTINGS. It is my understanding in that case, where we have developed specific information, that that would find its way into our watch list and be accessible.

Just the overstay with no other negative information I think is a policy that has yet to be established.

Senator SESSIONS. So a mere overstay with intelligence information.

Mr. HASTINGS. I believe that if the intelligence community has uncovered information that we need to know about, they would be

working through the FBI, and that information would be reviewed and made available in a watch list environment. In that case, I do not think we would be the lead agency on getting that done.

Senator SESSIONS. And, Mr. Hitch, what about a local police officer? Can they hold the individual?

Let's say it comes up on the NCIC—an overstay, flag, contact FBI before releasing—something to that effect is what it ought to say. What power does a local police officer have to hold a person who is illegally in the United States?

Mr. HITCH. Sir, I am not the best person to answer that question, but I do recall just in the past couple of weeks that the Attorney General has made some statements about pilot projects in Florida and elsewhere, where they are empowering the local police to be extensions of the INS in some ways. I know it is a very sensitive topic, but that is happening right now.

Senator SESSIONS. Well, it is not that complicated. Police officers hold people for all kinds of crimes, and if they can hold them for shoplifting, if they can hold them for absconding and not answering warrants for traffic tickets, they can hold them for being in the country illegally.

This is a political deal. It is a political deal that undermines the realistic ability of our country to enforce our immigration laws. So we passed a law, but we create a system so it cannot be effectively enforced.

So we need to deal with that. I think the Attorney General's steps are in the right direction, but it really needs to go a lot further, to me.

And I do not think police officers need 2 weeks of training on how to hold an illegal alien. If you do that, you have basically made it very difficult for them to do it.

Chairman SCHUMER. And on that strong note, we thank the panel.

We are now going to combine the next two panels, so we are going to call all four people up—Congressman Panetta, Mr. Terwilliger, Mr. Anderson, and Mr. Light. What we are going to do is, because Mr. Panetta came here with the proviso that he had a plane to catch, we are going to let him testify, ask him questions, and then go to the other three, if that is okay with you, Jeff. Great.

We put you closest to the door so you can get to that plane.

Is Dr. Anderson here as well? Yes. Great.

Okay, thank you. And I want to thank very much this panel for coming and very much appreciate Senator Sessions' participation and good questions. So what I am going to do is introduce Leon Panetta, let him testify. We will ask him questions, and then we will go to the other three, if that is OK with everybody. Is that all right? Thank you.

Because of his time commitment, I am going to be brief in my introduction. Leon Panetta is co-founder and director of the Panetta Institute, a nonpartisan center for the study of public policy. He has had a very long, very distinguished career, starting in politics in appointed office in his 20s; serving in the House of Representatives for 16 years, four as Chairman of the Budget Committee; and then serving President Clinton as both the head of OMB and then Chief of Staff.

In addition, he was my roommate for 12 years, and he is a man of hard work, intelligence, integrity—just the kind of public servant you want.

So, Leon, welcome. It is great to see you again, and your entire statement will be read in the record and you may proceed as you wish.

STATEMENT OF LEON E. PANETTA, DIRECTOR, PANETTA INSTITUTE, MONTEREY BAY, CA

Mr. PANETTA. Thank you. Thank you, Mr. Chairman, Senator Sessions.

Thank you for asking me to provide my views on the issue of the Office of Homeland Security and whether or not it should have more power in trying to meet this challenge of information sharing within the executive branch.

Let me preface my remarks by saying that obviously I am going to provide these views from the White House perspective. I realize, as with the testimony that you just received, that there are a number of efforts, I am sure, that are going on between the various departments to try to improve the situation.

Chairman SCHUMER. We wanted the first panel sort of to be a little bit of a case study, and now to take it to the larger issue.

Mr. PANETTA. That is why I would like to kind of address it from the larger perspective. Just let me get to the point very quickly.

I do not think there is any question that if you want to have an Office of Homeland Security be effective, it has to have additional power to be able to effectively coordinate the information and activities that are so necessary to protecting this country against the threat of domestic terrorism.

Part of the problem, obviously, is developing more effective technology. We understand that. They do have to develop more effective databases and better computers to put this information into and greater ability to share that information, obviously, at the local level.

And part of the problem is also organizing common policy between a very large number and a diverse number of agencies and departments that you have to work with to try to develop some kind of common strategy.

But make no mistake about it, the biggest problem to centralizing command and control here is the basic culture of the Federal bureaucracy. You have to be able to break through that. You have to be able to deal with a culture that basically resists the kind of coordination and sharing that is so essential to effective law enforcement.

As Chief of Staff to the President, I was responsible for policy development and, obviously, the flow of crucial information to the President of the United States. It is my experience that in the absence of a clear line of authority and a clear chain of command, that the sharing of information within the Executive Branch is haphazard at best.

When a crisis happens or when the White House directly says, "I want information, and the President wants information on a particular issue or a particular crisis," the agencies and departments are obviously forthcoming.

As an example of that, based on my own experience, when Oklahoma City took place and the bombing occurred there at the Federal building, what I did as Chief of Staff was convene a task force at the White House that included the representatives, obviously, of all of the responsible agencies involved with what had happened there for the specific purpose of making sure that they were sharing and coordinating crucial information on that crisis. We also needed to have a single place in which information flow could then go to the public.

In the absence of that kind of presidential mandate or when that kind of crisis begins to—as you see in the present situation—as it begins to move away from public attention, information is largely provided at the discretion of each department or agency.

I always found as Chief of Staff that good news can travel very quickly to the White House. People are willing to tell you if it is good news. But if it is bad news, usually it winds up on the front page of *The Washington Post* or the *New York Times*, and then you wonder why you did not hear about it or why the information was not shared—because nobody wants to provide that kind of bad news, obviously.

So regardless of Administration, I want you to consider the kind of deep and intractable factors that involve the operations of the bureaucracy.

Obviously, the first is protection of turf. There just is a natural instinct in every department and agency to try to protect their jurisdiction. I understand that. There is a loyalty that develops that is necessary for their particular operation. There is a certain competitiveness that is involved to try to sharpen their mission. Every secretary, every director basically talks about the special uniqueness of that particular operation. But the first loyalty is obviously to the President and the overall policy of the Administration and obviously to the American people, and that is a fundamental principle that is so often forgotten.

The size of the bureaucracy, the sheer numbers of departments and agencies that share responsibility for a given area are just overwhelming. Homeland security, as you know, involves well over 40 agencies. When there are that many involved, it is just very difficult to determine who knows what. There are different databases. There are different operations. You have heard some of that this morning. Even within a large department, it was my experience that information can have a difficult time just making its way through the internal chain of command that is within that department. I have had secretaries tell me, when something has happened that was of concern to the White House, I have had secretaries tell me that they had no idea that a certain policy decision was being made at a certain level or that a certain fact had taken place, just because of the sheer immensity of the bureaucracy within that department.

Security of information, you will hear a lot of that on issues that involve, obviously, national security or law enforcement. There is a concern about sharing that information, a concern about compromising an action or mission. And obviously, this is a legitimate concern, but there is no reason why that information cannot be shared

with those that have the proper credentials, particularly at the White House level or at the Homeland Security level.

Fighting for funding is another major problem, because every department and agency understands that their lifeblood is funding. They have developed their own approach to White House aides, to OMB aides, and to Members of Congress for the purpose of funding their particular programs. The dependence on certain Members and aides and programs just often inhibits the sharing of information. They basically understand that they have got to go to certain Members to basically make sure that those Members and those aides are working for them and not working for others.

And obviously, there are personality differences. This is something that is true everywhere, I am sure. But in a large operation like the Federal Government, if you have friction and political competition between personalities, that can seriously affect communications and operations. There has got to be a way to cut through that, and obviously, you do not expect that kind of behavior from professionals. But if they have vital information, it can be used to undermine each other, and that is a reality.

Recognizing the need for command and control, then, and coordinated information and response capability, what can be done to try to break through these bureaucratic barriers and try to accomplish the vital goal? I think the U.S. Commission on National Security in the 21st Century basically made this recognition before September 11, and I think it is still relevant, that we have to create a national homeland security agency with "the responsibility for planning, coordinating, and integrating various U.S. Government activities that are involved in homeland security." They recommended the agency be built on the capabilities of FEMA, the Federal Emergency Management Agency, and include the Customs Service and the Border Patrol and the Coast Guard. I think it can be designed in different ways, but you need to establish some kind of agency, department agency, that has a Cabinet officer that has responsibility in this area.

The appointment of a Director of Homeland Security, as the President has done, obviously is an important step. But unless that Director has direct line authority over the policies and funding of the agencies involved in homeland security, it is just very difficult to control and coordinate the effort. I do not care how likable that person. I do not care how nice that person may be. The reality is that he can persuade, he can try to convince people, but he cannot enforce, and you have to have the ability to enforce actions.

Even with the blessing of the President, the primary instinct of agencies and departments is to protect their own information and their own operations. The reality is that they will do that because there is little threat of consequences.

Funding and line authority primarily rest with each department and agency, so it makes them behave more like independent contractors than team players.

At the very least, and this is a suggestion that I make from my own experience as Director of OMB, Tom Ridge obviously has to have broader authority over funding. I can tell you it would be my view that he would be more effective if you made Mr. Ridge a deputy director at the Office of Management and Budget, responsible

for the budgets of the homeland security agencies, than just being another presidential assistant. At least in that position, you know that he has to oversee those budgets and that he can control the recommendations as to what those agencies ultimately get in their budgets.

A better approach, of course, would be to have and establish a national homeland security agency. Again, I recognize there is no silver bullet here, but having that kind of agency and having better control and coordination and having a clear line of responsibility, not just for the country, not just for the Administration, but for the Congress. You cannot have a situation where you have a Homeland Security Director who, for whatever reason, will not testify to the Congress. You have to have somebody who has the ability to come here, to share information with the Congress, and to be the primary spokesman to the country.

As a former Member of Congress, I recognize the difficulties of establishing any new agency. I know the turf battles that will go on, even in a situation that involves a national crisis. But I do not think that we can afford to simply have the internal politics of the Executive or Legislative Branch prevent the Nation from doing what is essential here to our security.

So, Mr. Chairman, you have a choice. You can either go with the status quo as it exists and try to beat up different agencies and departments as they come up here one at a time. Or you can try to centralize this in a homeland security agency with the power to do the job.

I think it is an important decision that hopefully you will proceed with.

[The prepared statement of Mr. Panetta follows:]

STATEMENT OF HON. LEON E. PANETTA, DIRECTOR, PANETTA INSTITUTE, WASHINGTON, D.C.

Mr. Chairman and Members of the Judiciary Committee:

Thank you for your invitation to provide my views on the issue of the Office of Homeland Security and whether it should have more power in meeting the challenge of information sharing within the Executive Branch.

Let me get to the basic point quickly: There is absolutely no question but that the Office of Homeland Security must have additional power if it is to effectively coordinate the information and activities relevant to protecting our country against the threat of domestic terrorism.

Part of the problem of coordination is developing more effective technology and part of the problem is organizing common policy among a large group of agencies and departments. But make no mistake—the biggest problem to centralizing command control is the basic culture of the Federal bureaucracy.

As Chief of Staff to the President and therefore responsible for policy development and the flow of crucial information to the President of the United States, it is my experience that absent a clear line of authority and chain of command, the sharing of information within the Executive Branch can be haphazard at best.

In a crisis or when the White House demands information on an issue, the agencies and departments are generally forthcoming. As an example, following the Oklahoma City bombing at the Federal Building, I convened a task force at the White House of all the responsible agencies and each day would meet for the specific purpose of sharing and coordinating crucial information on this crisis.

In the absence of that kind of Presidential mandate, information is provided largely at the discretion of the department or agency. Good news generally seems to flow much faster to the White House. Bad news seems to usually wind up first on the front page of the *Washington Post* or the *New York Times*.

Why is this? Regardless of Administration, there are some deep and intractable factors that characterize the operations of the bureaucracy.

(1) *Protection of Turf.* There is a natural instinct in each department or agency to protect their jurisdiction. Loyalty is an important quality necessary to the esprit of any Federal operation. And competitiveness can sharpen the performance of a mission. But the first loyalty is to the President and to the overall policy of an Administration and too often, that fundamental principle is forgotten.

