IMPROVEMENTS TO DEPARTMENT OF HOMELAND SECURITY INFORMATION SHARING CAPABILITIES—VERTICAL AND HORIZONTAL INTELLIGENCE

HEARING

OF THE

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERROSIM

BEFORE THE

SELECT COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JULY 24, 2003

Serial No. 108–21

Printed for the use of the Select Committee on Homeland Security

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

98–599 PDF WASHINGTON : 2005

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

SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, Chairman

JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
DON YOUNG, Alaska
F. JAMES SENSENBRENNER, JR., Wisconsin
W.J. (BILLY) TAUZIN, Louisiana
DAVID DREIER, California
DUNCAN HUNTER, California
HAROLD ROGERS, Kentucky
SHERWOOD BOEHLERT, New York
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PORTER J. GOSS, Florida
DAVE CAMP, Michigan
LINCOLN DIAZ-BALART, Florida
BOB GOODLATTE, Virginia
ERNEST J. ISTOOK, JR., Oklahoma
PETER T. KING, New York
JOHN LINDER, Georgia
JOHN B. SHADEGG, Arizona
MARK E. SOUDER, Indiana
MAC THORNBERRY, Texas
JIM GIBBONS, Nevada
KAY GRANGER, Texas
PETE SESSIONS, Texas
JOHN E. SWEENEY, New York

JIM TURNER, Texas, Ranking Member
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
KAREN MCCARTHY, Missouri
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
CHARLES GONZALEZ, Texas
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

JOHN GANNON, *Chief of Staff*
UTTAM DHILLON, *Chief Counsel and Deputy Staff Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

JIM GIBBONS, Nevada, Chairman

JOHN SWEENEY, New York, Vice Chairman
JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
HAROLD ROGERS, Kentucky
CHRISTOPHER SHAYS, Connecticut
LAMAR SMITH, Texas
PORTER GOSS, Florida
PETER KING, New York
JOHN LINDER, Georgia
JOHN SHADEGG, Arizona
MAC THORNBERRY, Texas
CHRISTOPHER COX, California, *ex officio*

KAREN MCCARTHY, Missouri
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
JIM TURNER, Texas, *ex officio*

CONTENTS

APPENDIX

QUESTIONS AND RESPONSES FOR THE RECORD

IMPROVEMENTS TO DEPARTMENT OF HOMELAND SECURITY INFORMATION SHARING CAPABILITIES VERTICAL AND HORIZONTAL INTELLIGENCE COMMUNICATIONS

Thursday, July 24, 2003

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INTELLIGENCE
AND COUNTERTERRORISM,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:10 p.m., in Room 2318, Rayburn House Office Building, Hon. Jim Gibbons [chairman of the subcommittee] presiding.

Present: Representatives Gibbons, Sweeney, Dunn, Cox (ex officio), McCarthy, Langevin, Markey, Lowey, Meek and Turner (ex officio).

Mr. GIBBONS. The House Subcommittee on Intelligence and Counterterrorism for the House Select Committee on Homeland Security will come to order.

I would like to begin by welcoming everybody here to our hearing today. We are going to start, and hopefully my colleague and friend Karen McCarthy from Missouri will be here shortly for our statement as well, and what I will do is begin my statement and then allow for Ms. McCarthy to enter her statement. Hopefully she'll be here by then and then we will open it up for other members of panel statement and then we will turn to our witnesses.

This looks like it is going to be a great hearing for us, very interesting panel we have before us today, and we are all looking forward to the information we are going to receive.

Let me begin by saying that since September the 11, 2001, terrorist attacks, Congress has focused on the performance of the Intelligence Community and whether intelligence and other information are effectively shared to prevent or respond to a terrorist attack.

Today governments at all levels recognize that they have a greater role to play in protecting the Nation from terrorist attacks, and to achieve this collective goal, homeland security stakeholders must effectively work together to strengthen the process by which critical information can be shared, analyzed, integrated and disseminated to help prevent or minimize terrorist activities.

The success of a homeland security strategy relies on the ability of all levels of government to communicate and cooperate effec-

tively with one another. Activities that are hampered by organizational fragmentation, technology impediments or ineffective collaboration blunt the Nation's collective efforts in this matter.

As it is with so many other homeland security areas, it is also the case for intelligence and information sharing that there are many stakeholders who must work together to achieve common goals. Effective analysis, integration and dissemination of intelligence and other information critical to homeland security requires the cooperative involvement of the Department of Homeland Security, the Central Intelligence Agency, the Federal Bureau of Investigation and a myriad of other agencies.

State and local governments have critical roles to play as well. Information is shared—is already being shared between and among numerous government agencies, information sharing practices benefit critical infrastructure protection by establishing trust relationships with a wide variety of Federal and nonFederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidences, to develop standards and agreements on how information will be used and protected. It also establishes effective and appropriate secure communication mechanisms and finally takes steps to ensure that sensitive information is not inappropriately disseminated, which may require a statutory change in some cases.

Clearly, these practices are applicable to intelligence and information sharing in the broadest sense. To optimize such an information sharing network, it is important to have a strong strategic planning framework and a supporting policy structure. The national homeland security strategy describes a number of incentives to better develop opportunities for leveraging information sharing among stakeholders, including integrated information sharing across the Federal Government, integrated information sharing across State and local governments, improved public safety emergency communication and reliable public health information and communications, all of which needs to be shared both horizontally and vertically.

Improvements in efficiency and effectiveness are rapidly occurring and are expected to continue for the long term, but there are costs and requirements as the new department faces communications, human capital, information technology and other integration challenges.

All of these changes of course will take time to fully implement. Today we focus on how effective the Department of Homeland Security is in information sharing, both vertically and horizontally. I would like to welcome the following witnesses from the Department of Homeland Security, acting Assistant Secretary for Information Analysis, Mr. William Parrish. From the Central Intelligence Agency, deputy executive director Philip Lago. From the Federal Bureau of Investigation, assistant director, Office of Intelligence Steven McCraw. From the State of New York, senior adviser to the governor on counterterrorism, James Kallstrom, which I will turn for further introduction to my cochairman here in a minute. And from the State of Virginia, senior adviser to the governor for commonwealth preparedness George Foresman. And from Maricopa, Arizona, preparedness planning and training manager Darin Daniels.

That looks exactly like the number of people I have in front of me, and I will turn now to the vice chairman of the subcommittee, Mr. Sweeney from New York, for any comments he may have and an introduction of his special guest.

[The statement of Mr. Gibbons follows:]

PREPARED STATEMENT OF THE HONORABLE JIM GIBBONS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEVADA

Since the September 11, 2001, terrorist attacks, Congress has focused on the performance of the intelligence community and whether intelligence and other information are effectively shared to prevent or respond to a terrorist attack.

Today, governments at all levels, recognize that they have a greater role to play in protecting the nation from terrorist attacks. To achieve this collective goal, homeland security stakeholders must effectively work together to strengthen the process by which critical information can be shared, analyzed, integrated and disseminated to help prevent or minimize terrorist activities.

The success of a homeland security strategy relies on the ability of all levels of government to communicate and cooperate effectively with one another. Activities that are hampered by organizational fragmentation, technological impediments, or ineffective collaboration blunt the nation's collective efforts.

As it is with so many other homeland security areas, it is also the case for intelligence and information sharing that there are many stakeholders who must work together to achieve common goals. Effective analysis, integration, and dissemination of intelligence and other information critical to homeland security require the cooperative involvement of the Department of Homeland Security, the Central Intelligence Agency, the Federal Bureau of Investigation, and a myriad of other agencies. State and local governments have critical roles to play. Information is already being shared between and among numerous government organizations.

Information sharing practices benefit critical infrastructure protection by:

- Establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;
- Developing standards and agreements on how information will be used and protected;
- Establishing effective and appropriately secure communications mechanisms; and
- Taking steps to ensure that sensitive information is not inappropriately disseminated, which may require statutory change.

Clearly, these practices are applicable to intelligence and information sharing in the broadest sense.

To optimize, such a information sharing network, it is important to have a strong, strategic planning framework and a supporting policy structure.

The national homeland security strategy describes a number of initiatives to better develop opportunities for leveraging information sharing among stakeholders, including:

- Integrated information sharing across the federal government.
- Integrated information sharing across state and local governments.
- Improved public safety emergency communications.
- Reliable public health information and communications.

Improvements in efficiency and effectiveness are rapidly occurring and are expected to continue for the long term, but there are costs and requirements, as the new department faces communications, human capital, information technology, and other integrationchallenges.

All of these changes of course, will take time to fully implement. Today we focus on how effective the Department of Homeland Security is in information sharing, both vertically and horizontally.

Mr. SWEENEY. Thank you, Mr. Chairman. Let me first say that—congratulate you on your leadership and thank you for your leadership in putting together this fine panel and say that in a year and a half's time, I have been, in one form or the other, whether it is the appropriations process or the authorization process, participating in a variety of hearings and oversights into the questions of homeland security, the questions of intelligence gathering and

counterterrorism, the linkages, the connecting of the dots that needs to happen, and I don't think I have ever been as excited about a panel as I am about this one, because I think that this panel and opportunity we have here today is really to do some constructive planning forward by virtue of the testimony that each of you have already submitted and that is all be submitting.