(2) *Size of Bureaucracy.* The sheer numbers of departments and agencies that share responsibility for any given area can be overwhelming. Homeland security alone involves well over 40 agencies. When that many are involved, it is difficult to determine who knows what. Even within a large department, information can have a difficult time making its way through the internal chain of command.

(4) *Security of Information.* In areas that involve national security or law enforcement, there is a concern about protecting information so as not to compromise an action or mission. While this can be a legitimate concern, there is no reason why information cannot be shared with those in authority at other agencies or the White House who have the proper security credentials.

(5) *Fighting for Funding.* Because the lifeblood of each department and agency is money, each has developed its own approach to White House aides and the Congress for funding programs. Obviously, this dependence on specific members, aides and programs often inhibits the sharing of information between agencies if they believe it can hurt their particular budgets.

(6) *Personality Differences.* In any large operation, particularly in government, friction and political competition between personalities can seriously affect communications and operations. Withholding vital information can be one of the ways people try to undermine each other. Again, there is no excuse for this kind of behavior by professionals, but it can be a reality.

Recognizing the need for command control and a coordinated information and response capability for effective homeland security, what steps can be taken to overcome these bureaucratic barriers and accomplish this vital goal?

The U.S. Commission on National Security in the 21st Century laid out the most important step—the creation of a National Homeland Security Agency with "responsibility for planning, coordinating and integrating various U.S. Government activities involved in homeland security." They recommended building this agency on the capabilities of the Federal Emergency Management Agency and including the Customs Service, Border Patrol and Coast Guard.

While the President has appointed a Director of Homeland Security within the White House, unless that Director is given direct line authority over the policies and funding of the agencies involved with homeland security, it will be very difficult to control and coordinate their efforts. He can persuade but he cannot enforce.

Even with the blessing of the President, the primary instinct of these agencies and departments will be to protect their own information and operations first because there is little threat of any real consequences. Funding and line authority will primarily rest within each department and agency, and that makes them act more like independent contractors than team players.

In the very least, Tom Ridge needs broader authority over funding. As a former Director of the Office of Management and Budget, it is my view that it would be more effective to make Mr. Ridge a Deputy Director at OMB in charge of the budgets for the homeland security agencies rather than just another Presidential assistant.

The better approach is for the President to support and the Congress to establish a National Homeland Security Agency. Not only would this ensure better control and coordination within the Executive Branch, it would establish a clear relationship with the Congress and the country as to who is responsible for overall homeland security policy.

As a former Member of Congress, I recognize the difficulties of establishing any new agency, even one essential to dealing with a national crisis. But if September 11 told us anything, it is that we cannot afford to allow the internal politics of either the Executive or Legislative branches prevent the Nation from doing what is essential to its security.

Mr. Chairman and Members of the Committee you have two choices: You can accept the status quo—a Homeland Security Director with little or no direct line authority; or you can establish a single Homeland Security Agency with the power needed to do the job. This is not just a political decision; it is a national security decision that will determine whether we can more fully protect our citizens from acts of terrorism. I urge you and the Congress to make the right choice.

Chairman SCHUMER. Well, thank you, Leon Panetta, and once again your remarks are excellent. Whether one agrees or not, they are just laid out terrifically.

Let me ask you this. The report that you refer to that was made before 9/11 gave rather limited agencies. You know, there were a few there—the Border Patrol and FEMA and others. Would you, just off the top of your head, think other agencies would have to be part of this, or at least parts of other agencies?

And the second question is, there are some agencies you would not want to put under the direct authority of the Office of Homeland Security, but you would certainly want that person to have authority to get certain things done. Take information sharing between the FBI and the State Department, let's say. How do you accomplish that in this kind of an office as well?

Mr. PANETTA. Well, obviously there would be, I think, at least parts of other agencies that I think that ought to be included here.

Having seen efforts to try to get the Coast Guard located in a number of other areas, it is impossible to do. I mean, with all respect to the commission, that is going to be tough to do. But in the very least, if you could get an element of Coast Guard that is associated with enforcement located there, I think that would be important, and the same thing is true for these other agencies.

I think building it on FEMA does make sense, just because FEMA has the responsibility for emergency response, and I think that is true for others, so I would look at that.

In addition, I do think that you need a council at the White House. I would have the head of the Homeland Security Agency chair that council. But the difference is that as a Cabinet member and a lead Cabinet member, that person would have greater authority then to get responses from the other agencies at the table.

So the way to get at having the Defense Department, having the CIA, having DIA, having these other agencies at the table would be make sure that you, in addition to establishing a Homeland Security Agency, that you formalize a council within the White House for that purpose.

Chairman SCHUMER. Let me ask you, does it make sense to have a strong and statutory national chief information officer, maybe under the homeland security person, to deal with the problems that we face? I mean, the model is so obvious.

Mr. Hitch talked about now how he has authority within the Justice Department, which no one had ever had before, to sort of knock heads and get one information-sharing system. But of course, if that model works, then the obvious question is, why don't you use a similar model when you go interagency as opposed to intra-agency in this kind of chief information officer, on the area of information would make sense. What do you think of that?

Mr. PANETTA. I think either a directorate or an assistant director responsible for coordinating that information would be very important, because again, even though within the departments there will be efforts now to try to better coordinate information, you have to be able to establish a larger information base in which different agencies can be able to share information, and you can require that information to be shared.

Right now, there is no central location for that kind of information. In the absence of that, you basically have to go hat in hand, then, to Justice, to CIA, to these other departments and say, "What do you know about this and what is happening?"

Chairman SCHUMER. What about the answer to this?

And I have read in the paper now that the White House is actually considering upgrading Tom Ridge's office, which my guess is, if they were to propose it, it would pass the House and Senate like a hot knife through butter.

But what about the alternative answer, which says, look, the President is in charge of this. You do not really need this Cabinet-level officer, because that is his job to do. If he wants it done, he will get it done, and if he does not want it done, no matter who you have there, he will not get it done.

Mr. PANETTA. The President of the United States has responsibility in a number of areas each day. He is dealing obviously with foreign policy crises. He is dealing with legislative issues. He is going out on political trips. He is going here. He is going there. Admittedly, the President of the United States appoints somebody as an assistant to oversee that, but the problem is that the agencies and departments know very well that unless the President is calling on every issue that the Homeland Security Director is trying to enforce, that they can basically nod, say "yes", and walk away and nothing happens.

You have to have line authority. And the only way you really have line authority is controlling the purse strings.

Chairman SCHUMER. So you would say that this office has to have authority, but budget authority as well?

Mr. PANETTA. Absolutely. Absolutely.

Chairman SCHUMER. OK. I know you are in a hurry. We very much appreciate your remarks. I am going to ask the other witnesses what they think of them, and have a safe flight.

Mr. PANETTA. Thank you, Mr. Chairman.

Chairman SCHUMER. Thank you. Great.

Okay, now let's introduce our next three witnesses and hear from them and see what they have to say about chief of staff, Congressman Panetta's fairly strong views on these issues.

First, we are honored to have somebody just like Leon Panetta, who stands for excellence in government and has been there a long time in many different capacities, even though now he is out of government. My guess is he will be back at some point or another. But George Terwilliger is a partner now in the office of White & Case, which is an international law firm. He represents institutional clients in dealings with the U.S. Government. During 15 years of public service, Mr. Terwilliger was the Deputy Attorney General of the United States, second-ranking in the Department of Justice. He was the U.S. Attorney in Vermont and Assistant U.S. Attorney in Washington, DC, and in Vermont. On policy matters, he was a principal in the highest councils of government charged with addressing a broad array of legal, policy issues arising in the Executive Branch. Mr. Terwilliger has served as counsel to a U.S. Senate investigation, outside general counsel to Federal commissions, as well as confidante and counselor to elected and appointed officials.

We are also honored to have Dr. Phil Anderson. He is a senior fellow in the international security program at CSIS, the Center for Strategic and International Studies. He specializes in homeland security studies and was previously Director of Defense and Aero-

space Content for the Intellibridge Corporation, a provider of customized Internet-based intelligence and advisory solutions. He also served 23 years in the Marine Corps, and his military experience includes leadership of operational organizations, from platoon through battalion, with deployments worldwide. He was the principal operations adviser to the commander of the U.S. Marine Corps Forces Atlantic, where he conducted research and onsite analyses, resulting in successful antiterrorism force protection plans for the U.S. forces assigned to Haiti.

And finally, Dr. Paul Light is the founding director of the Center for Public Service and Vice President and Director of Governmental Studies at Brookings. After serving as director of studies at the National Academy of Public Administration from 1984 to 1997, he came to Capitol Hill as a senior staffer to the Senate Governmental Affairs Committee. He then became Associate Dean and Professor of Public Affairs at the University of Minnesota's Hubert H. Humphrey Institute and was Director of the Public Policy program at the Pew Charitable Trust in Philadelphia. Dr. Light has written 15 books, including "Thickening Government," "The Tides of Reform," and "The True Size of Government."

Each of your entire statements will be read into the record.

And, Mr. Terwilliger, you may proceed.

Senator SESSIONS. Mr. Chairman?

Chairman SCHUMER. Please.

Senator SESSIONS. If I could have a moment of personal privilege to welcome my good friend George Terwilliger. He used to be my boss; he was the Deputy Attorney General.

But more than that, what we liked about him, and all the prosecutors out around the country liked, he had been a line prosecutor; personally tried hundreds of cases and knew all about that, and then had served in Vermont as a United States Attorney, where he was a hands-on United States Attorney.

So not only did he have a view from the high echelons of the Department of Justice, but he knows what it is like out in the real world.

George, it is great to have you before us.

STATEMENT OF GEORGE J. TERWILLIGER III, PARTNER, WHITE & CASE, WASHINGTON, DC

Mr. TERWILLIGER. Thank you, Jeff, Senator Sessions, and thank you, Mr. Chairman. I do appreciate being invited here.

I cannot help but observe, in light of your kind introduction and Senator Sessions' remarks, that Jeff and I shared duties at the Justice Department on the Attorney General's Advisory Committee of United States Attorneys when we were both United States Attorneys. Regretfully, I must say that some of the very information sharing-issues, and the effect of information sharing on how things really work out in the real world where the rubber meets the road, were topics of more than a few of those meetings, some of the selfsame issues we are here to talk about today.

Chairman SCHUMER. Which might give us cause for pessimism. [Laughter.]

Mr. TERWILLIGER. Well, actually, I think what it may be is that, for all of the tragedy of September 11, it may in fact be the impetus

to change some things that will not only help us in dealing with terrorism, but with a lot of other national problems.

Mr. Chairman, thank you for taking my statement for the record. I will try to briefly summarize a couple of the points that I have here, in the interests of time.

I do want to say at the outset that despite your very generous introduction, I do not claim to have all the answers, maybe not even some of them. I am not sure I even know all the questions, but I will share some observations.

My statement goes into some detail about the importance of intelligence historically to success in our military endeavors. Today, while we may be in a different kind of war, we are in a war, and this is not a metaphorical war. I have heard some people recently describe it that way. We are really facing a new paradigm of warfare.

But it is a war, and it is a war where our fundamental liberty interests are what is at stake. In my view, knowledge is the most important weapon we have to be able to fight that war against terrorists.

We can tighten our borders. We can improve aviation security. We can do a bunch of other things that will improve infrastructure security. But there is a real danger, I think, in concentrating on those tangible and visible improvements that we could develop a Maginot Line-type mentality that will lull us into a sense of security based on what we see, but does not protect us from the real threat.

The fact of the matter is, Mr. Chairman, I believe that we cannot remain the kind of free and open society that we exist to be without remaining vulnerable to people who are both willing to subvert the rule of law and to surrender their own lives or perhaps the lives of others to create mayhem and destruction in our midst.

What this means is that intelligence, information about who our foe is, what they are planning to do, how they operate, is what is essential to victory in order to preempt further attacks. I would also observe that, as we divide the response to terrorism into prevention or preemption and consequence management, intelligence has great value on the consequence management side as well. We cannot prepare for everything that we have to deal with. It makes more sense to know more about what we are most likely to face and prepare for that.

So the first question for me in terms of how the government is organized in terms of dealing with counterterrorism—how it is best organized—is how can we improve our counterterrorism intelligence effort. I think first the fact that this hearing is being held and that this topic is before the Congress and before the Administration is important, because we simply have to recognize and understand how important information is to our eventual success.

On a more practical level, somebody has to be in charge of that function. It is one of the principal functions of the counterterrorism effort, and somebody has to be in charge of it. I think if you asked the question today, "Who is in charge of counterintelligence intelligence functions within the government?" the answer would be a lot less clear than it ought to be.

There are also several policy issues that may inform a reasoned judgment about how to best organize the government to deal with this. For example, is this a law enforcement function? I would say, not entirely. Is it a military function? Not necessarily, but perhaps sometimes. Is it largely a national security function? Arguably so.

I do not think these are academic points. The need to defend ourselves here at home, based on information to be acquired both here and abroad, diminishes the traditional distinctions between counterterrorism responsibilities of law enforcement agencies and those in the intelligence community.

In addition to that, I think when we talk about reorganizing the law enforcement functions of some of our major agencies to focus on counterterrorism, we should not lose sight that even though counterterrorism, as you remarked before, Mr. Chairman, will be with us for decades, it is not going to be here forever.

I see my light is on, so I will submit the rest of my statement for the record, if I may just make a couple of closing points.

I think we ought to consider some other kind of an agency to perform at least the intelligence function in counterterrorism. It is clear that somebody has to be in charge. It is clear that it has to be someone that bears the President's authority and can direct the activities of other agencies, coordinate with State and local governments, and, indeed, the private sector, as I mention in my statement.

The idea of having an agency or a unit or a combination of agency functions to do this is not inconsistent, as Mr. Panetta mentioned, with also having a council that is a domestic analog to the National Security Council at the White House performing this function with someone bearing the President's authority in charge of that.

I do not think it is a good idea to take what is essentially now Governor Ridge's office and make it operational. The White House should not run operations.

Thank you, sir.

[The prepared statement of Mr. Terwilliger follows:]

STATEMENT OF GEORGE J. TERWILLIGER III, PARTNER, WHITE & CASE, WASHINGTON, D.C.

Mr. Chairman and Members of the Committee: I was asked to assist your consideration of government organizational issues related to counter-terrorism. I thank you for the invitation, but let me say at the outset that I do not claim to have a lot of answers, nor even to know all the questions. Thus, I offer no advice to anyone. Rather, I am pleased to share some observations based on my experience that I hope will assist consideration of how to best defend the United States from terrorist attack. Biographical material concerning my background is attached for your reference.

Tomorrow is the 226th anniversary of one our fledgling Nation's early intelligence successes. When Paul Revere rode through the Massachusetts countryside awakening the citizen army, he was functioning as intelligence officer, analyst and disseminator of product. Observation of the British fleet, signaling the enemy's intentions from the tower of the North Church and a call to arms from horseback combined to provide and disseminate the intelligence that made the following day a success for the colonial forces fighting a war.

Today we are in a different kind of war, but a war nonetheless. This is not a metaphorical war. We are confronted with a new paradigm of warfare.

It is one where we face a clandestine foe using tactics that include the use of common instrumentalities of our commerce as weapons against us. It is every inch a war to defend our country from fundamental threats to liberty.

In my view, knowledge is the most important weapon we have in the war against terrorists. We can and should tighten our borders, improve transportation security, increase immigration controls and take a host of other security measures. However, there is a danger of developing a "Maginot Line mentality" that would mistake these tangible and visible improvements to security as a complete defense against the terrorist threat. We cannot remain a free society without also remaining vulnerable to those willing to subvert the rule of law and surrender their own lives in order to create mayhem and destruction. The only way to best such people is to know who they are, what they are planning and to stop them.

This gives us something in common with our colonial predecessors. It means that intelligence—information about who our foe is, how it operates and what its plans are—is essential to our victory. Today the objective is to acquire the information necessary to preempt further attacks. Large, clandestine outlaw organizations cannot be completely eliminated. But their capabilities to operate can be greatly diminished and even destroyed if we understand who they are and how they function. Intelligence also has value in helping those who must manage the consequences of attack anticipate what particular challenges they are most likely to face.

So, for me, the first question concerning how the government is organized to deal with terrorism today is how can we improve our counter-terrorism intelligence effort? I have a few observations.

First, we need to simply recognize and understand how important the intelligence effort is to success. If one accepts the premise that our counter-terrorism program requires detailed information about our foes, then it must be asked, who is in charge? Perhaps because perception of the current threat has emerged gradually and only become a matter of great urgency in recent months, I think the answer to that question may be less clear than it ought to be.

Second, there are several policy issues that may inform a reasoned judgment about how the Government would be best organized to fight terrorism today. Chief among these is the issue of defining clearly the nature of the current counter-terrorism mission here in the United States. Is this a law enforcement function? Not entirely. Is it a military function? Not necessarily. Is it a largely national security function? Arguably so.

I do not intend an academic discussion. These questions, and other related issues, have very practical implications. The need to defend ourselves from attack at home with knowledge of what is going on both here and abroad may diminish the traditional distinction between the counter-terrorism responsibilities of law enforcement agencies and those of the intelligence community. For example, is the FBI gathering information in criminal investigations or for other intelligence purposes? Can the CIA and other community agencies share classified terrorism information with Federal law enforcement agencies?

Likewise, we might bear in mind that while making us safe from terrorist attack will take time, it is a mission that is more limited than the general Federal law enforcement responsibility. Thus, one might question whether the broad powers and authorities necessary for counter-terrorism measures should be provided as general law enforcement authority. This could result in relatively extraordinary powers being applied to a wide range of investigative activities having nothing to do with terrorism. Conversely, the authority necessary to effectively combat terrorism may be withheld out of concern that we not expand law enforcement powers in general. In my view, despite some current modernizing that is necessary, the FBI and other Federal law enforcement agencies have built well deserved reputations for excellence in making this Nation more safe from crime. For all these reasons, I believe we should be cautious in fundamentally altering the role and authority of Federal law enforcement agencies.

My third observation is that, given the foregoing considerations, it maybe worth considering a new organizational approach to counter-terrorism, especially as to the intelligence function. This could be a new organization, or new unit or task force made up of a combination of parts of existing agencies. What to me renders this worth considering are three principal factors:

1. The counter-terrorism intelligence challenge today is a domestic-international hybrid which may obviate the utility of traditional distinctions between domestic and international terrorism;

2. Preempting further attacks and neutralizing terrorist capabilities are likely to necessitate intrusive investigative activities at home and unprecedented coordination of domestic and international intelligence functions.

3. The organizations and the people performing these tasks must have clear and unambiguous legal authority for their work.

A smaller organization dedicated to counter-terrorism intelligence may be both more nimble in, and more accountable for, the use of more powerful investigative

authority that also crosses traditional legal, policy and agency jurisdictional lines. This may not be any answer at all, but we should not let the way we have been organized to date dictate what we do going forward without consideration of alternatives.

My fourth point is that, regardless of the organizational structure used, we must improve the quality and quantity of information made available to those upon whose work our security depends. We cannot allow their work to be hindered by systemic inadequacies. For example, putting terminals from multiple information systems in one room and calling it an "intelligence center" is no substitute for true systems integration. Our Nation is in the forefront of information technology and our intelligence agencies should have state-of-the-art information systems. If government procurement procedures are an impediment to keeping these vital functions on the cutting edge of this rapidly changing technology, then the way government acquires, maintains and updates this technology needs to change.

My fifth and final observation is that further organizational changes in government to address the terrorist threat must account for the necessary involvement of many Federal agencies, State and local governments and the private sector as both contributors and consumers of counter-terrorism intelligence. Federal agencies of limited jurisdiction, such as Immigration, Customs, BATF and others make extremely important contributions to counter-terrorism, including by collection of valuable intelligence in the ordinary course and by executing specific tasks in furtherance of intelligence objectives. Each performs part of a critical intelligence function that must be, in my judgment, not just coordinated, but directed.

The same premise is true as to State and local governments, including their law enforcement components. While Federal direction is not called for, coordination in counter-terrorism is. Time and again State and local authorities, which have the most frequent and routine encounters with the general population, discover information that, when placed into a bigger picture, may be critical to counter-terrorism objectives.

The private sector's potential to contribute should not be overlooked. Experience has shownthat the terrorist organizations and their support networks make considerable use of private sector services, educational and employment opportunities. Business can be a great help, but the effort needs Federal leadership and assistance.

Are we doing a better job of all of this today then before September 11? While I have no access to non-public information, I am sure that we are doing better, much better. I would not be surprised to learn at some point in the future that our government and our allies have succeeded in stopping one or more significant terrorist episodes in the last several months. The recent capture of a key terrorist leader is a reminder that there are many people whose names we will probably never know, and whose faces we will never harm's way in distant places so that see, going we and our families may sleep in safety and security. If something more can be done here, we owe it to them to do it.

Thank you.

Chairman SCHUMER. Thank you, Mr. Terwilliger, again, for your intelligence and being right to the point.

Dr. Anderson.

STATEMENT OF PHILIP ANDERSON, SENIOR FELLOW, INTERNATIONAL SECURITY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, WASHINGTON, DC

Mr. ANDERSON. Good morning, Mr. Chairman, Senator Sessions. It is an honor to be here this morning, and I thank you for accepting my longer statement into the record.

I would like to begin by saying that we are barely 7 months into what I believe to be a much deeper examination of the homeland security issue.

The President has given Governor Ridge the task of developing a national strategy for homeland security, and it is important to note that despite the criticism in the media and on Capitol Hill that the Office of Homeland Security is understaffed and has no budget authority or power to make decisions. I believe that the

public should understand that the Administration has really not been given enough time to fully address this new challenge.

While time is of the essence, this new environment demands some patience to allow a comprehensive strategy to emerge. In the absence of a comprehensive strategy, there can be no clear understanding of the threat to be addressed or any real sense of the priorities from which specific requirements will emerge. Assuming the Office of Homeland Security can produce a comprehensive strategy this year, once it is published, the debate can begin on implementation.

Although there are numerous challenges associated with securing the homeland, the following are a few that I believe should be given priority going forward.

First, a national strategy as the basis for initiating government reform. In the absence of a comprehensive national strategy which addresses all aspects of waging an ongoing war against terrorism—to include detection, preparation, prevention, protection, response, and recovery—there can be no framework for establishing clear priorities or defining requirements to base decisions on how to organize the government and spend the taxpayers' money.

With real threats to the homeland and agreement that we are unprepared to deal with those threats, what is needed is continued leadership in the Administration to finish a comprehensive national strategy. Significant organizational reform cannot happen without all the strategic underpinnings—the strategy and all its interrelated parts that enables government to make decisions on how best to move forward.

Second, a national strategy that addresses the principal obstacles to information sharing and coordination. No one disagrees the coordination and the sharing of information is absolutely essential in this environment, but there is little mention or debate about the cultural barriers that exist both within the Federal Government and between the Federal Government and the State and local governments, and between all aspects of government and the private sector. With extremely large agencies like those in the intelligence community, the senior leadership has their own business interests and their own relationships with customers and capabilities that they think they are protecting, that truly are the source of their influence.

The CIA is a good example, and in many ways is supposed to be the focal point for the intelligence community. The CIA has privileged access to the President of the United States and privileged access to the Congress. Why would the Director of Central Intelligence want to cooperate fully with other intelligence agencies and give up the power that he has as CIA Director?

That said, I believe that behavior can be changed through incentives and disincentives. Leadership is critical to cultural change—leaders who see the broader need, the greater good, and aggressively pursue them to initiate change in their organization and across government.

The inherent distrust between the Federal Government and State and local governments is another obstacle that will have to be overcome. In this new environment, State and local assets will play the lead role in responding to and managing the consequences

of an attack. With the exception of some specialized Federal capability in the Department of Energy for nuclear weapons and in the Department of Defense's capability for chemical and biological response, the majority of first response assets will come from State and local governments.

It would seem that much attention has been focused on the Federal apparatus, but the national strategy, to be comprehensive, must establish the framework for effective communication and coordination at every level of government.

The terrorists who attacked the World Trade Center and the Pentagon on September 11th were able to move information, people, and finances across a sophisticated terrorist network. The fact that government at all levels is not networked must be addressed.

The intelligence community again offers a good example. There are 14 agencies in the intelligence community doing analysis. Coordinating intelligence across those disparate agencies involves moving information across those agencies.

The terrorists of September 11th proved that they could beat us at this game. On September 12th, if you were employed by the Nuclear Regulatory Commission, for example, you were getting reports about Osama bin Laden's potential attack against nuclear facilities. Most assuredly, those reports came from a newspaper or from CNN, but not from the intelligence community.