I am going to use my statement to introduce a friend and a fellow New Yorker and someone that we are very proud of, and I am particularly proud that he is here, because Jim Kallstrom is a model for the country to help us win the war on terrorism. He served in the Marine Corps. He has had a distinguished career at the FBI and was stationed in New York on three tours in 1971, 1976 to 1990, 1993 to 1997, including a special agent in charge and assistant director in charge of the largest bureau in the country, and including in that, overseeing the operations of a Joint Terrorism Task Force in one of the most critical areas of this Nation.

He has worked in the private sector as a senior vice president for security and management, committee member of the MBNA of America, and this is the part that I am most particularly proud of Jim Kallstrom. He was asked by Governor Pataki to be New York's first director of the Office of Public Security. He has left his private sector responsibilities and dedicated himself once again to public service. He is still serving his State and his country as a senior adviser for counterterrorism to the governor, and most importantly, he was ahead of the curve on the terrorist threat and knows from the inside what is needed to strengthen the intelligence and information sharing, and he will share with us today his realistic initiatives that I believe the country should accept and I think this is a good—as is the case with each of you, this is a good opportunity to start down a very constructive path, and I thank you.

Mr. GIBBONS. Thank you very much, Mr. Sweeney, and let me turn to the vice chairman of the full committee, Jennifer Dunn from Washington, if she has any remarks or opening statement.

Ms. DUNN. Thank you very much, Mr. Chairman. While I too am looking forward to your testimony, we have heard Mr. Parrish most recently, I think. He gave excellent testimony and answers, and today is a chance for us to investigate how we communicate all this information that you all have access to.

Unfortunately, we are going to be interrupted by a series of eight votes, and so don't know how the chairman is going to handle that, but we will have to leave you hanging for a while. Please understand it is not our choice. It is the last couple of days of our session, and a lot is being accomplished in these days. A lot of it I think is going to be helpful to us if we get our appropriations right and make sure that homeland security is funded to the degree it should be.

Thanks for being with us.

Mr. GIBBONS. Thank you very much, Ms. dunn, and I will turn to the ranking member of the full committee, Mr. Turner of Texas, for any remarks he may have, opening remarks.

Mr. TURNER. Thank you, Mr. Chairman. I will try to be brief, because I do know we have votes. In the nearly two years that have expired since September 11th, I think we have identified a number of things that we all can agree we must do to protect our home-

land, but it seems at the heart of the effort has to be an improved effort to share information about the terrorist threat. Our committee has had a lot of hearings on this particular subject, and it seems to me that we could do a lot better job than we are doing defining our responsibilities and determining who it is at the Federal level that our State and local law enforcement and other officials, as well as the private sector, is supposed to be communicating with, whether providing information up the chain or receiving information back from the Federal Government.

So I am pleased today, Mr. Chairman, that we have on this panel officials from three different States who can talk to us about the information flow issue and how we can improve it. It seems to me that there is some confusion here that we ought to be able to easily clear up. I have no doubt that everyone involved at the State, Federal and local level has good intentions, but I think it is our responsibility as a committee to be sure that we ask the right questions and help you accomplish the tasks that I know each of you are jointly committed to achieving for us. So thank you, Mr. Chairman.

Mr. GIBBONS. Thank you very much, Mr. Turner.

Mr. GIBBONS. And Mr. Meek of Florida for any opening remarks he may have.

Mr. MEEK. Thank you, Mr. Chairman, and it will definitely be brief. I am excited about being here and getting an opportunity to hear all of your perspectives as it relates to intelligence. As you know, the great debate here on the Hill and in Washington is good intelligence, what is good and what is bad. I am hoping as we go through that struggle of finding out what is good and bad, that it doesn't jeopardize the security of the homeland, and State, Federal, me being a creature from the State Legislature in Florida myself, being able to share information, being a past law enforcement person myself, is sometimes very difficult as it relates to the different entities and agencies; but I am interested to hear the camaraderie that you have now, and hopefully the camaraderie that you will have in the future in the times of doing a good job and being able to seek out and find out and flush out individuals that are going to harm the homeland.

Thank you so very much, Mr. Chairman. I look forward after our series of eight votes to hear from our witnesses.

Mr. GIBBONS. Thank you very much, Mr. Meek. And to our witnesses, first of all, let me extend the apology of the subcommittee, because as you realize, the series of votes that are being called call us away from our duty here, and all of us are here to hear your testimony, and we know that this is going to inconvenience you by delaying your ability to communicate with our panel. I want to advise the committee here we have a series of eight votes. There is about 8 minutes remaining or 7 minutes remaining on the first vote followed by seven 5-minute votes. So as we can see, that is about—it is going to be about 40-some minutes, 45 minutes from now before we can get back here. So I would like to apologize once again and just recess the committee until we return from this vote. And we ask for your patience and your indulgence in the process here today, and we will be right back. Thank you very much.

[Recess.]

Mr. GIBBONS. The subcommittee will come back to order and first again let me apologize to our witnesses. There were three dilatory motions that were held that cost an additional 15 minutes per vote, and there were three of them. So it took an extra 45 minutes, and I do apologize for that.

PREPARED STATEMENT OF THE HONORABLE CHRISTOPHER COX, CHAIRMAN, SELECT COMMITTEE ON HOMELAND SECURITY

Good afternoon. I join Chairman Gibbons and Ranking Member McCarthy in welcoming our witnesses this afternoon to what should be a significant and informative discussion. Our topic today—"Improvements to DHS Information Sharing Capabilities—Vertical and Horizontal Intelligence Communications"—has a variety of dimensions—and could be no more timely than to fall on the very day the intelligence committees have released their joint report on the 9/11 attacks. [Our own committee looks forward to exploring aspects of that topic in a hearing later this year.]

We are, today, first talking about information sharing. If it is true that, as the tragedy of the 9/11 attacks teaches, information—good intelligence—is the lifeblood of homeland security, then it is also true that information must move, must circulate. Sadly, that hasn't always happened. An article in this morning's New York Times states that the 9/11 investigation found that "key National Security Agency communications intercepts never were circulated." We must, today, talk about the timely sharing of all relevant information—about where it goes and how it gets there.

The purpose of today's hearing is to look forward. We want to ensure that key information, regardless of its origin, now can and will get to the right place at the right time. We are here to probe, not to politicize; to point the way, not to point fingers.

We are focusing on the Department of Homeland Security and its capabilities—both human and technical. The Department is the very core of the solution to the 9/11 information sharing problem. It is the tool Congress and the President devised soon after the 9/11 attacks in order to make absolutely certain that all information that might shed light on terrorist capabilities, intentions, plans, and activities is comprehensively analyzed and moves in the ways and to the places it must go, if we are to frustrate the intentions of those who seek to mount the next massive terrorist attack. The Department—in particular, its Information Analysis and Infrastructure Protection directorate—must, in short, succeed. And, on behalf of the President and the Congress, this committee will do everything in its power to make sure that it does.

I will say again: What we don't know empowers our enemies—and what we do know will help defeat them. In this new war—the ongoing battle for our future—knowledge is the very essence of power. If information doesn't move, people may die—it's that simple—that's the lesson of 9/11. We simply must get key information to those who need it most, and we cannot be satisfied with inefficiency or delay. What must happen must be made to happen.

We in the Congress and on this committee will also do our part. We will insist on breaking down barriers, on revising the ill-fitting regulations of the past so as to enable, rather than impede, the flow of information. Our ability to defend the American people, our homeland and interests, our economy and way of life depend on it. We have learned the lesson of 9/11. We will insist on effective information sharing. There is no acceptable alternative.

Let me be clear. In this new world—in this great battle to protect our people, homeland, and way of life—we cannot tolerate parochialism. We cannot allow the information taxpayer dollars have bought to be held by Government agency collectors as their exclusive property, protected behind a wall of antique regulations. All the information we have must be used to protect us all. The President recognized that long since, and we in the Congress have acted upon it in passing the Homeland Security Act and the USA-PATRIOT Act. Barriers are coming down—but stovepiped cultures and proprietary habits die far harder.

Today's witnesses represent both ends of a new spectrum, a new two-way information sharing partnership in which federal agencies that collect and provide information—through the new Department—to their new state and local government customers also wait eagerly to receive the information those same customers provide to them.

In this new war, federal, state and local officials are equal players. We must overcome the notion that the federal Government is the source of everything worth knowing—federal agencies must learn to listen. State and local governments, as

well as businesses may also be sources of key information. That, of course, makes sense, since they are where the action is, out where the rubber hits the road—as they will always be. Federal government agencies must support them. State, local, and private sector officials are now among the Intelligence Community's key customers—and each federal agency represented here today must learn to serve them well—largely through the Department of Homeland Security and the FBI. Where homeland security is concerned, it is not an act of largesse for the federal government to share threat-related information with state and local officials; it is essential—and the Homeland Security Act requires it.