We are still in the infancy stage of determining how best to do this, but in the context of homeland security, if you are a fireman or if you are a policeman, you certainly do want and should expect relevant information and effective communication from your Federal government. As the concern about security abates, as it inevitably will, networking the Federal Government with State and local government functions must be aggressively pursued.

Third, a national strategy that provides for private sector involvement. A good example of the complexity of initiating public-private cooperation can be seen in the containerized shipping industry. Approximately 7.5 million containers enter the United States each year, and the Customs Service only inspects 2 percent of those. The contents of these containers originate with approximately 450,000 shippers globally. This would appear to represent an unworkable number, but I believe that there are steps that can be taken now to reduce this vulnerability. An interesting statistic is that the contents of 60 percent of those shipping containers entering the United States originate with just 1,000 large shipping companies worldwide. This would seem to be a workable number where cooperation between government and the private sector could again make a difference and drastically reduce our overall vulnerability.

Recently, and I think it was just yesterday, 60 large corporations agreed to work with the government as part of the Customs Trade Partnership Against Terrorism to ensure adequate security of goods entering the United States, in exchange for faster passage through border checkpoints.

Much of the Nation's strength rests on its privately owned critical infrastructure, but the private sector does not just own and operate the Nation's critical infrastructure. The private sector owns a lot of expertise that could improve the way in which government

approaches the information-sharing problem. The Y2K problem is a good example, where the private sector did a much better job in understanding the problem in developing responses to it.

And I will wrap this up quickly.

Networking is an area that the private sector has mastered. They proved that during the Y2K situation.

In the National Security Council or Homeland Security Council, you will not find our Federal agencies networked in the same way that you would find similar functions networked in the private sector. Developing public-private partnerships is complicated by the need to protect sensitive information and the lack of information sharing and coordination between the numerous agencies of the Federal Government with responsibility for homeland security.

The national strategy must be the vehicle for simplifying the communication and coordination problem within government and between government and the private sector. The private sector should be included in the development of the strategy, and the strategy must formalize the means to ensure private sector involvement in its implementation.

In conclusion, Mr. Chairman, over the long term, in the absence of a comprehensive national homeland security strategy, there can be no clear understanding of the threat to be addressed or any real sense of priorities from which specific requirements will emerge.

Mr. Chairman, my time is way passed up. We appreciate the Committee's leadership on this issue and we look forward to helping in any way we can at CSIS.

[The prepared statement of Mr. Anderson follows:]

STATEMENT OF PHILIP ANDERSON, SENIOR FELLOW AND DIRECTOR, HOMELAND SECURITY INITIATIVE, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

I. Introduction.

Good morning, Mr. Chairman, Members of the Committee, it is an honor to be with you today, to present my views on "Should the Office of Homeland Security Have More Power? A Case Study in Information Sharing." Let me begin by saying that the statement I am about to give represents my views and in no way should be taken as the institutional view of CSIS. Before beginning though, let me provide you with some background on the work we are doing at CSIS.

CSIS has completed a number of homeland security projects both prior to and since the tragic events of September 11. In January 2001, CSIS released a report on the results of an 18-month study, *Homeland Defense: A Strategic Approach.* In June 2001, CSIS co-directed *Dark Winter*, a high-level simulation of a smallpox attack originating in Oklahoma City. In the immediate aftermath of September 11, CSIS convened an internal task force on terrorism, the results of which were published in *To Prevail: An American Strategy for the Campaign Against Terrorism.*

CSIS is currently working on two projects in the area of Critical Infrastructure Protection:

(1) A comprehensive series of events to address critical infrastructure issues facing the United States establishing the foundation for a report that will focus on what business and government can accomplish together to meet future threats—pulling together public-private partnerships.

A simulation exercise, patterned after our *Dark Winter* effort—to focus on energy infrastructure in the United States. Rather than consequence management, this simulation exercise will focus on the less understood—and explored—scenarios in which policymakers must decide on whether and how to act in the case of a credible threat against critical energy infrastructure.

II. Overview.

In the 7 months since the tragic events of September 11, there has been a great deal of momentum, both inside and outside of government—and it would seem that we are all developing a clearer understanding of the Homeland Security problem in

all of its complexity—but most often, solutions remain out of reach—which should be expected at this point—as we are barely 7 months into a much deeper examination of the issue which in most ways represents the most daunting challenge the United States has ever had to address.

In this new and very dangerous environment, it is clear that government reform will be necessary to ensure clear lines of authority, responsibility and most importantly, accountability to unify the efforts of the 46 Federal agencies that, to varying degrees, have responsibility for Homeland Security. With responsibility spread across so many agencies, effective communication and coordination is extremely complicated and will only become more difficult in the long term as threats to the homeland increase. This is made far more complex by the additional requirement for the Federal Government to coordinate and communicate efforts with State and local governments and further, to develop the means to work with, and cooperate with the private sector.

The most important question to consider at this juncture is: When should reform be initiated? Some would argue that there is no time to waste and that well-informed decisions should be acted on immediately in this environment. However, the President has given Governor Ridge the task of developing a strategy for National Homeland Security and as such, the Office of Homeland Security should be allowed some time to fully address the problem. In the absence of a comprehensive strategy, there can be no clear understanding of the threat to be addressed or any real sense of priorities from which specific requirements will emerge. If the strategy that emerges is truly comprehensive, the debate that will follow will certainly involve the appropriate organization of government to address the problem.

It would seem that with each passing day, the Administration, in the process of developing a National Strategy, is learning that organizational and process reform will be necessary to streamline the process of coordination and communication. At a Senate hearing on April 11, to address Senator Lieberman's proposal to create a Department of National Homeland Security and a White House Office to combat terrorism, at which I was also fortunate to testify, OMB Director Mitch Daniels Jr., told the Senate Government Reform Committee that President Bush "has said from the outset that the structure for organizing and overseeing homeland security may evolve over time . . . should the ongoing strategy review ultimately recommend to the President a different homeland security structure, there is a chance it may resemble Senator Lieberman's bill." Among the many organizational issues the strategy will have to address, the following would seem most important:

Create a foundation for unifying the efforts of the Federal Government or at least establish the conditions for effective cooperation and coordination.

(2) Point the way for those agencies of the Federal Government, with direct responsibility for Homeland Security, to effectively cooperate, coordinate and communicate with State and local governments.

(3) Establish the conditions for every level of government to effectively cooperate with the private sector since they own and operate most of the critical infrastructure in the United States and as such, are ultimately responsible for securing it.

Developing a National Homeland Security strategy that points the way toward effectively addressing these issues is no small task, it is truly a daunting challenge—the likes of which have never been faced at any other point in our Nation's history. It is important to note that despite the criticism in the media and on Capitol Hill—that the Office of Homeland Security is understaffed and has no budget authority or power to make decisions—the public should understand that the Administration has really not been given enough time to fully address this new challenge. While time is of the essence, this new environment demands some patience to allow a strategy to emerge. The strategy should serve as the basis to initiate government reform and allocate resources and assuming the Office of Homeland Security can produce a comprehensive strategy this year—and once it is published—the debate can begin on implementation.

III. The Challenges.

Although there are numerous challenges associated with securing the homeland, the following are a few that should be given priority going forward:

A National Strategy as the basis for initiating government reform: There have been numerous commissions and studies conducted—the Hart-Rudman Commission, the Gilmore Commission, the Bremer Commission, and the Center for Strategic and International Studies Working Group on Homeland Defense—that addressed the lack of coordination among the 46 Federal agencies that have specific responsibilities for Homeland Security. There have also been a number of proposals floating around in the Administration and in Congress that call for consolidating some of the agencies responsible for securing the homeland. The Administration's proposal

to consolidate Immigration and Naturalization Service, Customs and the Border Patrol in one agency and Senators Lieberman and Specter's proposed National Homeland Security and Combating Terrorism Act of 2002 are just two examples. Governor Ridge's original proposal also included the Coast Guard and border-related parts of the Agriculture Department. In addition, many commissions and studies recommended that Congress develop the means for reviewing the President's policy and budget for Homeland Security. The lines of responsibility are unclear in the Executive Branch but they are just as unclear in the Legislative Branch given the existing committee structure that further complicates coordination in the Executive Branch.

Most importantly, in the absence of a comprehensive National Strategy which addresses all aspects of waging an on-going war against terrorism to include, detection, preparation, prevention, protection, response and recovery, there is no framework for establishing clear priorities and defining requirements to base decisions on how to organize the government and spend the taxpayers' money. With real threats to the homeland and agreement that we are unprepared to deal with those threats, what is needed now is leadership in the Administration to finish a comprehensive National Strategy. Significant organizational reform cannot happen without all the strategic underpinnings—the strategy in all its interrelated parts—that enables government to make decisions on how best to move forward.

A comprehensive threat assessment as the basis for the National Strategy: It would seem that the Administration has, since September 11, taken a "vulnerabilities-based" approach to the problem. That is, in the absence of a strategy, they have attempted to identify the Nation's critical vulnerabilities and focus attention and resources accordingly. Unfortunately, at this juncture, this is exactly the condition the public should expect where everything appears to be a critical vulnerability. This situation will not resolve itself until the Nation has a comprehensive Homeland Security strategy.

At the heart of any effort to develop a strategy is the requirement to address the likely threats. The strategy that emerges at the end of the development process will need to be first and foremost, *threat-specific.* However, defining likely threats in this new environment is problematic in that they will likely derive from multiple sources with different objectives and various means to do us harm. Defining the threat is risky but absolutely necessary to developing a coherent National Strategy to fully address the problem. It is hard to develop plans, organize and allocate resources to address the myriad vulnerabilities that exist without taking an informed position on potential threats.

While we remain extremely vulnerable in many areas, most do not represent critical vulnerabilities simply because they are not likely targets. How many people would argue, at this point, that commercial aviation is a critical vulnerability? On the other hand, private aviation with 500,000 private pilots and 200,000 private aircraft operating from approximately 18,000 airfields could represent a critical vulnerability. Some would argue that the nuclear power industry is critically vulnerable. I would submit that the nuclear power industry, the most regulated in the United States, is far less vulnerable than other aspects of energy infrastructure to include, liquid natural gas operations, refineries and petro-chemical operations. Without an informed assessment of how those that would do us harm may act, the ability to organize and allocate resources effectively is extraordinarily difficult, if not impossible. Another important point relates to the way in which the current organization of government looks at the threat. FEMA is a good example—with an organizational culture that has, for the most part, addressed natural disasters rather than a thinking enemy.

A National Strategy that addresses the principal obstacles to information sharing and coordination: There are numerous obstacles that stand in the way, culture certainly not the least among them. No one disagrees that coordination and the sharing of information is absolutely essential in this environment but there is little mention or debate about the cultural barriers that exist both within the Federal Government and between the Federal Government and State and local governments, and between all aspects of government and the private sector. With extremely large agencies, like those in the intelligence community, the senior leadership has their own business interests and their own relationships with the customers and capabilities they think they are protecting that are the source of their influence. The CIA is a good example and many ways is supposed to be the focal point for the intelligence community. CIA has privileged access to the President of the United States, and privileged access to the Congress. Why would the Director of Central intelligence want to cooperate fully with the other intelligence agencies and give up the power that he has as the CIA director? However, behavior can be changed through incentives and disincentives. Leadership is critical to cultural change—leaders who see

the broader need—the greater good—and aggressively pursue them to initiate change in their organizations and across government.

The inherent distrust between the Federal Government and State and local governments is another obstacle that will have to be overcome. In this new environment, State and local assets will play the lead role in responding to and managing the consequences of an attack. With the exception of some specialized Federal capability in DOE for nuclear weapons and DoD's specialized chemical and biological capabilities, the majority of first response assets will come from State and local governments. It would seem that the Federal Government is primarily focused on the Federal apparatus, but the national strategy, to be comprehensive, must establish the framework for effective communication and coordination at every level of government.

The terrorists who attacked the World Trade Center and the Pentagon on September 11 were able to move information, people, and finance across a sophisticated terrorist network. The fact that government at all levels is not networked must be addressed. The intelligence community again offers a good example. There are at least 11 agencies in the intelligence community doing analysis. Coordinating intelligence across those disparate agencies involves moving information across those agencies. The terrorists of September 11 proved that they could beat us at this game. On the September 12, if you were employed by the Nuclear Regulatory Commission, you were getting reports about Osama bin Laden's potential attack against nuclear facilities. Most assuredly, those reports came from a newspaper or from CNN not from the intelligence community. We are still in the infancy stage of determining how best to do this, but in the context of homeland security, if you're a fireman or policeman, you certainly do want and should expect relevant information and effective communication from your Federal Government.

As the concern about security abates, as inevitably it will in our society, networking the Federal Government with State and local government functions must be aggressively pursued. To effectively respond to threats to the homeland, government at every level is going to have to be networked.

A National Strategy that accounts for the primary missions of Federal agencies associated with Homeland Security: The national strategy must establish the framework to account for large gaps in missions that potentially stand in the way of unifying around the homeland security mission. Most agencies that are now focused on homeland security have other primary missions that will have to be accounted for. The Customs Service is a good example because its mission is as a revenue-generating agency, focused on goods and trade, not on security. Last year, the Customs Service collected in $23.5 billion in taxes, fees, and penalties, second only to the Internal Revenue Service in generating government income. The Coast Guard is another good example with non-homeland security missions associated with routine law enforcement, fisheries, and deep-water drug and political refugee interdiction.

A National Strategy that provides for private sector involvement: A good example of the complexity of initiating public-private cooperation can be seen in the containerized shipping industry. Approximately 7.5 million containers enter the United States each year. The Customs Service only inspects 2 percent. The contents of these containers originate with approximately 450,000 shippers globally. This represents an unworkable number, but there are steps that can be taken now to reduce our vulnerability. Recently more than 50 large corporations agreed to work with the government to ensure adequate security of goods entering the United States in exchange for faster passage through border checkpoints. An interesting statistic is that the contents of 60 percent of shipping containers entering the United States originate with just 1000 large shipping companies worldwide. This would seem to be a workable number where cooperation between government and the private sector could again make a difference and drastically reduce our overall vulnerability.

Much of the Nation's strength rests on its privately owned critical infrastructure, but the private sector does not just own and operate the Nation's critical infrastructure, the private sector owns a lot of the expertise that could improve the way in which government approaches the homeland security problem. The private sector does not just have interest in working with the government, the government absolutely has to have help from the private sector. The Y2K problem is a good example where the private sector did a much better job in understanding the problem and developing responses to it. Networking is an area that the private sector has mastered. In the National Security Council or Homeland Security Council, you won't find our Federal agencies networked in the way you would find similar functions networked in the private sector.

Developing public-private partnership is complicated by the need to protect sensitive information and the lack of information sharing and coordination between the numerous agencies of the Federal Government with responsibility for homeland se-

curity. The national strategy must be the vehicle for simplifying the communication and coordination problem within government—and between government and the private sector. The private sector must be included in the development of the strategy and the strategy must formalize the means to ensure private sector involvement in its implementation.

IV. Conclusion

Mr. Chairman, over the long term, in this new and very dangerous environment, government reform must be initiated to ensure unity of effort and clear lines of authority, responsibility and most importantly, accountability. In the absence of a comprehensive national homeland security strategy, there can be no clear understanding of the threat to be addressed or any real sense of priorities from which specific requirements will emerge. The strategy should be the vehicle that establishes the framework for every aspect of government to move forward together in a unified and coordinated way to fully address what is surely the most complex problem our government has ever had to face.

Mr. Chairman, the road ahead remains complex and dangerous with numerous challenges yet to be addressed. The Center for Strategic and International Studies is ready and willing to help.

Organizing effectively to secure the American homeland is essential to our country's prosperity and to the prosperity of our allies. We appreciate the Committee's leadership on this issue, and we look forward to helping in any way we can.

Chairman SCHUMER. Thank you, Dr. Anderson. I very much appreciate your testimony as well.

And finally, Dr. Light.

STATEMENT OF PAUL C. LIGHT, VICE PRESIDENT AND DIRECTOR, GOVERNMENTAL STUDIES, BROOKINGS INSTITUTION

Mr. LIGHT. It is nice to have the last word again on this issue.

As you know, the Governmental Affairs Committee is considering legislation to create both a Cabinet department and a statutory Office of Homeland Security.

Before I go into a brief summary of my statement, I should note that there already is a de facto national chief information officer. That individual is the deputy director of the Office of Management and Budget for management. That is a position that has been vacant for 16 months. There is no nominee currently pending before the United States Senate. There is no individual who has been announced for that position.

Last week, this Committee received testimony from the Webster Commission about streamlining and improving the FBI review process for appointees. We have over in the Governmental Affairs Committee now legislation co-authored by Senators Lieberman and Thompson that was favorably marked up earlier this session called the Presidential Appointments Improvement Act.

I cannot speak for those two Senators, obviously, but a friendly amendment to ask the FBI to accelerate and make less burdensome the review process for presidential appointees might improve the odds that we would actually get somebody into the position that you clearly have heard a case made for today.

My statement here basically argues that there is not necessarily too little information in the Federal Government today regarding potential threats, but possibly too much. Perfect hindsight suggests that government often has the information it needs to make decisions, but that it cannot sort it, integrate it, or interpret it. I think that historians 20 or 30 years from now will be making that argument regarding September 11th.

The Office of Homeland Security does not appear to have the power to break down the barriers and address the most serious problems facing those who desire to harm this country.

Interestingly enough, in my analysis of the Office of Homeland Security, it may be young, it may be new, it may be understaffed, but let me tell you, Senator, it is thick. The organization chart for this young office is one of the most complicated organization charts for a White House unit or for a departmental unit that I have seen in my career. I make a career of pointing at organization charts, and I have just never seen on what appears to have been designed to complexify the movement of knowledge.

I do not question Governor Ridge's sensibilities in putting together this organization chart. I just point out that it is a rather novel and complicated organization chart that may make the procurement, production, and integration of information more difficult than it needs to be.

My statement looks at seven components of an integrated information chain that the Office of Homeland Security might need. I talk about production of information, which the office does not do and does not have the power to do. I talk about the procurement of information. The office does not have the authority to order, purchase, or otherwise gain information that does not currently exist. It cannot order the study of a particular issue. It cannot analyze a particular body of information.

The word "coordinate" appears 33 times in the Executive Order establishing the office. The word "investigate" appears once. The word "analyze" appears not at all. The word "study" appears not at all.

The office does appear to have considerable authority to collect information, but as my colleagues have argued at Brookings and elsewhere, there is not enough staff or capability in the office right now to basically crunch that information into meaningful analysis. It does not have the power to assess the quality of information or the capability to assess the quality of information. It does not have the capability to assess trends, to do analysis. It absolutely does have the authority to disseminate information, but ironically—and this is an important issue for this Committee and for the Senate as a whole—the President's assistant for homeland security does not have one authority to disseminate information to the United States Congress. He may not disseminate information through formal hearing or testimony before the United States, and I think that is a weakness in the office, which can be easily remedied by making that position a Senate advise and consent position.

The director does have the power to classify information as Top Secret, but does not have the power to declassify information that he deems to be in the national interest to be declassified.

My recommendations in my testimony are, number one, to give the office a statutory base. That is the coin of the realm. You want to go toe-to-toe with these agencies, you have to have a statutory base which means Senate confirmation. You need additional staffing. You need the dollars and the authority to produce and procure information, and you need to be able to coordinate an information technology plan for the agencies of government.

I submit my testimony for the record and am open to any questions you may have.

[The prepared statement of Mr. Light follows:]

STATEMENT OF PAUL C. LIGHT, THE BROOKINGS INSTITUTION, WASHINGTON, D.C.

I am pleased to appear before the Subcommittee today to consider options for strengthening the Office of Homeland Security. I believe this Subcommittee is right on target in asking whether and how the office might improve the flow of information to and from key decisionmakers. Although there are many causes of the September 11 tragedy, none was so easily addressed as the failure to collect, interpret, and share information.

I believe the question of information sharing involves two discrete parts. First, is the Federal Government currently producing the right information? Second, is that information available to the right people at the right time?

The Immigration and Naturalization Service is a perfect case in point. It suffers from a dearth of high-quality information on potential threats to national security, and has serious vulnerabilities in making sure that high-quality information reaches the right people at the right time. Bluntly put, even if the agency were to discover a potential threat, it is not clear that the information would make it to key law enforcement and security officials in time to prevent a tragedy.

We know, for example, that the INS does not have the information technology to track visitors to the United States. The agency simply does not have the right information about who is entering the country under what conditions and for what purpose, nor does it know where current visitors might be located, or whether they have over-stayed their welcome. Although there is nothing the Office of Homeland Security can do at this point to better coordinate, share, or monitor information that does not exist, I believe there are ways that the office can better control the production of information through expanded authority.

We also know that the INS does not have the technology to share the information it does have with the right people at the right time. We know, for example, that information about the individuals involved in the September 11 attacks on New York City and Washington, D.C., did not make it to the right people at the right time in the Immigration and Naturalization Service and its contractors. Otherwise, one would be hard-pressed to explain last month's extraordinary news that ACS, Inc., had mailed visa notices on behalf of Mohamed Atta and Marwan Al-Shehhi. Although one can argue that there was no harm, and, therefore, no foul, the lack of communication up and down the INS hierarchy speaks to the extraordinary problems in sharing information in a timely fashion.

Deja Vu

The INS is hardly the only Federal agency with problems collecting and sharing the right information. Indeed, recent Federal history is replete with examples of breakdowns caused by either bad information or good information ignored, including the security problems at the Nation's nuclear weapons laboratories and the taxpayer abuse at the Internal Revenue Service. Looking back with perfect hindsight, we can now see the outlines of a remarkable information breakdown at the core of the September 11 attacks, not the least of which were bits and pieces of evidence from flight schools and simulation centers. As in so many similar cases, from Pearl Harbor to Vietnam, we are likely to discover that the Federal Government had significant information about the potential threat, but could not put the pieces together in time.

The fact is that the Federal Government, indeed most organizations, almost always have the information to prevent failure, but not the analysis or communication chains. That was the case in the 1980s with the HUD scandal and the savings & loan debacle, in the 1990s with espionage at the nuclear weapons labs and taxpayer abuse at the Internal Revenue Service, and the early 2000s with the INS. Sadly, I have made a living out of showing the problems associated with communication failures in the Federal Government. We see the same problems over and over and over again as information gets lost, distorted, mishandled, improperly classified, or misinterpreted up and down the ponderous Federal hierarchy. See the appendix of this testimony for a side-by-side confirmation of my conclusion.

Assessing the Case at Hand

Our task today is not to look back for culprits, but to look forward to solutions. Simply asked by the Subcommittee, should the Office of Homeland Security have more power? As I and my colleagues at the Brookings Institution have argued, the

answer is "yes." Much as one can credit Governor Ridge with substantial success in shaping the budgets of the agencies involved in homeland security, his office does not provide the levers that are essential for coordinating, let alone assuring the flow of high-quality information in real time. He should be congratulated for having made the best of a very difficult situation, but should be fully empowered to make sure that the Federal Government has the information it needs.

Unfortunately, I do not believe Governor Ridge has the authority to prevent communication failures in the future. Even a cursory review of the Office of Homeland Security organization chart confirms the problem. According to the latest available Yellow Book listing, the office is structured around an assortment of titles whose primary tasks focus more on outreach than information collection or analysis: (I have numbered the layers within the office using conventional nomenclature.)

1. Assistant to the President for Homeland Security (Ridge)
2. Deputy Assistant to the President and Deputy Director
3. Deputy Assistant to the President (Communications & Legislative Affairs)
4. Deputy Assistant to the President for Legislative Affairs
   Senior Associate Counsel to the President and General Counsel
5. Special Assistant and Senior Director for Information Integration and Chief Information Officer
   Special Assistant and Senior Director for Policy & Plans
6. Special Assistant and Executive Secretary
   Special Assistant for External Affairs
7. Protection & Prevention Senior Director
   Response & Recovery Senior Director
8. Special Assistant and Director of Communications
9. Special Assistant for External Affairs
   Special Assistant for Public Liaison
10. Assistant Director for Intergovernmental Affairs
11. Communication Strategy Director
12. Staff Assistant

Much as one might question the problems associated with 12 discrete layers in the office, and much as one might ask whether the special assistant for information integration and chief information officer is (1) placed high enough in the bureaucratic pecking order, and (2) has too many competitors for access, the more important question at hand is whether Governor Ridge and his team have the authority needed to assemble the information they need. The answer appears to be "no." At best, information collection and analysis is but one of many competing priorities in the Office of Homeland Security. At worst, it appears to reside in a single unit that has multiple responsibilities, not the least of which is ensuring that the office itself has adequate computer technology, which is the traditional concern of chief information officer posts across government. At a minimum, I would recommend splitting the information integration and chief information officer posts, while raising the former to the level of deputy assistant to the President.