We must also discard the common assumption that the most important information is classified—because in this new world, it may not be. The long-haul trucker in the small hours of the night may be the only one who sees the critical, anomalous act that indicates a possible terrorist attack—and we must have a system to ensure that what that trucker sees moves upstream quickly and reliably to the local, state, and federal government officials for whom it may be the critical, missing piece of a complex puzzle. Information sharing is not, in short, some grand gesture of noblesse oblige by a privileged coterie of federal agencies. To indulge the assumption that the federal Government—including CIA and FBI—has collected, and therefore knows, all that is most worth knowing at any given time is dangerous paternalism. But where state and local officials—including our "first responders" and law enforcement officers—do need access to classified information in order to protect us, they must have it—period. We must speed the clumsy clearance processes that keep them from the information that they need.

Each of today's federal government witnesses represents a member agency of the Intelligence Community. Each is involved in the federal government's effort to implement the Homeland Security Act. It was, in fact, last October, testifying before joint intelligence committees during their investigation into the 9/11 attacks, that the Director of Central Intelligence expressed the critical new commitment we stress today. He said:

> "We must move information in ways and to places it has never before had to move. . . We need to improve our multiple communications links—both within the Intelligence Community and now in the Homeland Security community. . . . Now, more than ever before, we need to make sure our customers get from us exactly what they need—which generally means exactly what they want—fast and free of unnecessary restrictions."

He was right. And we need to make sure that the implications of that statement are well understood. Because the implications of full commitment to information sharing in the homeland security context—the kind of commitment Congress intended and the Homeland Security Act requires—are enormous. It may even mean that an agency must, to protect the American people from attack, "lose control of" the information it originates—for example, in a networked environment where each recipient of a piece of information can, in turn, augment it—as the Markle Foundation suggested in a report last year.

The good news is that we're not starting from scratch. In early March, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence took a major step towards implementing the information sharing requirements of the Homeland Security Act. They signed a Memorandum of Understanding binding all Intelligence Community and federal law enforcement agencies, as well as the disparate entities that comprise the Department of Homeland Security. They didn't blink; they knew the stakes. They stated that:

> "Providing all timely and relevant [homeland security-related information] to those who have a need-to-know it in order to assist them in meeting their homeland security-related responsibilities is fundamental to the success of the Department and [to] all other efforts to ensure the security of the homeland from terrorist attack. Delay in providing such information risks frustrating efforts to meet these critical responsibilities and could result in preventable attacks against U.S. persons or interests failing to be preempted, prevented, or disrupted." [MOU at sec. 3(h)]

The information sharing MOU commits intelligence, law enforcement, and homeland security agencies alike to certain core principles and specific actions to implement the Homeland Security Act. It provides, for example, that those entities must generally disclose homeland security-related information—and intelligence is just relevant information—"free of any originator controls or information use restrictions." {3(k)] It says that providing homeland security-related information to one organization does not discharge or diminish the originating agency's obligation to share that same information with any other entity that has responsibilities for protecting the homeland. {3(m)]

The MOU goes on to say that "homeland-security related analytic efforts. . . must be informed by the most comprehensive, accurate, and timely information available, regardless of its nature and source," and it recognizes that "the Federal government must, to the greatest extent possible, speak with one voice to state and local officials, private industry, and the public, in order to prevent confusion, mixed signals, and, potentially, dangerous operational conflicts." {4(b)] It requires that classified homeland security-related information "reaches DHS promptly with accompanying high-content 'tear lines' suitable for onward passage at an unclassified level." {6(a)(i)]

And the MOU states that if this new mission requires "more expansive" information sharing than existing departmental policies and procedures do, then the MOU's more expansive information sharing mandates will prevail. These are new standards for our new, post-9/11, reality. They recognize that the irreducible minimum any government owes its citizens is to protect them—that homeland security is now everyone's number-one priority.

To prevent the unthinkable, we must, in short, reach beyond the limits we have tolerated in the past. It is a message worth stressing today, as we absorb the report of the intelligence committees' investigation into the 9/11 attacks.

And I am grateful to our witnesses for giving us their agencies' status report today—and grateful to Chairman Gibbons and Ranking Member McCarthy for convening this important hearing.

PREPARED STATEMENT OF THE HONORABLE JIM TURNER, CHAIRMAN, SUBCOMMITTEE ON INTELLIGENCE AND COUNTERINTELLIGENCE

Today's hearing of the Subcommittee on Intelligence and Counterterrorism continues the Committee's focus on how we are sharing information about terrorists intending to attack America.

In the nearly two years following the attacks of September 11, we have identified a number of things we need to do to protect the homeland, such as improved border security and preparing first responders. But even if we make these improvements, we will not be safe unless we are effectively sharing information about the terrorists' intentions against us.

The Committee has held a number of hearings to address whether terrorism information is being provided to all those who need it, whether they serve at the Federal, State or local level. Earlier this week, the Committee heard from the Department of Homeland Security, the Terrorist Threat Integration Center, and the FBI. My impression from the hearing was that while the federal agencies were working hard to improve performance, their roles were not clearly defined. This was especially true with respect to the responsibilities for communicating information to state and local officials. Both the FBI, through its Joint Terrorism Task Forces, and the Department of Homeland Security are providing terrorism information to state and local governments, but there did not appear to be a clear division of responsibility or established mechanisms for coordinating the flow of information.

Today we have the opportunity to find out from officials from three different states whether the information really is flowing, and whether it is useful.

According to one of our witnesses, Mr. Foresman, there is currently more confusion than clarity. As a Cabinet-rank state homeland security official for Virginia, he has found a lack of clarity in the coordination of information and intelligence flow, and that the current confusion only adds to the dangers we face.

For example, he finds that the Department of Homeland Security has become a new layer in the communication between the federal agencies and the states. But this new layer has not been coordinated with existing channels of communication, and has resulted in more confusion. He is receiving information from the Joint Terrorism Task Force, and then finding that Department of Homeland Security officials are unaware of the information. On other occasions, he has received information about potential security threats from the Department of Homeland Security and then finding that other federal officials in the field did not have the same information.

The confusion sometimes extends to the quality of the information. Mr. Foresman's written testimony relates one instance when he received information from the Department of Homeland Security, only to have another federal agency attack that information as "old news" and unreliable, having been over taken by events. As a state homeland security official, Mr. Foresman was then left to try to determine whether this was a case of "turf war" or whether there were substantive problems with the information.

As we have learned from the report released today from the congressional intelligence committees, one of the contributing factors to 9/11 was the failure of federal agencies to share and act upon information about the hijackers in their possession.

We know that we are a nation still at risk, as terrorists could be plotting another attack on the United States. In order to thwart the next attack, we must ensure that information about terrorist threats gets to every official with homeland security responsibilities. That can only happen if everyone involved has a clear understanding of standards that define the movement of information across all levels of government.

I am very pleased that we have the officials representing the federal agencies as well as the state and local homeland security offices here with us today to speak on this vital issue. I look forward to your testimony.

PREPARED STATEMENT OF THE HONORABLE KAREN McCARTHY, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE AND COUNTERERRORISM, SELECT COMMITTEE ON HOMELAND SECURITY

Thank you Mr. Chairman. I am very pleased that we have the opportunity today to examine the issue of information sharing within the federal government and with state and local officials.

One of the many tragic aspects of the attacks of September 11 is that the federal government did have some information about the hijackers in the files of various agencies. Although we cannot be sure that we could have prevented the attacks by connecting these dots, we must do everything in our power to make sure that information about the next plot does not slip through the cracks.

We as a nation have taken a number of steps to get at this problem. We have created a Department of Homeland Security, and the President ordered the creation of the Terrorist Threat Integration Center. We have also emphasized the importance of the federal government sharing terrorism information with the officers at the state and local level who have responsibilities for the security of their communities.

But do we actually have improved information sharing, as we approach the second anniversary of 9/11? That is what I hope this hearing will answer. On Tuesday, we heard during the full Committee hearing on the Terrorist Threat Integration Center that threat information is being fed to both the TTIC and the Department of Homeland Security. We did not get a clear answer on what TTIC and the Department of Homeland Security do with the information. As for sharing with the state and local officials, we heard that the FBI shares information through its Joint Terrorism Task Forces, and that Homeland Security also pushes information to its state and local "customers." What we did not learn was whether the FBI and Homeland Security are coordinating what they provide to state and local governments, or if there is a clear understanding of the roles of each agency.

The basic problem is very simple. If all the players in homeland security, at whatever level of government, do not have the same understanding of their roles and responsibilities, it will be all too easy for another failure in information sharing to occur. The consequences of such a failure, as we know, are grave.

I am very pleased to have representatives from the Federal, State, and local levels of government with us today so they can inform us on the status of information sharing and to alert us to problems that remain. Hearing from those on the front lines will assist us to do our part in breaking down barriers to sharing information critical to our homeland security. Thank you.

Mr. GIBBONS. I am going to turn now to the witness statements and I will begin with Mr. William Parrish from the Department of Homeland Security. Welcome, Mr. Parrish. The floor is yours. We look forward to your testimony. And to all our witnesses, your full complete and written statement will be entered into the record. If you wish to summarize and shorten your statement, that is okay too, because we realize the time is short and you have been here a while, and it is only getting longer each day.

So Mr. Parrish, welcome.

STATEMENT OF WILLIAM PARRISH, ACTING ASSISTANT SECRETARY, FOR INFORMATION ANALYSIS, DEPARTMENT OF HOMELAND SECURITY;

Mr. PARRISH. Good afternoon, Mr. Chairman. I appreciate that, and distinguished members of the subcommittee, I am delighted

and honored to be here this afternoon. This hearing is very important to the Department of Homeland Security, as I too believe it presents an opportunity to provide the status of a critical element within the Department, and that is the information analysis directorate.

It is also a special hearing, as it represents the 100th Congressional hearing for the Department of Homeland Security, since our beginning on March 1st, something I will proudly be able to share with my grandson. I am the Acting Assistant Secretary for information analysis in the Information Analysis and Insfrastructive Protection Directorate. Prior to assuming that position on July 3rd of this year, I was the senior Department of Homeland Security representative to the Terrorist Threat Integration Center. In this capacity, I served in the senior leadership position as the Associate Director for Homeland Security, and prior to my assignment with DHS, I served as the first Executive Director for the Office of Antiterrorism at U.S. customs.

During my tenure with Customs, the importance of information sharing became more evident. What I saw firsthand was the amount of information that Customs inspectors were able to acquire on the movement of people, goods and materials entering into our country.

Information that when analyzed could produce critical pieces of intelligence that may lead to connecting the dots and the detection or prevention of terrorist attacks to our homeland.

Today, within the Department of Homeland Security, we have the operational organizations that have access to potentially valuable information, such as that acquired by Customs. For example, today with the integration of the Customs and Border Protection Organization, the opportunity to acquire critical pieces of information enhances the analytical process within the information analysis directorate. Our ability to assess and then correlate this information against other agencies' information both within the Department and external to the Department supports our ability to connect the dots.

For example, on a daily basis, the Customs and Border Protection entities process over 1.1 million passengers arriving into our Nation and seaports, inspecting over 57,000 trucks daily and 580 vessels, 2,500 aircraft and over almost 325,000 vehicles across our borders.

Significant amounts of information could be acquired through each and that data could provide information that may tie it to potential terrorist nexus. The Immigration and Customs Enforcement entities investigate cases involving alien smuggling, terrorist financial operations and other crimes associated with terrorist organizations, and the Transportation Security Administration screening approximately 1.5 million passengers aboard commercial aircraft.

To further enhance the process of correlating information from other agencies, we have within IAIP the Homeland Security Operations Center, with representation from over 15 Federal agencies. Their presence, their connectivity back to their parent agencies, provides a very robust and comprehensive exchange of information, both horizontally and vertically.

IA has initiatives underway to reach out to another very important and relevant source of information, and that is our customers and our partners at the State and local government, as well as the private sector receiving reports from these organizations regarding suspicious activities, surveillance operations or stopping suspect individuals with potential terrorist nexus.

As these reports are received into Homeland Security Operations Center, they are passed to the information analysis directorate where we analyze the information and coordinate with other agencies including the FBI in order to identify any possible correlation or ties to terrorist activities.

For example, a report of a suspicious person videotaping the entrance to a nuclear power facility in one location and two days later a similar description is reported at another facility 100 miles away. In order to assess if there is a correlation to these incidents, the information analysis directorate will coordinate with appropriate State, local and Federal agencies to assess any and all information that may be related to these two incidents.

IAIP is working aggressively to implement the necessary information technology connectivity as well as the associated logistics requirements for this initiative to begin.

Currently within our Homeland Security Operations Centers, we are communicating with members of the State, and local governments as well as the private sector as our IT program continues to expand. The processes and procedures that I have described will further enhance our efficiency and analysis and assessment of potential terrorist activities.

I am confident, sir, that the procedures and the process that I have described ensures that IAIP is in full compliance with the legislation passed by Congress in the Homeland Security Act of 2002.

Each day we are making further progress to enhance our capabilities in the 19 functions outlined in the Homeland Security Act. Secretary of Homeland Security has placed the highest priority on expeditiously completing the new home for IAIP, and when completed will give us more personnel, and appropriate electronic connectivity.

However, in the meantime, we have identified procedures to ensure we are meeting our tasks and accomplishing our mission. Procedures such as employing liaison personnel from other agencies, bringing in members into our Homeland Security Operations Center, as well as into the information analysis directorate.

I have recently initiated a program for our analysts to be able to coordinate directly with analysts of the FBI, the Terrorist Threat Integration Center, and other members of the Intelligence Community. This exchange of personnel and direct access to other analysts will provide the face-to-face and the voice-to-voice connectivity that provides essential connectivity to ensure that all information is shared.

I am confident that these work-around measures are succeeding in ensuring a timely and efficient flow of information both into as well as out of the Department of Homeland Security.

Hearings such as yours today provides each of us an opportunity to look back at where we have come from since the Nation's dark day in our history on September 11th.

We need to recognize and extend thanks to you, to your staffs, our Federal agencies to include our law enforcement and intelligence agencies, the dedicated State and local authorities and the private sector and the American people in general. We have all risen to the challenges of combatting the new enemy threatening our security. Because of the coordinated efforts of all of us in sharing challenges as well as the responsibilities, we have made a difference in our Nation—and our Nation has not suffered another attack.

However, we must not become complacent nor tired nor weary. The dedication and commitment must continue and above all, continue as prayers for the safety and security of this great Nation.

Sir, I thank you and I look forward to your questions.

Mr. GIBBONS. Thank you very much, Mr. Parrish, and we do appreciate your testimony. It is always a pleasure to have you before the committee, and especially your agency, and we have always felt that it has contributed to our better understanding of how the progress is going of this important agency as we move along.

[The statement of Mr. Parrish follows:]

PREPARED STATEMENT OF WILLIAM H. PARRISH

Good morning Mr. Chairman and distinguished members of the Committee. I am delighted to appear before you today to discuss The Department of Homeland Security's responsibility in information sharing both vertically and horizontally.

I am currently the Acting Assistant Secretary for Information Analysis in the Information Analysis and Infrastructure Protection Directorate (IAIP). Prior to assuming this position on July 3rd of this year I was the Senior DHS representative to the Terrorist Threat Integration Center (TTIC). In this capacity I served in a senior leadership position as the Associate Director for Homeland Security. My tenure in US Customs as the Executive Director of Anti-terrorism provided the opportunity to gain an appreciation for the criticality of information sharing and the necessity for recognition and understanding of individual agencies' capabilities in the fight against terrorism.

Although only four months old, I can assure you that IAIP is moving forward in carrying out our statutory responsibilities, and the key missions of Information Analysis which include:

- Providing the full range of intelligence support to senior DHS leadership
- With IP, mapping terrorist threats to the homeland against our assessed vulnerabilities in order to drive our efforts to protect against terrorist attacks
- Conducting independent analysis and assessments of terrorist threats, including competitive analysis, tailored analysis, and "red teaming"
- Integrating the work of all of DHS' components as well as managing the collection and processing of information into usable and actionable information from DHS' intelligence components, e.g., the Bureau of Customs and Border Protection, Immigration and Customs Enforcement, Transportation Security Administration Coast Guard, and Secret Service
- Working closely to maintain transparent information exchange between those DHS/IA officers assigned to work on DHS' behalf at the TTIC, IA officers conducting the threat analysis mission at DHS Headquarters, our TTIC partners and Federal Agencies, state and local officials governments and the private sector
- Disseminating time sensitive alerts and advisories to federal, state, local governments and private sector infrastructure owners and operators

IAIP is unique among U.S. intelligence and law enforcement elements in authority, responsibility, and access to information. IAIP has robust, comprehensive, and independent access; as mandated by the President and in the law, to information relevant to homeland security, raw and processed, collected domestically and abroad. Accessing the information and intelligence from this mosaic of programs and systems of federal, state and local agencies supports our mission to analyze data and take action to protect against terrorist attacks directed at the U.S. homeland. IA has the ability to conduct its own analysis and to leverage the information of the FBI, CIA, and the remainder of the Intelligence Community and federal govern-

ment, plus state and local law enforcement and private sector entities, to protect of the homeland.

Central to the success of the DHS mission is the close working relationship between the Office of Information Analysis ("IA") and the Office of Infrastructure Protection ("IP") to ensure threat information is correlated with critical infrastructure vulnerabilities and protective programs. This threat and vulnerability information can then be used to recommend preventative and protective measures. The integration of information access and analysis on the one hand, and vulnerabilities analysis and protective measures on the other, is the fundamental mission of the IAIP Directorate.