An Inventory of Authority

More importantly, however, I worry that the office as currently constructed does not have the authority to implement an aggressive information collection, analysis, and dissemination strategy. Let me suggest the following problems facing the office today:

1. *Production.* The Office of Homeland Security does not have the authority to produce information that it deems essential to its planning process. Although it does have a talented, albeit small staff, the office does not have the internal capacity to investigate or study problems that Governor Ridge deems essential. To the extent words have meaning, "coordinate" appears 33 times in the President's Executive Order establishing the Office of Homeland Security, while the word "investigate" appears only once. "Study" and "analyze" do not appear at all.

2. *Procurement.* The Office of Homeland Security does not have the authority to order or purchase information, whether through private contractors such as the RAND Corporation, which has extraordinary capacity for conducting the kind of exploratory analysis that Governor Ridge might find particularly useful in anticipating potential threats, or through government intelligence agencies. Nor does the Office of Homeland Security have the dollars to make such purchases. If Governor Ridge wants a special analysis of trends across or within agency databases, one presumes he must ask.

3. *Collection.* The Office of Homeland Security appears to have adequate mechanisms for tapping into the Federal Government's vast inventory of information. The question is whether an office composed of a scant 100 or so individuals, many of whom are dedicated to prevention, outreach, legislative affairs, communications,

etc., can hope to swallow from the fire-hydrant of information that currently courses through government. I do not see, for example, the capacity to evaluate the quality of information flowing into the office, nor do I see the ability to reach down into agencies to demand the release of information that already exists. Even more importantly, I do not see the capacity needed to compel the release of information that agencies might or might not know they have.

4. *Quality.* I do not see firm evidence that the Office of Homeland Security has the internal capacity to assay the quality of information flowing from inside or outside government. At least for the time-being, the office must rely on its sources to validate information.

5. *Analysis and Interpretation.* The Office of Homeland Security does not appear to have adequate mechanisms for analyzing information. That might mean, for example, resolving disputes between different portraits of threats, or pulling strands of analysis together into a particular whole. Such analysis requires a much greater staffing complement than currently exists. By way of comparison, I would point the Subcommittee to the National Security Council staff, which contains a series of well-staffed directorates for monitoring international threats, as well as a well-developed administrative infrastructure. Although it is fair to argue that it has taken more than a half century to develop, the Nation does not have another 50 years to wait. This problem is particularly significant given the office's role in maintaining the Homeland Security Advisory System, which assigns threats on a green (low) to red (highest) level.

6. *Dissemination.* The Office of Homeland Security appears to have adequate capability for disseminating information about potential threats.

7. *Classification and Declassification.* Although the Office of Homeland Security has ample authority to classify information as "top secret," it does not have parallel authority to order the immediate declassification of information that it deems in the national interest.

Recommendations for Action

I do not believe statutory authority can solve all of these problems. However, it can improve the odds that the Office of Homeland Security can produce the right information at the right time. At a minimum, I strongly recommend that the office be given the authority, and budget, needed to produce and procure its own analysis. Some may argue that such analysis would merely duplicate already existing information. I would argue to the contrary. The Office of Homeland Security has a special obligation to examine information through a very broad lens and from a vantage point that no other agency of government has.

I also strongly recommend that the office be given enough staff to interpret, analyze, and assay the information that it currently receives, and to make recommendations to Congress and the President regarding improvements in the information system. That might mean, for example, that Congress would provide the funding for a minimum staff floor, or create a special information directorate within a new Office of Homeland Security. That might also mean that Congress would require the office to conduct an information audit of the Federal agencies it coordinates, and make recommendations regarding the technology investments needed to assure secure, high-quality information. Finally, I recommend that the director of Homeland Security be given limited authority to declassify information deemed in the public's interest.

These authorities will be wasted, however, if the current office or its statutory successor is allowed to thicken with needless bureaucracy. The thickening has already begun. Being lean and flat is not just a value that the President himself espoused in the 2000 Presidential campaign; it is also the sine qua non for effective information sharing. For whatever reason, the current Office of Homeland Security has already become one of the thickest units in the White House. That not only weakens communication within the office, it merely adds to the extraordinary thickening of other units of government. To the extent the President relies on Governor Ridge to stay in touch with the front-lines at the INS, for example, he is staring down an information chain with 30-35 links. That is more than the Nation can afford.

Chairman SCHUMER. Thank you again. I think all three of you really helped contribute.

Let me start off with one question. Our first panel gave a pretty sanguine view of how information sharing was going within the Justice Department. You could argue that that makes the argument all three of you have made in different ways that we ought

to do the same thing within the whole Federal Government, because we do have a new person here, Mr. Hitch, who has the power, which I did not know until this testimony, to order all the agencies to share information within Justice, and can tell the INS and FBI, et cetera, to coordinate.

First, do you think things are going as well within the Justice Department, based on your experience, as they say?

And second is the analogy that I am making: If it is good for within the Justice Department, which has traditionally had problems with information sharing, then it is probably good for the whole government as well.

Mr. Terwilliger.

Mr. TERWILLIGER. Senator Schumer, let me observe that I think it is no particular insight to say there is no issue more critical than information management to this effort, and there is no weakness that has traditionally been greater in government, particularly in the Justice Department and law enforcement, than information management. So the steps taken seem to be ones very much in the right direction.

I am not sure that I am in a position to know whether it is working or not, maybe no one is at this point.

Chairman SCHUMER. You have been aware of all the turf problems when you were there.

Mr. TERWILLIGER. Yes, painfully.

Chairman SCHUMER. And do you think that the advent of 9/11 and a new person, who seems a fairly capable fellow who has done this in the private sector and other places very well, would be enough?

Mr. TERWILLIGER. No. I think that they both will be important reasons for things to change, but there are systemic issues that will get in the way of accomplishing what Mr. Hitch and the Attorney General and others are setting out to do—how the government procures technology, how it designs it, how it uses it. All of those are systemic issues that giving someone license and authority are simply not going to be sufficient to solve.

The biggest problem, in my view—and I will just confine my remarks to the Justice Department for the time being—in information management is that every agency wants to own the solution. If it is not an idea that has been homegrown and developed by that agency, then largely it is not a good one. There is precious little attention to how the use of that information may affect the functions and responsibilities of other components.

Chairman SCHUMER. In the model that we have seen, doesn't Mr. Hitch have the ability to say, okay, even though this was developed by FBI, INS, you have to use that system.

Mr. TERWILLIGER. Yes, I hope so. And I guess I would, to quote another famous American, say: I trust his testimony, but I would verify that that will happen.

Chairman SCHUMER. Right.

Dr. Anderson or Dr. Light, either one?

Mr. ANDERSON. My perspective as an outside observer is that there is a far greater awareness clearly among those in government that this is important. I think that within departments, there has

been some progress made, but it is between departments where the problem still exists.

There is all kinds of great technology out there that will allow you to address this problem, but there is not any technology that is going to influence the willingness of people to contribute to input the system.

You can appoint an information czar, but I am not convinced that even though they may have the legal authority that it is going to make a lot of difference.

I think that this is truly a function of leadership. You have got to get the leaders involved in trying to change the cultures of their organizations such that they can work department to department and between multiple agencies of government that would have to try and solve this problem.

Chairman SCHUMER. Do you think an Office of Homeland Security with Cabinet authority, budget authority and statutory basis could do that?

Mr. ANDERSON. I think it would be a good start. I am convinced at this point that the strategy is going to point in that direction. I think that to the extent that you can reduce the number of agencies or at least consolidate a number of those agencies in one department, it is probably a step in the right direction. But a word of caution there relates to the primary missions of these agencies.

If you look at Customs, they are a revenue-generating agency, second only to Internal Revenue. So that function is going to have to be accounted for in any organizational structure or any organizational reform.

The Coast Guard has a deepwater mission. There are a lot of other missions non-homeland-security-related that are going to have to be accounted for.

That said, the most important concern at this point is homeland security. So you deal with that problem first, and then resolve the secondary tertiary missions after the fact.

Chairman SCHUMER. Dr. Light.

Mr. LIGHT. I have watched the chief information officer concept develop over the last 12, 14 years. The first CIO was created in the Department of Veterans' Affairs back in 1988.

It is a slender reed on which to build a policy for integrating information. These offices are staffed by talented individuals, but 80 percent of their expenditures now are contracted out, and they are primarily concerned with systems.

This augmentation of the CIO's office in Justice with a policy function is a novel departure from prevailing practice. We will just have to see how it works. I would rather see it as a higher level within the agency and combining both systems and policy.

Chairman SCHUMER. Each of you had sort of different recommendations, but similar and not as grand, I guess, as the Office of Homeland Security. There could be an addition to it, obviously.

Mr. Terwilliger is a chief counterintelligence officer at the White House, and I believe Dr. Light said let's build this deputy director for management who could help coordinate a lot of this. I take it both of you feel that that is necessary, but not sufficient.

Mr. TERWILLIGER. Yes, I think that is right. Just to be clear, I would not recommend putting the intelligence function for

counterterrorism in the White House. I would put it out somewhere in an agency that is dedicated to that task, whether it is an existing agency or whether it is—and I would frankly prefer to see a new agency dedicated to that function in one form or another. There is, frankly, a model among some of our allies for that type of thing.

I think we will quickly recognize, if we do not already, that what we are doing now is not enough.

Chairman SCHUMER. By the way, is there a model for a country that does this better? Obviously, we are probably the largest with the number of people, the amount of money spent, responsibilities.

Mr. TERWILLIGER. Yes.

Chairman SCHUMER. But is there a smaller country that does a better job of this that we should look at, on intelligence, information sharing particularly when it comes to intelligence.

Mr. TERWILLIGER. You put your finger on the biggest problem we have, Mr. Chairman, and that is just the size of the problem and the breadth of the information we have to deal with. But in terms of conceptual models, when you talk to the people who are really experts in this and the professionals, they point, as much as it may strike some as odd to say so, to some of our European allies such as France, who at times appear not to have been totally supportive of some of the things we are doing in counterterrorism, but when they had a problem with terrorists who were threatening to blow up their symbols of democracy, they empowered their domestic security agency—I have worked with them in my days at the Justice Department—they are very effective. And they created a small cadre of very special investigating magistrates, who are the equivalent of our prosecutors, to be totally focused on terrorism and gave them extraordinary investigative authority.

Chairman SCHUMER. Were they geographically—I mean, was one for Paris, one for Marseilles?

Mr. TERWILLIGER. That is a good question that I do not know the answer to. But the point is I think that the danger of giving these extraordinary powers to law enforcement in general is that they then become available for a lot of problems that have nothing to do with terrorism. Conversely, if that is where we talk about reposing the power, we may not give them the authority they need to get the job done out of that very concern.

Chairman SCHUMER. Dr. Light, I had asked you also about this deputy director for management, which is necessary, but I take it you would say hardly sufficient.

Mr. LIGHT. It's a pivot point to note that we have serious problems in the presidential appointments process. I have a colleague behind me who would be very disappointed if I did not make some segue here to argue for presidential appointee reform.

I am a strong supporter of putting a statutory base under the Office of Homeland Security. I think that is essential.

Chairman SCHUMER. One final question, and then I will turn to Jeff. Each of you has pointed out that even if we were to do that, you would still have many of these barriers and it would take a long time and you all have years of experience either doing this or studying it. And so let me go back to the question I asked I think it was the first panel.

What about this idea to make this—I understand that you need more than technology. But if you have a technological direction, a lot of the other things fall by the wayside. So what about this idea of a single computer, a supercomputer, that Ellison model that says all our intelligence information is shared on this one thing, and everybody—it is not their only computer, but that has all their intelligence. If you require them to input the information and then the selected agencies have access to it, it makes information sharing—it overcomes a lot of the cultural barriers, technological barriers, turf issues, et cetera.

So I think it is more than just a technology. In a sense, it is sort of a tool to overcome the age-old barriers that each of you has very aptly pointed out. There is a privacy issue, obviously, but I am not sure that is dispositive.

The final question is each of your views on that.

Mr. TERWILLIGER. I think that is a good vision. The answer probably is not—and I know you do not intend it to be as simple as you say, just technology or a computer.

This is a problem that is not new. This is just a different subject matter to which it applies. We had this problem when Senator Sessions and I were at the Justice Department with drug intelligence.

And our solution, one of which I frankly spilled a lot of blood internally within the Administration over, was to create a fusion intelligence center, to have a computer system where information from all the agencies that had drug-related intelligence would fuse. It has worked to a certain degree, but it only works as well as someone forces people to contribute to the knowledge base that is in that system. I think that the system without the authority—frankly, the authority of the President over it—that you must contribute this kind of information to that knowledge base, will not solve the problem. So I think it is going to take both.

Chairman SCHUMER. What if you had the authority?

Mr. TERWILLIGER. If you have the authority, yes, because we have to remember where we are trying to go here. We are trying to find out what our enemy is up to here and stop them before they do it. The ability to do that will follow naturally from having the information.

Chairman SCHUMER. Dr. Anderson.

Mr. ANDERSON. I agree completely. I would like to say, though, that there are no 100 percent solutions in this environment.

Chairman SCHUMER. In this area, we would settle for 50 percent.

Mr. ANDERSON. Senator, I think that is the most important point. We need to do what we can do now. If we can address 60 percent of the containers that are coming into the country, we need to do that. The airport analogy is a great one because any one of us goes to an airport, we are all treated the same way. But the bottom line is, through some simple identification means and methods, we could probably reduce that number to 30 or 40 percent. And how much better would we be in scrutinizing that percentage of the entire population? A lot better.

So we do what we can do now. And to the extent that we can get people to input a central system, we ought to do it, but I do not think we are going to get 100 percent willingness and ability, short of forcing agencies of government to contribute.

Chairman SCHUMER. Last word, Dr. Light.

Mr. LIGHT. It is kind of a "Field of Dreams" phenomenon, isn't it? I mean, if we build it, will it come? And the answer is that I think that if you build an integrated system and you put authority behind it, I think we will probably do better than 50 percent, less than 100 percent. It is part of a broad attack on this particular problem, which has an asymmetry to it. We do not know where the next attack will come from. All we can do is be prudent and use due diligence to respond.

So if it can be built and it does not cost every last penny in our coffers, I would say let's try.

Chairman SCHUMER. Jeff.

Senator SESSIONS. Thank you.

Chairman SCHUMER. I thank all of you.

Senator SESSIONS. It is very interesting and a great discussion.

The best example I know of, of really uniting behind a concept, was when your former Mayor, Rudy Giuliani, was Associate Attorney General, he declared that we did not want Federal agencies in Washington setting the policy of every one of the offices in America, that each region would meet and set their priorities. And it caused quite a stir, because the FBI thought they should decide what their priorities were. So did DEA, and so did Customs.

But because the President said, we are going to do it, and Rudy Giuliani's drive and vision, he just overcame the bureaucracy. And it just happened.

And it is still out there functioning. I do no think quite as well. I think the agencies have sort of stovepiped since then. But for a glorious time there of several years, there was real unity within Federal law enforcement.

If you create a new Cabinet position, there is just one more Cabinet position. That Cabinet position cannot order the Attorney General or the Secretary of Treasury or the Secretary of Transportation to do anything. It is ultimately the President.

So I do not think we should dismiss entirely what is happening now with Mr. Ridge, because I think that what the President essentially said was, "This needs a lot of time, a lot of personal attention. There are a lot of bureaucratic problems out there. I want to be personally engaged in it, but I cannot personally do everything, so I am choosing somebody I trust to be engaged in it, to advise me. All of this is an Executive Branch function, and they are to come to me and we will make sure that things happen."

The way I understand what Mr. Ridge has done and does do, is he meets with agencies where there is a dispute—like you used to do, George—within the Department of Justice, but he is doing it within the whole government.

He says, "Well, having heard all this, I think Treasury, you should give it up to Justice." And they say, "No, we are not going to do it. You do not have any legislative authority." And what does Mr. Ridge say? "Well, let's just go meet with the President, and we will talk about it." Well, then the agency heads say, "Well, maybe we need to settle this thing. We really do not want to go to the President, bickering over some jurisdictional matter." And things do happen that way.

So a good, strong leader, who has the personal confidence of the President, could even in some ways be more effective because he is known to speak directly to the President of the United States. If he is given one more Cabinet head, I am not sure that would have as much clout in this area.

It is a complex deal, and I can remember the battles over intelligence within the Department of Justice—just brutal sometimes.

I would say, you mentioned, Dr. Light, and I know Mr. Panetta did, and I am sorry I did not have time to question him, but there is a lot of power in the OMB, within the Administration. In other words, if an agency asked for money to start their intelligence system and another agency is asking for money to do theirs, and the President has to submit a budget, and he picks the one he wants. Could you explain the power of OMB and how that could be a vehicle for eliminating duplicity and creating some coherence in our government?

Mr. LIGHT. In theory, the budget requests move up from the bottom of that agency and eventually reach a decision point where somebody, a program associate deputy, would basically say, there is a conflict here, or we need to integrate.

I think where Governor Ridge has had his greatest influence has been affecting the movement of budget information regarding the homeland security function.

Currently within OMB, there is nobody per se who integrates across the various program associate program levels to say, okay, here is the homeland security issue. That goes all the way up to the Director's office, which would be Mitch Daniels, and one assumes that he looks at every budget request through the lens of what is the total for homeland security.

Senator SESSIONS. But I guess the point is, assuming you had it staffed properly, that is traditionally thought to be the spot where duplications in organizations get fixed. Is that right? Or at least it has that potential.

Mr. LIGHT. On information technology, there is no question that Congress has given OMB responsibility for integrating and modernizing our computer systems. No doubt about it whatsoever. We have the Office of Federal Procurement Policy within OMB, which has been responsible for streamlining the way we purchase technology. The deputy director for management is theoretically responsible for convening the council of CIOs from around government.

I mean, this all is supposed to happen within OMB. But you know, it is a moving process, and if you do not get the attention to it, and if you do not focus on it, we do not get the result we want.

Senator SESSIONS. Mr. Terwilliger, sometimes OMB does not catch it, or maybe it is below their radar screen. Do you remember the duplication between ATF and FBI over forensic analysis of firearms? To me, that was a classic unfortunate event when two Federal agencies were competing around the country, trying to get their system chosen throughout the country.

Mr. TERWILLIGER. That is true. And as you know, Senator Sessions, there have been a number of those. When the FBI was developing automated fingerprint identification, one of the Treasury

agencies started a program to do that. In fact, Attorney General Barr and I at one point tried to create a law enforcement technology council and budgetary function with the blessing of OMB. Every law enforcement agency in the government, including our own, objected to it.

But I think that those experiences have to be put in a proper perspective. What we are really grappling with here is that we have never had this particular issue before, at least since 1812. And if we had this problem at the beginning of the 19th Century, we would call the Army and ask them to go take care of it. That is not, for a number of reasons, a very good idea right now.

So what we are really talking about is, how do we deal with a pernicious, serious threat to the security of the homeland of the United States? The President has chosen to create a domestic analog to the NSC. But the NSC largely—I have sat at the table in the situation room of the deputies committee of the NSC—and the NSC largely has a policymaking function, and then the agencies at the table carry that policy out, and that policy carries the President's authority.

I think what we are talking about in terms of the tasks that involve homeland security, it does certainly involve policy, but it is much more than that, particularly when it comes to information management, consequences management, and preemption of attack.

Senator SESSIONS. Mr. Chairman, we tend to blame the Executive Branch, but a lot of these things are congressionally created. We have said, "Secret Service, you have this jurisdiction. You have this authority." "Coast Guard, you have this authority by law." So Mr. Ridge—or whoever is in charge of trying to work this—has got to utilize existing agencies, unless we intend to do the most monumental reorganization of agencies the government has ever seen, and maybe that is not a bad idea.

Chairman SCHUMER. Everyone talked about turf in the Executive Branch—something unheard of in the Congress.

[Laughter.]

Senator SESSIONS. Well-said.

So I mean probably the best way to do this thing is to make sure that the Border Patrol agent, the Customs agent on the docks, the DEA agent who may be monitoring an international smuggling organization, the FBI agent who is doing counterintelligence in organized crime and those kind of things, probably we are going to be stuck with this solution, making sure that they are moving relevant information promptly to the right places when it is uncovered in the course of their work, and perhaps giving each one of them some expanded additional duties with regard to homeland security, enhancing that as a priority of theirs.

So then how do you at the top fix that? Do you try to create a separate Cabinet agency that basically is going to be dealing with all the other Cabinet secretaries and their subordinate units? Or does the President try to have his personal coordinator to try to coordinate? Do you have any comments on that?

Mr. TERWILLIGER. Senator, if I may just make an observation? You have several times brought your perspective of how decisions here in Washington affect how the people we are depending on in

the street do their jobs. One of the things from talking to some of those people since 9/11 that I think is critically important for the Congress to bear in mind and deal with is, we have to give them the clear and unambiguous legal authority for what we ask them to do.

Right now, I think there are law enforcement agents and others out in the field doing things that they have been asked operationally to do that they are not sure they really have the authority to do, or at least there is uncertainty. That is not fair to them, and it is not very efficacious in the long term.

Senator SESSIONS. And that is our responsibility as Congress to give them that legislative authority.

All our agencies are limited, Mr. Chairman. They are given jurisdiction over certain kinds of crime and only those kinds of crimes. And sometimes that does impede their ability to reach their maximum effectiveness.

Mr. LIGHT. I suspect that what we are going to end up with a border control agency and a statutory adviser for Homeland Security. I suspect that is where this confluence of debate is heading, that we do not have the wisdom to put together a Cabinet department just yet, but there is this old saying that if it ain't broke, don't fix it, and then, if it ain't broke, don't break it.

Well, you have a couple of agencies under this Committee's jurisdiction that are pretty badly broken, and you are going to have to do something. The INS problems are going to lead inevitably towards reorganization. Where does that take us in terms of a border control agency? And on the other side, we want a strong policy adviser who is allowed to testify before Congress.

I do not know what the shape is going to be, but I would put money on that particular outcome sometime later this year.

Chairman SCHUMER. But we are not sure that would deal with the information sharing, which is, to me, at least, the most important one of them all.

Mr. LIGHT. And I think that you, the Subcommittee here, should be working on the tasking on this particular issue. It is a fundamentally important question that you are raising in this hearing, and it is one that is not being worked anywhere else in this conversation that I know of.

If you can come up with that supercomputer or you can come up with that answer, put it in a bill and get it through. Nobody is working this issue with diligence.

Chairman SCHUMER. Because we are all divided, too. We had Justice and all of their agencies, but there are lots of others.

Senator SESSIONS. And we have legislation. We have at least four or five bills now with different ideas about how to organize this thing. So there are a lot of different ideas out there.

Sooner or later, we have to be realistic and do something that makes a big step forward, which I believe we can do. I do not think that anybody would disagree that, if we focused on it, we can make a large improvement from our current status.

Mr. ANDERSON. I do not think this really, Senator, should be viewed in general terms any differently than the way we view national security. We have a number of different Cabinet secretaries with very clearly defined responsibilities, and departments with

very clearly defined functions. They coordinate through the National Security Council and there is a National Security Advisor. It would seem to me that we should have the equivalent on the homeland security side and at least one Cabinet secretary, who consolidates potentially the border responsibilities, which seem to be at this point our most critical vulnerability.

But it would seem in general, and certainly this is far more complex and involves far many more agencies, but the national security apparatus would probably be, in my view, a good starting point for the way to approach this problem organizationally going forward.

Chairman SCHUMER. Jeff has a few more questions. I have a 12 o'clock appointment, so I am just going to excuse myself, thank the witnesses, and let Jeff continue to chair the hearing and close it.

Senator SESSIONS. Thank you, Mr. Chairman, for your leadership.

Chairman SCHUMER. I really appreciate it. It was really excellent, and it is getting us thinking.

Senator SESSIONS. It is important for us to be thinking about this.