Beyond the unique IA–IP partnership; the Homeland Security Operations Center (HSOC) serves as a focal point for the Nation's efforts to protect our homeland. The HSOC is a 24 x 7 x 365 days a year Watch Center and is comprised of members from over thirteen federal agencies from the Intelligence Community, Law Enforcement Agencies, emergency preparedness organizations and entities focused on infrastructure protection. Given the information provided from the parent organizations of these entities, and the all-source data provided by other DHS partners; information and intelligence relating to threats to the homeland is analyzed from multiple arenas. This all-source data-fusion performed at IAIP allows products to be tailored to address a specific threat to allows DHS constituents to prioritize resource allocations in the enhancement of their security posture to counter potential terrorist acts. IAIP is the central information nerve center of DHS' efforts to coordinate the protection of U.S. homeland security. As such, IA supports DHS's law enforcement components through timely and integrated analytical support. For example in a single day:

- In coordinating with BCBP which process over 1.1 million passengers arriving in our Nation's airports and seaports, inspection of over 57,006 trucks and containers, 580 vessels, 2,459 aircraft, and 323,622 vehicles coming into this country, IA has immediate access to valuable information of potential terrorist activities which further enhances our ability to develop threat plot lines—connecting the dots
- In coordinating with BICE; which investigates cases involving alien smuggling, terrorist financial dealings and other crimes associated with terrorist operations, IA analysis and assessments have the ability to identify potential trends of terrorist related activity
- In coordinating with the Transportation Security Administration; which screens approximately 1.5 million passengers before they board commercial aircraft, IA assists in determining individuals to be entered on the "No–Fly list" and Watch Lists

IA ensures that homeland security products derived from the fusing of disparate types of information is shared with Federal, state, and local governments, as well as the private sector. Recent products include;

- Information Bulletin discussing July 4th General Awareness issues
- Advisory on the Potential Al Qaeda Threats to the U.S. Water Supply
- Advisory on reconnaissance tactics and techniques operatives have employed in attacks overseas; i.e. Riyadh Bombing of 12 May
- Information Bulletin discussing Compromised Private Branch Exchange (PBX) and Telephone Voicemail systems
- Information Bulletin speaking to Chemical, Biological, Radiological and Nuclear (CBRN) Materials and Effects
- Information Bulletin speaking to Potential Indicators of Threats Involving Vehicle Borne Improvised Explosive Devices (VBIEDs)

Additionally, IA coordinates with the Federal Bureau of Investigation in publishing combined DHS–FBI Intelligence Bulletins.

In addition to mapping terrorist threats to the homeland, and carrying out its many other intelligence-support and analytic functions, IA is a full participant in the TTIC, with IA personnel physically located at the TTIC. The assignment of IA analysts to assist in the carrying out of DHS' analytic mission as full partners in TTIC ensures the timely and relevant information flow to and from the IAIP directorate. This is not a substitute for the receipt of information directly at DHS Headquarters, but rather represents a recognition that, as provided by Congress and the President, authorities and capabilities to deter and disrupt terrorist threats, particularly overseas, are shared among a number of departments and agencies and such activities often must be undertaken in concert with state, local, and foreign governments.

Recent experience has shown that terrorist groups may attempt to coordinate multiple attacks, both overseas and within the United States, and that threats that appear to be directed overseas may actually be directed towards the homeland, and vice versa. The threat information integration and analysis that is the beginning,

not the end, of DHS' protective mission, will most effectively be carried out, as Congressional and other reviews have recommended, when all terrorism threat-related activities of the U.S. Government work together seamlessly. This includes counterterrorism activities directed against threats overseas, as well as criminal investigation and prosecution activities, which the President and Congress did not, and, as a matter of effective government and common sense, should not, direct be carried out exclusively by DHS.

The direct receipt at DHS Headquarters of information provided by statute and Presidential direction to DHS, the complimentary work of IA personnel assigned to TTIC, IA analysts detailed to other Intelligence Community partners, coupled with the multi-agency representation in the HSOC, ensures IA a robust, comprehensive, and independent access to information; raw and processed, collected domestically and abroad; relevant to analyzing terrorist threats to the homeland

I come before you today to tell you that progress has been, and continues to be made on a daily basis in the IAIP Directorate. As with any new organization, there is work to be done. I will be the first to admit that we are not where we wish to be, but we are moving rapidly in a well-conceived and strategic way to get there in the very near future. IAIP is building a strong team of professionals and assigning dedicated and knowledgeable individuals in key liaison positions within our partnering agencies. This will further enhance the timely access to critical information that when placed in the hands of the dedicated and competent members of DHS serving at our borders, airports, seaports across America, will increase our ability to detect, prevent and deny terrorists from striking our Homeland. With the continued support of Congress, I am confident that IAIP and our partners in the war against terrorism can succeed in meeting the challenges presented before us.

As Secretary Ridge has stated on numerous occasions, "When our hometowns are secure, our homeland will be secure." That is not merely rhetoric, but a fundamental principle of the nation's homeland security effort. Everyone is a partner in the effort. We must be aggressive in connecting and staying connected with our partners to provide an extraordinary and unprecedented exchange of information. This information must be actionable by local law enforcement and first responders, but must also empower the average citizen to do their part in assisting with securing our homeland.

Mr. Chairman, and Members of the Subcommittee, this concludes my prepared statement. I would be happy to answer any questions you may have at this time.

Mr. GIBBONS. Gentlemen, if I may, I have been advised that Mr. Kallstrom has a time constraint that is going to affect his time that he can be before us, and with that and your concurrence, I would like to invite Mr. Kallstrom to submit his testimony right now, and then we will move back for the rest. So Mr. Kallstrom, I apologize for the delay in getting to you. I appreciate the fact that you have come down to testify and would welcome you to speak now, and we are looking forward to hearing what you have to say.

STATEMENT OF JAMES KALLSTROM, SENIOR ADVISER TO THE GOVERNOR ON COUNTERTERRORISM

Mr. KALLSTROM. Thank you, Mr. Chairman. Thank you for your great service. I was reading your bio. It is quite impressive.

Mr. GIBBONS. Well, Mr. Kallstrom that and about $3.50 at any Starbucks Coffee will buy you the regular decaffeinated version. So thank you.

Mr. KALLSTROM. Thank you Congressman Sweeney, who I have had a great year and a half working with in New York, and Congressman Meek, thank you for being here.

Good afternoon. I would like to begin by thanking you for inviting me to participate I think in this very important hearing. From those terrible moments on September 11th, the security of the United States and its interests has become our Nation's highest priority. Some 22 months later, our country's most urgent objective remains the prevention of another devastating terrorist attack. In meeting this immense responsibility, we must immediately recog-

nize that the extraordinary security challenges we face, in large part, can best be met by implementing an effective and workable intergovernmental approach. We must align the walls separating Federal intelligence and law enforcement agencies and State and local law enforcement. We must redefine the appropriate roles for authorities at all levels of government and in so doing, give State and local law enforcement the tools they need, timely and relevant counterterrorism information to partner in the national effort to protect our country and our citizens. We must find ways to empower State and local police and others to identify indications and warnings of potential terrorist activity.

Although many challenges lie ahead, much has been accomplished since September 11th. Within weeks of the attacks, Governor Pataki created one of the Nation's first State homeland security offices, the New York State Office of Public Security. He asked me to become the Office's first directorate and tasked us with developing a comprehensive statewide strategy to prevent, deter and respond to terrorist threats and events. He asked us to do everything we could do as a State to, in his words, never let this happen again.

Our first order of business was to more fully engage the State's 75,000 sworn law enforcement officers. Our eyes and ears in our neighborhoods and communities in the war on terrorism. To do this, we divided our State into 16 counterterrorism zones. Within each zone, law enforcement agencies now operate in a coordinated manner to best share resources, information, training and best practices relevant to counterterrorism.

In addition, we developed and deployed a New York State counterterrorism network throughout these zones. This network has effectively linked all of our State's police and sheriffs in a secure stand-alone counterterrorism information-only communications system.

In a little over a year and a half, more than 350 dedicated counterterrorism network computer terminals have been installed in virtually every corner of the State. To date, almost 200 terrorist-related advisories and alerts have been disseminated to local law enforcement and related health, education, fire, first responder and private sector communities.

In August, New York State will open its Counterterrorism Center. The Center will serve as a central State clearinghouse for information sharing and in particular, counterterrorism information at all levels.

As we recognize in our State, the inclusion of the country's 700,000 sworn State and local police officers and sheriffs in a systematic information-sharing loop is critical for us to succeed in the national war on terrorism. But in the loop, it is not necessary that all police officers receive access to everything, including classified documents within secure Federal databases. Rather, the Federal Government must provide the police officer on patrol with the ability under controlled and orderable circumstances to request a comprehensive search of Federal databases, including outstanding warrants and intelligence indices, including terrorist watchlists in order to receive a green light, yellow light, red light indication regarding a subject of interest as a possible link to terrorist activity.

By means of connectivity with a central clearinghouse like the New York State Counterterrorism Center, the cop on the street could receive focused and vetted guidance as to the immediate action he or she should take with respect to the individual in question. This can be done without providing the details of sensitive information or the methods and sources of collection. Better decisions can and will be made on the street in realtime.

We advocate the creation of a green light, red light, yellow light system that would make lawful use of the information currently maintained by relevant Federal agencies coupled with State information, and thus provide local law enforcement with the timely answer to a very basic question, does this individual have a known or suspected relationship to terrorism? And if so, what are my next steps?

The September 11th hijackers lived among us before they perpetrated their lethal attacks. Several of those hijackers had interception with State and local law enforcement officers during traffic stops. If the officers involved in these incidents were fully aware of the patents and indications of the terrorist threat to the United States and had appropriate and timely access to the Federal Government's various databases and watchlists, the September 11th attacks just might have been uncovered.

We will never know this for sure, but one lesson learned is that local and State law enforcement officers in the field must have access to a one-stop shopping resource where in realtime they can query an individual's name or identity against all terrorism-related databases.