I am inclined to think the National Security Council adviser model may be the right approach, too, Mr. Anderson. In other words, this would be a person that answers directly to the President. It today coordinates international matters, and advises the President from the multiplicity of sources of information that come in. A good bit of information comes in outside of the State Department, so State should not be the only person advising the President on foreign policy issues. So you could do that for homeland security.

Would the three of you like to briefly just comment on that model as a potential? You already have, Mr. Anderson. Would the other two like to comment on that?

Mr. LIGHT. The analogy is often made between the Office of Homeland Security and the NSC. I think there are some areas where the analogy is appropriate, and other areas where it is not.

The Office of Homeland Security has a public face to it that the NSC and the National Security Advisor do not. Governor Ridge has a dissemination and a public awareness function, a coordination function, that is fairly significant, and I think leads us more towards thinking of him as we would the Director of OMB or the international trade representative or the drug czar. But I think that takes us a somewhat different direction.

Mr. TERWILLIGER. I think, Senator Sessions, that at least the President intended to mirror in many respects the NSC model and the NSC adviser's model in creating the current Office of Homeland Security and Governor Ridge's position. But because there is no one else to do a lot of the other things that go with the issue and the tasks of homeland security, I think that office has been inundated with responsibility that goes well beyond anything we would expect in the national security arena for the National Security Advisor to do.

So it may very well be that we will always need that kind of function, a domestic security adviser at the White House. The ques-

tion remains whether we need something else in addition to that. There are two ways to go about that.

Senator SESSIONS. Well, you could put those within existing agencies.

Mr. TERWILLIGER. Exactly. Or you can create some new agency, which would mean taking some functions from other agencies.

When I was Deputy Attorney General, I would attend the TREVI ministers conference, which is the G-7 nations international organization to deal with terrorism and immigration. And most of my counterparts at those meetings were from the ministry of the interior in the European nations, for example. Their chief legal officers do not function as our Attorney General does. They do not run the police. They do not handle internal security. That is in a separate ministry.

We have just evolved in a different way. It may be that, given time, I think—I am not advocating for or against this—it just may be that given time and maturity, that the idea of having someone of Governor Ridge's authority under presidential order as a domestic analog to the National Security Advisor may work.

The question that I have about that is whether we have the time to let that mature, given the threat that we are facing.

Senator SESSIONS. Dr. Light, just briefly, you mentioned the distinction between the National Security Advisor and the drug czar. Are you aware of their legislative powers and how they are different, and why one might be preferable to the other?

Mr. LIGHT. The drug czar, as well as the international trade rep, are subject to Senate confirmation, which I think is important. The drug czar has some certification authorities regarding budgets. I think if we look at the drug czar and say, you know, "Gee, how successful has that been in the war on drugs?" I am not sure we would all say that is the model. But you look at the international trade rep and the OMB Director and other Executive Office of the President's positions, and there is that legal basis for action.

I am reminded here that, you know, the Office of Homeland Security is currently responsible for the homeland security advisory system, which alerts the American public to the level of threat. But again, we are in a situation where the adviser himself cannot come before Congress to explain why it is that we are in one level of threat or another.

I agree with my colleague here that a lot of responsibilities have flowed into this office that have gone there because there is no place else to go, in a sense.

Senator SESSIONS. Any other thoughts on that subject?

Well, it is a difficult matter, how to organize this government. As a United States Attorney, you represent the United States Government, and I used to have a little phrase. It would say something like: "Here are the agencies; the United States of America is one. It can only speak with one voice."

But the agencies become so independent over the years that they think that they have a right to do policies contrary to another agency's policies and conflict with them and fight with them. But they have no authority to do that. They were created to be part of one government, and when you get to court, there is only one position the United States can take.

So it always has taught me a lesson that there is only one goal for our agencies, and that is to serve the United States' interest. And how we do it is very difficult.

I remember writing Associate Attorney General Rudy Giuliani a wonderful letter I spent days writing, telling him that he should merge not DEA with FBI, but merge ATF with DEA. ATF and DEA—that would be a perfect match. And he said "It cannot be done." I said "why?" And he said, "Well, that is Treasury and Justice. We cannot even merge people within Justice. How are we going to get the Secretary of Treasury's agency to merge with Justice?" That was a lesson for me in how a bureaucracy works and how difficult it is to overcome.

Thank you very much for your insight. We have to continue to wrestle with this. I thank Senator Schumer for his leadership in calling this hearing. I know, having suffered as he did in New York—the pain of all of that—he feels a particularly strong mission to make sure that we do everything we can to make sure that does not happen again.

If there is nothing else, we will stand adjourned.

[Whereupon, at 12:18 p.m., the hearing was adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

STATEMENT OF SENATOR PATRICK LEAHY,
U.S. SENATOR FROM THE STATE OF VERMONT

Today the Senate Judiciary Subcommittee on Administrative Oversight and Courts holds an important hearing on the sharing of information and the power of the Office of Homeland Security, and I thank Senator Schumer for his focused attention on this issue. The Judiciary Committee has a critical oversight responsibility to ensure that counterterrorism information is properly shared among Federal Government agencies and that homeland security functions are managed effectively. The apparent mission and authority of the Office of Homeland Security relate extensively and directly to the Department of Justice and to Federal law enforcement and border control operations for which the Judiciary Committee has legislative and oversight jurisdiction. Strong leadership is needed to bring together the necessary organizations, both within and outside the Justice Department, and design procedures, with adequate safeguards against abuse, for sharing information across agencies that have different missions, information technologies, policies and cultures.

Policies for sharing counterterrorism information were among the most controversial issues during congressional consideration of the USA PATRIOT Act last year. There was wide agreement on the principle that unnecessary barriers to the sharing of intelligence and law enforcement information on international terrorism should be removed. At the same time, there was great concern that sensitive information, such as information derived from grand juries or surreptitious wiretaps, should not be shared without close supervision by Federal judges who have traditionally played an important role in overseeing the grand jury and electronic surveillance process. Another controversial issue was the scope of information sharing that would be permitted for purposes beyond counterterrorism.

As enacted, in Section 203, the USA PATRIOT Act reduced but did not completely eliminate the role of the courts in the sharing of grand jury information. The Act also provided for the sharing of foreign intelligence information from criminal investigations for national security purposes beyond counterterrorism, but definitions and procedural safeguards were included in an effort to minimize the dissemination of "foreign intelligence" about lawful activities of United States persons and domestic groups acquired incidentally in criminal investigations. The new law, in Section 905, also requires law enforcement agencies to notify the Intelligence Community when a criminal investigation reveals information of foreign intelligence value.

I noted upon passage of the USA PATRIOT Act that the Judiciary Committee has a responsibility to exercise careful and continuing oversight with respect to implementation of the information sharing provisions of the USA PATRIOT Act. On April 11, 2002, the Attorney General made an announcement on information sharing that directed "the Assistant Attorney General for Legal Policy, in consultation with the Justice Department's Criminal Division, to draft for consideration and promulgation, procedures, guidelines, and regulations to implement Sections 203 and 905 of the USA PATRIOT Act in a manner that makes consistent and effective the standards for sharing of information, including sensitive or legally restricted information, with other Federal agencies." The Attorney General stated, "Those standards should be directed toward, consistent with law, the dissemination of all relevant information to Federal officials who need such information in order to prevent and disrupt terrorist activity and other activities affecting our national security. At the same time, the procedures, guidelines, and regulations should seek to ensure that shared information is not misused for unauthorized purposes, disclosed to unauthorized personnel, or otherwise handled in a manner that jeopardizes the rights of U.S. persons, and that its use does not unnecessarily affect criminal investigations and prosecutions. The standards adopted will govern the coordination of information directed by this memorandum, and [sic] well as other voluntary or mandated sharing of criminal investigative information."

I welcome the Attorney General's assignment of responsibility for the drafting of these information sharing procedures, and I look forward to consultation by the Department of Justice with this Committee before rules are promulgated on such an important matter.

Information sharing involves technology and cultural issues as well as policy considerations. Over the past month the full Judiciary Committee has held two hearings on the FBI that highlighted the weaknesses in the Bureau's information technology and security. On March 21, 2002, the Justice Department Inspector General described serious information management problems that contributed to the delay in producing documents in the Oklahoma City bombing case. On April 9, 2002, Judge Webster discussed his Commission's report findings on information security

flaws that helped make it possible for FBI Agent Robert Hanssen to commit espionage undetected. At both hearings, senior FBI officials described the challenges they face in designing and deploying new information technologies and management tools to meet the operational and security needs of the FBI.

Today's hearing reminds us that the FBI cannot function in isolation from the rest of the Justice Department or from other Federal agencies. Other Justice Department components such as the Immigration and Naturalization Service, the Criminal Division, the Office of Intelligence Policy and Review, and the new Foreign Terrorist Tracking Task Force share responsibility for counterterrorism and homeland security and are at different stages in their development and use of information technologies. The appointment of Mr. Vance Hitch as new Chief Information Officer for the Department of Justice is a welcome opportunity for leadership that integrates the work of Departmental components internally and with other agencies. I encourage all elements of the Justice Department to work closely with Mr. Hitch to achieve as much collaboration as possible in the design of technologies and information sharing policies that achieve shared national counterterrorism and homeland security objectives.

Many of those national objectives and required actions have been set out by the President in a series of policy directives based on the advice of Governor Ridge, with the support of the staff of the Homeland Security Office. Presidential decisions on homeland security are coordinated through interagency bodies chaired by Governor Ridge and his staff. Several witnesses today will testify as to the advantages and disadvantages of various legislative proposals to enhance or supplement the limited powers that Governor Ridge and his office currently have under Presidential directives.

Whatever may be the legislative route, however, it is important to stress that the Department of Justice and law enforcement agencies generally have the principal domestic role in the operational implementation of the President's counterterrorism and homeland security policies. If any new Senate-confirmed positions are established to lead counterterrorism or homeland security organizations that directly and substantially affect Federal law enforcement, either in the White House office or in a new department or agency, the Judiciary Committee has the duty to ensure that the nominees are qualified to perform the functions of their office and to oversee their performance. In any event, this Committee, both through the work of the full Committee and the capable leadership of its subcommittee chairmen, will continue to monitor and engage in constructive and productive dialog with the Administration and Justice Department in this important work.

DEPARTMENT OF JUSTICE,
Washington, DC., April 26, 2002.

HON. CHARLES SCHUMER, *Chairman,*
Subcommittee on Administrative Oversight and the Courts,
Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: I am writing to clarify two statements that were made concerning the admission of Mohammed Atta and the issuance of Forms I-20 to Atta and Marwan Al-Shehhi during opening remarks at the April 17, 2002 hearing of the Senate Judiciary Committee, Subcommittee on Administrative Oversight and the Courts. I ask that you enter this letter into the hearing record.

In your opening statement, you said that, "since September 11, 2001 every local, State, and Federal Government agency has been scrambling to repair the holes in our homeland defense," and cited "sending student visas to known terrorists" as an example. On March 19, 2002, before the House Committee on the Judiciary, Subcommittee on Immigration and Claims, Commissioner Ziglar testified that, contrary to some reports, the Immigration and Naturalization Service (INS) did not recently approve the applications for Atta and Al-Shehhi to change their non-immigrant status. Adjudication of Atta's change of status application took place on July 17, 2001, and adjudication of Al-Shehhi's change of status application took place on August 9, 2001. What Huffman Aviation International School received on March 11, 2002, were file copies of paperwork originally prepared on behalf of Atta and Al-Shehhi. No new visas were issued and no new decisions were reflected in the documents sent to them.

It has been acknowledged that prior INS procedures and contract terms for data entry and the mailing of student approvals were not effective or desirable—both have changed. Commissioner Ziglar has ordered that student notifications (I-20s) be mailed directly to the schools at the time of adjudication. In addition, INS proce-

dures and the related contract have been modified to ensure that schools are promptly notified when a student enters the United States at a port-of-entry.

You also summarized your perception of the information-sharing problem by quoting Larry Ellison of Oracle, who said that, "We knew that Mohammed Atta was wanted. We just didn't check the right database when he came into the country." As the Commissioner has testified, Atta was not the subject of a lookout or watch list at any time that he was admitted into the United States. Again, let me emphasize that the INS had no intelligence information that Atta was a potential terrorist.

Thank you for the opportunity to explain this information to you. Please contact me if you have additional questions or concerns about this or any other immigration-related matter.

Sincerely,

JOSEPH KARPINSKI,
Director, Congressional Relations and Public Affairs,

○