We are well aware that this system must be appropriately tailored to be used only in connection with counterterrorism efforts. Comply with existing law and be subject to audit and review.

I must stress that the FBI Joint Terrorism Task Forces have been at the forefront and instrumental in handling terrorism-related investigations on a nationwide basis and have successfully apprehended individuals with a nexus to terrorism or organized terror groups on many, many occasions. I can speak from personal experience that these task forces are absolutely vital in the war against terrorism.

However, we have found important information obtained from these national investigations does not reach the offices responsible for patrolling the cities, towns, highways, villages and neighborhoods of our country in all cases. State and local police officers comprise far less than 1 percent of these task forces. Their scope and breadth of mission and their ability to learn what they now do not know mandates the use of State and local police as eyes and ears in their support.

To use a military metaphor, State and local police can be effective listening posts and forward observers for the task forces. Our concern is not only what the task forces do not know. It is what we as State and local communities have not been empowered to do to assist these task forces.

With means readily and routinely at our disposal, they will know more and be better positioned to protect our country.

Almost one year ago, the ten northeastern States from Delaware to Maine, including New York form the northeast region of home-

land security agreement as a consortium to combine the homeland security efforts of our States. The northeast regional agreement has focused on developing, among other things, regional information and intelligence sharing strategies. We have worked diligently with the Department of Homeland Security on these concerns, and strongly believe the northeast regional agreement would make an excellent starting point for a pilot project envisioned in the recently passed Intelligence Authorization Act of 2004, H.R. 2417.

At the State level, intelligence centers like the New York State Counterterrorism Center can be created, either within each State or as appropriate on a regionalized basis. A staff of cleared personnel assigned to the center while maintaining a direct secure line of communications with a Federal coordination center would interact both with State police and all local police departments.

Partnering with the Federal Government effective counterterrorism information sharing could be almost immediately accomplished on a regional basis.

As the Department of Homeland Security becomes increasingly operational, we must continue to connect the counterterrorism pipes to enable interagency and both international and national information on intelligence sharing on a regular basis.

America's State and local police officers are one of our country's first lines of defense against another terrorist attack. They are our forward observers. They are our boots on the ground. In this extraordinary and historic effort, they must be fully empowered and given the necessary tools to wage this great fight of our times.

We look forward to continuing to work with you to meet this challenge. Thank you.

Mr. GIBBONS. Thank you very much, Mr. Kallstrom, and I appreciate that.

[The statement of Mr. Kallstrom follows:]

PREPARED STATEMENT OF JAMES KALLSTROM

Good afternoon Mr. Chairman and members of the Committee.

I would like to begin by thanking you for inviting me to participate in this important hearing.

From those terrible moments on September 11th, the security of the United States and its interests has become our nation's highest priority. Some twenty-two months later, our country's most urgent objective remains the prevention of another devastating terror attack. In meeting this immense responsibility, we must immediately recognize that the extraordinary security challenges we face in large part can best be met by implementing an effective and workable intergovernmental approach. We must realign the walls separating federal intelligence agencies and state and local law enforcement. We must redefine the appropriate roles for authorities at all levels of government and in so doing, give state and local law enforcement the tools they need—timely and relevant counter-terrorism information—to partner in the national effort to protect our country and citizens; we must find ways to empower state and local police and others to identify indications and warnings of potential terrorist activity.

My remarks today will concentrate on the significantly enhanced function state and local law enforcement must assume in matters related to homeland security. In addition, I will outline the need to expeditiously build a bridge over the information-sharing gap that exists between the federal and state and local governments. I will share several positive and innovative steps New York State has already taken to close that gap. But because the states cannot do this alone, I will ask your support to enable a unified and workable plan for the prevention of terrorism in our country, states, cities and neighborhoods.

Although many challenges lie ahead, much has been accomplished since September 11th. Within weeks of the attacks, Governor Pataki created one of the na-

tion's first state homeland security offices, the New York State Office of Public Security. He asked me to become the Office's first Director and tasked us with developing a comprehensive statewide strategy to prevent, deter and respond to terrorist threats and events. He asked us to do everything we could do as a state to, in his words, "Never let this happen again."

Our first order of business was to more fully engage the state's 75,000 sworn law enforcement officers, our eyes and ears in our neighborhoods and communities, in the war on terrorism. To do this, we divided our state into 16 Counter-Terrorism Zones. Within each zone, law enforcement agencies now operate in a coordinated manner to best share resources, information, training and best practices relevant to counter-terrorism. In addition, we developed and deployed the New York State Counter-Terrorism Network throughout these zones. This Network has effectively linked all of our state's police and sheriffs in a secure, stand-alone counter terrorism information-only communications system.

In a little over a year and a half, more than 350 dedicated Counter-Terrorism Network computer terminals have been installed in virtually every corner of the state. The Counter-Terrorism Network has become a national model for counter-terrorism information sharing among state and local law enforcement authorities. To date, almost 200 terrorism-related advisories and alerts have been disseminated to local law enforcement and related health, education, fire and first responder and private sector communities.

In August, New York State will open its Counter-Terrorism Center. The creation of this Center is part of an integrated program that will provide for the routine and coordinated exchange of information and intelligence between federal, state and local law enforcement. The Center will serve as a central state clearinghouse for information sharing and in particular counter-terrorism information.

As we recognized in our state, the inclusion of the country's 700,000 sworn state and local police officers and sheriffs in a systematic information-sharing loop is critical for us to succeed in the national war on terrorism. By "in the loop," it is not necessary that all police officers receive access to everything, including classified documents, within secure federal databases. Rather, the federal government must provide the police officer on patrol with the ability, under controlled and auditable circumstances, to request a comprehensive search of federal databases, including outstanding warrants and intelligence indices (including terrorist watch lists) in order to receive a "green light—yellow light—red light" indication regarding a subject of interest's possible link to terrorist activity. By means of connectivity with a central clearinghouse like the New York State Counter-Terrorism Center, the cop on the street could receive focused and vetted guidance as to the immediate action he or she should take with respect to the individual in question. This can be done without providing the details of sensitive compartmented information or the methods and sources of collection. Better decisions can and will be made on the street in real time.

We advocate the creation of a "green light—yellow light—red light" system that would make lawful use of the information currently maintained by relevant federal agencies coupled with state information and thus provide local law enforcement with the timely answer to a very basic question—"Does this individual have a known or suspected relationship to terrorism and if so, what are my next steps?" With guidance and information already maintained by the government and provided through contact with such a center, a state or local police officer could then be guided to take appropriate action.

The September 11th hijackers lived among us before they perpetrated their lethal attacks. Several of those hijackers, including Mohammed Atta, Hani Hanjour, and Ziad Jarrah had interaction with state and local law enforcement officers during traffic stops. If the officers involved in those incidents were fully aware of the patterns and indications of the terrorist threat to the United States and had appropriate and timely access to the federal government's various databases and watch lists, the September 11th attacks just might have been uncovered. We will never know this for sure, but one lesson learned is that local and state law enforcement officers in the field must have access to a ″one stop shopping″ resource where in real time they can query an individual's name or identity(s) against all terrorism-related databases. We are well aware that this system must be appropriately tailored to be used only in connection with counter terrorism efforts, comply with existing law and be subject to audit and review.

At the Federal level it is essential that various agencies that constitute the intelligence community create one central repository for terrorist-related information or a method to rapidly check these repositories. The post September 11th investigation has exposed examples where critical information was "stovepiped" in the hands of one agency failing to get to appropriate people in another agency. The most telling

example of such a case is information collected on September 11th hijackers Khalid al-Midhar and Nawaf Alhazmi Midhar. Sectors of the federal intelligence community had determined the two men were al Qaeda operatives. One carried a U.S. multiple-entry visa and there were indications the two might attempt travel to the United States. However, other relevant federal agencies were not fully enlisted in the effort to track these individuals. In hindsight, it is evident that agencies like the FAA and INS might have been able to thwart entry of the hijackers into this country if there had been broader knowledge and access to just a portion of this information.

I must stress that the FBI-Joint Terrorism Task Forces have been at the forefront and instrumental in handling terrorism-related investigations on a nationwide basis and have successfully apprehended individuals with a nexus to terrorism or organized terror groups on many, many occasions. I can speak from personal experience that these Task Forces are vital in the war against terrorism.

However, we have found important information obtained from these national investigations does not reach the officers responsible for patrolling the cities, towns, highways, villages and neighborhoods of our country. State and local police officers comprise far less than one percent of these Task Forces; their scope and breadth of mission and their ability to learn what they now do not know mandates the use of state and local police as eyes and ears in their support. To use a military metaphor, state and local police can be effective listening posts and forward observers for the Task Forces. Our concern is not what the Task Forces cannot do; it is what we, as a state and local community, have not been empowered to do to assist these Task Forces. With means readily and routinely at our disposal they will know more and be better positioned to protect our country.

The Department of Homeland Security is now the cabinet-level agency responsible for coordinating the protection of America's citizens and infrastructure from the threat of terrorist attacks. Charged also with coordinating state and local government efforts for that purpose, it is logical that the DHS take the initiative in accomplishing this mission. Under whose auspices the system would fall should not be the crucial issue - the quick creation of such a system and the capacity to render it fully functional must be our ultimate goal.

The Intelligence Authorization Act for Fiscal Year 2004 (H.R. 2417), which recently passed the House by an overwhelming margin, moves toward the goal of greater information sharing between the federal, state and local governments. Section 336 of the bill would amend the Homeland Security Act of 2002 to authorize the DHS Undersecretary for Information Analysis and Infrastructure Protection (IAIP) to conduct 3 year pilot projects in several cities to encourage state and local governments, and representatives of various industries with critical infrastructure in the project areas, to collect and pass on counter-terrorism information to the federal government. As part of the proposed pilot projects, DHS would be allowed to share with state and local governments intelligence information in its possession through the use of tear-line reports. The bill would also allow the Director of Central Intelligence to establish an orientation and training program for certain state and local officials. The Director of the Terrorist Threat Integration Center would be mandated to establish two advisory councils, one of which would have as its primary focus privacy and civil liberties and the other would focus on the information needs of state and local governments. While this bill and its companion, S.1025, will need further strengthening, it provides a suitable template for airing the concerns of the intelligence communities of both state and local governments and would greatly facilitate the exchange of information between the different levels of government.

Almost one year ago, the ten northeastern states from Delaware to Maine, including New York, formed the Northeast Regional Homeland Security Agreement as a consortium to combine the homeland security efforts of our states. The Northeast Regional Agreement has focused on developing, among other things, regional information and intelligence-sharing strategies. We have worked diligently with the Department of Homeland Security on these concerns and strongly believe the Northeast Regional Agreement would make an excellent starting point for a pilot project envisioned by this bill. At the state level, intelligence centers like the New York State Counter-Terrorism Center can be created, either within each state or as appropriate, on a "regionalized" basis. A staff of cleared personnel assigned to the center, while maintaining a direct, secure line of communication with a federal coordination center, would interact both with state police and all local police departments. Partnering with the federal government, effective counter-terrorism information sharing could be almost immediately accomplished on a regional basis.

In preparation for effective and meaningful sharing of sensitive information, New York State agencies have been working with the Department of Homeland Security to obtain varying levels of security clearances to appropriate personnel. It is impera-

tive that selected and cleared individuals on a state level receive tear line intelligence reports relevant to terrorist activity so they can prepare appropriate response action plans and overlay them with the "fabric of their community." Working in tandem with select local officials awarded the same security clearance will help coordinate counterterrorism efforts from the federal level down to police officers on the street. Currently, a top-secret clearance issued by the Department of Defense may not be recognized or deemed comparable by the Federal Bureau of Investigation, thus halting the flow of vital and often timely intelligence. Therefore, New York State supports federal efforts to streamline and standardize security clearances among all Federal agencies.

Just as the federal government relies on state and local communities to be the primary first responders to a scene, we must continue to work toward the empowerment of state and local police to play a necessary role in assisting the Task Forces in the prevention of future acts of terrorism. Simply stated, we must have the ability to share what we gather on the streets and thereby materially bolster JTTF counter-terror investigations. As the Department of Homeland Security becomes increasingly operational, we must continue to connect the counter-terrorism pipes to enable interagency and both international and national information and intelligence sharing on a regular basis.

America's state and local police officers are our country's first line of defense against another terrorist attack. They are our forward observers, and our "boots on the ground" in this extraordinary and historic effort. They must be fully empowered and given the necessary tools to wage the great fight of our times. We look forward to continuing to work with you to meet this challenge.

Mr. GIBBONS. We have been joined on the panel on the dais today by the ranking member, Karen McCarthy from Missouri, and the chairman of the full committee, Mr. Chris Cox of California. Welcome, and we appreciate their being here as well.

Ms. McCarthy indicated that she will submit her opening remarks for the record, and they will be entered into the record.

Right now we will turn to—back to the schedule of witnesses, and thank you, Mr. Kallstrom, for your remarks. Very helpful and enlightening as well. We are pleased to see New York is out there on the leading edge in doing what they are doing, and we certainly look forward to studying more of what you are doing an how it is working out and—.

Mr. KALLSTROM. Thank you, Mr. Chairman.

Mr. GIBBONS. We will turn now to Mr. Lago for your comments.

STATEMENT OF V. PHILLIP LAGO, DEPUTY EXECUTIVE DIRECTOR, CENTRAL INTELLIGENCE AGENCY

Mr. LAGO. Good afternoon, Chairman Gibbons, Ranking Member McCarthy, Chairman Cox and members of the subcommittee. I thank you for the invitation to come here and speak with this distinguished panel. The discussion on the information flow and how it gets to the people who need it most is at the heart of defending the homeland. I also thank you for the break we have had. We have managed to get a lot of business done while you were gone.

Mr. GIBBONS. That is making lemonade out of lemons. Right?

Mr. LAGO. We do the best we can, sir.

I also appreciate the fact that you really want to get to the question and answer period, and since I have submitted a detailed written statement, I am going to keep my opening comments very brief. I believe we have some good-news stories. I believe we are clearly not there yet. We have a long way to go, and we have a lot of challenges ahead of us. I believe that the information flow between the CIA and the Department of Homeland Security is good. It is getting better, and it will continue to get better.

We are working with our colleagues in the Department and the Bureau to work with the State and locals to ensure that we get the information flowing both ways to get the right information to the right people at the right time.

If I accomplish nothing else today, I would like to leave you with three messages. First—and let me be clear on this—the CIA is committed to providing all of the information required by the Department of Homeland Security to do the mission that it was asked to do in the Homeland Security Act of 2002.

Second, we are working with our partners to ensure that the flow of information goes both ways to ensure that we have the maximum amount of usable, actionable information at the right place, at the right time.

And third, the CIA and the Department of Homeland Security have a unique relationship. The missions are complementary. The relationship has been interactive. We will not simply throw information across a transom and walk away. We are going to work with them. We have been working with them from the beginning to ensure that the flow of information is as best as we can get it. We supported then-Governor Ridge when he was made the special assistant to the President. We sent CIA officers immediately to help him.

When you enacted the Homeland Security Act of 2002, we immediately sent officers to the transition teams to support the transition to the Department of Homeland Security. We have CIA officers embedded into the Department of Homeland Security today. These people have been there to facilitate the flow of information back and forth. We were there at the beginning. We are going to be there now, and we are going to be there in the future.

We believe we are off to a good start. You could argue it is not fast start and you could argue it was not a pretty start, but it is a good start. We have had interactions at all levels of the organizations. We are working desperately to find the seamless movement of communications from all Federal entities to the State and local entities. We clearly are smarter today than we were 6 months ago. We are going to be smarter 6 months from now.

I tell you the only thing with certainty that I can project in the future is we are going to make changes. The way we look today is going to be different tomorrow. If we are good, it will keep evolving until we get a seamless mechanism to make this second nature to us.

As you know, to the Central Intelligence Agency, this is a new mission, to have mission partners in a domestic entity has been something that is very, new to us. Before it was very difficult to find foreign information and understand that the information could be used to defend New York, Reno, Kansas City. It was very important for us to turn our direction. We have turned. Our director has been very clear to us. We will lean as far forward as possible. We will make sure that we work with the Department of Justice and make sure we protect the civil liberties and don't get caught in those issues, but we will lean as far forward as possible to ensure that the right information is with the right people at the right time.

I look forward to this process. I look forward to the rest of this hearing today, and I again appreciate the invitation. I thank you for your time.

Mr. GIBBONS. Thank you very much, Mr. Lago. We appreciate your consideration of all this, and we also appreciate your taking time to share with us those highlights. They will be very helpful.

[The statement of Mr. Lago follows:]

PREPARED STATEMENT OF V. PHILLIP LAGO

Good afternoon Chairman Gibbons, Ranking Member McCarthy and the Members of the Subcommittee on the Intelligence and Counterterrorism of the House Select Committee on Homeland Security.

I appreciate the opportunity to join my colleagues from the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the state and local law enforcement community to discuss information sharing with the Department of Homeland Security.

At the outset, let me be clear that the Central Intelligence Agency (CIA) is committed to providing all of the information required for the Department of Homeland Security to execute the mission assigned to it by the Homeland Security Act of 2002. In fact, there are significant initiatives underway within the CIA and across the intelligence Community aimed at providing intelligence support to the national effort to protect our homeland. This support is evolving over time, and through an interactive partnership, we are all learning as we go.

The CIA and DHS have a very unique relationship. While our mission has always been to collect information upon foreign threats to our nation and, as directed by the President, take appropriate action to negate or reduce that threat, we now also have the responsibility to support DHS in its new mission to protect the homeland. Our missions are complimentary, and reflect the intent of Congress in both the National Security Act of 1947 and the Homeland Security Act of 2002. We work together to ensure that no gaps exist in our defenses. For many years, the CIA has had relationships with several of the major organizations that were brought together to form DHS. As DHS stands up and evolves, our relationship with it is also evolving. Under Secretary Libutti and Acting Assistant Secretary Parrish have already made great strides in defining the type of information that the department needs to ensure it can perform its mission. We have been addressing those issues, we are addressing those issues today, and we will continue to address them in the future. One of the truths about the future that I am sure of is that this relationship will continue to evolve and change over time as we, as a nation, continue our discussions on how to keep the homeland secure while protecting civil liberties.

Let me quickly walk you through the evolution of our relationship with DHS. Shortly after the attacks of 11 September 2001, Director Tenet designated a focal point for coordinating DCI support to this vital mission. CIA has taken an active interest in identifying the needs of the homeland security community and improving the availability of information on terrorism. For example, the CIA significantly increased the number of reports and products that not only had compartmented information but also versions that could be released in collateral or unclassified formats. The CIA sponsored numerous, non Intelligence Community individuals for expedited security clearances to ensure that critical personnel in high-risk areas could have access to information. We provided officers to certain FBI Joint Terrorism Task Forces to help prevent the terrorists from finding a seam in our defenses. When the President named, then Governor Ridge as his Homeland Security Advisor, and established the Office of Homeland Security, we made immediate contact with Governor Ridge and contributed personnel and resources to help stand up this vital office.

We went through our next budget cycle projecting the need for us to support Governor Ridge and an Office of Homeland Security that would have about 300–400 officers. In early 2002, we announced the creation of the position of Associate Director of Central Intelligence for Homeland Security (ADCI/HS) including a small staff to help focus CIA and Intelligence Community support to this Office. Shortly after the announcement, the nation evolved in its planning and established a Department of Homeland Security with over 170,000 officers. Clearly we had to resize our efforts. Initially, CIA officers were assigned to both the former Office of Homeland Security and the transition team for the new Department. Since the activation of DHS on 1 March, CIA has expanded the range of products and services provided to DHS. CIA officers are assigned to the Directorate of Information Analysis and Infrastruc-

ture Protection (IAIP) and other elements of DHS, working to provide both a core analytic capability and establish an infrastructure for the care and feeding of the new Department. These officers have supported tasks as diverse as information analysis, information system management, security oversight, and watch center operations management.

In addition, CIA provides DCI Representatives to both the Homeland Security Advisor and Secretary Ridge. The representatives are senior officers who serve as the primary conduits for the Homeland Security Advisor, Secretary Ridge, and their staffs to raise issues of concern and identify topics of special interest for the Intelligence Community to address, as well as providing a mechanism for providing DHS requirements to the Intelligence Community.

Secretary Ridge and his senior advisors receive daily intelligence briefings. The Senior Executive Intelligence Brief (SEIB) is also available to numerous officers at the department.

CIA is responding to intelligence requirements issued by DHS in addition to the standing intelligence requirements received from several organizations and components that were incorporated into DHS. We will continue to provide information directly to DHS/IAIP, in addition to information provided via the DHS representatives at TTIC and to DHS component agencies, while working with the Department to better synchronize and streamline the disparate requirements that were generated from legacy agreements.

DHS is on the distribution list for all of CIA's raw terrorism reporting, which it began to receive directly immediately upon the implementation of their communications system. Prior to that capability existing, CIA reporting was sent via indirect channels. In addition, all subordinate organizations continue to receive CIA reporting based on their requirements—as they did prior to the creation of DHS—via their existing communication chains, to ensure that the information is received by the action elements as well as DHS headquarters.

Finished intelligence products and analysis are also shared with DHS and their components. CIASOURCE provides direct, immediate access to the Directorate of Intelligence's finished intelligence products. Access to these products is determined by the reading requirements established by the requesting organizations. In the case of DHS, we are providing intelligence products based upon two distinct categories of requirements. Prior to the creation of DHS, CIA had established relationships with a number of organizations that were incorporated into the new Department. These organizations included the U.S. Secret Service, the U.S. Coast Guard, the old U.S. Customs Service, the Transportation Security Administration, the Federal Protective Service, the Federal Emergency Management Agency, and the Immigration and Naturalization Service. Although these organizations are now part of DHS, we continue to satisfy their intelligence requirements that were established before the activation of DHS. In some cases, such as the new Bureau of Immigration and Customs Enforcement (BICE) and FEMA, these requirements lists are more than 80 pages in length. In addition, the Intelligence Directorate of the U.S. Coast Guard is separately a member of the Intelligence Community and has access to intelligence products available to the Intelligence Community.

We are committed to providing all necessary and relevant intelligence to the Department of Homeland Security. It is our intent to create a dialogue with DHS and help drive out a meaningful, manageable way to flow information, in both directions. We will not simply throw information over the wall and walk away declaring that our job is done. Our goal is to develop a full and interactive partnership with the DHS.

In addition to our multiple avenues of support to DHS Headquarters elements, we also support the work of the Terrorist Threat Integration Center (TTIC), a shared partnership including DHS, CIA, FBI, DOD and the Department of State, by providing: CIA staff officers assigned to TTIC—including managers, analysts, and support personnel—the CT-Link information system, personnel positions, and funding, as legally permissible.

The TTIC partner elements use these resources, in part, to carry out the mission of directly supporting DHS and other organizations. Also, the Community Counterterrorism Board and its community warning function, with eight staff positions, has been transferred from the DCI's Counterterrorist Center to TTIC. The mission of TTIC does not transfer our responsibilities to report directly to DHS.

Thank you for this opportunity to describe CIA's role in the evolution and support of DHS. I would be pleased to answer your questions.

Mr. GIBBONS. We will turn now to Mr. McCraw from the FBI and ask for your testimony. And welcome before the committee. We look forward to hearing what you have to say.

STATEMENT OF STEVEN McCRAW, ASSISTANT DIRECTOR, OFFICE OF INTELLIGENCE, FEDERAL BUREAU OF INVESTIGATIONS

Mr. MCCRAW. Thank you, Mr. Chairman. It is an honor to be here today and I will dispense even with my prepared oral testimony and just get to the—first, I want to commend Mr. Parrish's agency and certainly the CIA. I did in my written testimony. I meant it. It is earnest. At the horizontal level, there is unprecedented sharing of information. I would contend that it is seamless. I mean, we are side by side, whether it is out in the field or whether it is at FBI headquarters, the CTC, TTIC, that day-to-day information sharing is happening, and it is nice to see. It is critical that we do it, because as I pointed out in my written testimony, I mean, the greatest force multiplier unquestionably is the sharing of information.

As Mr. Kallstrom pointed out, which I will kind of divert to the vertical sharing—I just came back from an assignment as SAC in San Antonio, Texas and had, you know, three JTTFs working under me, and of course, I would like to state for the record some of the best investigators I have ever supervised in counterterrorism weren't necessarily FBI agents. They were State and local officers. They were Customs, INS analysts from the agency, and they do a tremendous job. And clearly it requires a combined effort.

One of the things when I was out there, it was obvious to me was that we weren't doing the type of work that we needed to do to get information into State and local, the vertical side of it. Tommy Davis, the head of the Texas Department of Public Safety, former agency before I got into my bureau, made it quite clear to me in terms that he didn't have a shared comprehensive view of the threat, and it is important to note that it is these men and women that are charged and responsible for protecting the community.

So they need information, and they need it fast. They need security clearances, because they don't need just unclassified information. They need it up to certainly the top secret level many times, because they are charged with protecting public safety in their cities.

Also as Mr. Kallstrom pointed out, which I think is absolutely right on target, you know, we are blessed in this Nation to have an army of dedicated professionals, men and women—the army is up to 700 authorization, or it is over 700,000 now, and if we can arm them, they need to be armed with information, because they need to know about trade craft. They need training, and that training needs to incorporate in terms of the latest trade craft, and the more we can do, the better we can do, the better educated that we can use them out on the particular streets because they are collectors of information. Not only the first line of defense.

Moreover, the advantage of plugging into them is that if they know what the requirements are, what the collection requirements are, then guess what, they are going to be better armed to collect that type of information that goes back and gets integrated, again, into that shared threat. And we need to leverage them.

Now, the FBI, I am proud to say, has always been great collectors of information. In fact, I would argue that we have always had a great intelligence program that has been organic to our investiga-

tive mission. What we haven't done, though, however, there has never been a core competency to sharing information. We have never had an enterprise-wide plan to share information in the FBI. It has been done on a case-by-case basis. It has been done with the JTTFs person to person. However, we have not mastered that process.

Right now we are in a 10-week program. We fortunately stole someone from a—a 24-year veteran from the Intelligence Community, because we are not afraid to take advice. We are working right now instituting in the FBI an enterprise-wide intelligence program, and of one of the core, basic principles that you have to address, and it is critical, is information sharing, which is forcing us to look at and where we need to be is at a customer driven or customer centric place.

Now, I have laid out a number of things that the FBI has done. Certainly I am a big believer in the reports officers function that we have got trained professionals to extract the essential elements of information, get it out, intelligence reports back to the community, but also we need to put those people out in the field so they are also supporting that customer at the State and local level.

And chiefs of police and sheriffs and heads of State police departments, they need a global view of the particular threat, because if you happen to be the chief of police in San Francisco, and there is a global threat that includes bridges in New York, you need to know that too. You need to see it. I mean, the world has changed. Events that happen in Pakistan and Yemen can make a difference to a chief of police in Paducah, Texas and also the sheriff. That is just the way it is now.

So the director is clearly committed to doing that, and thankfully with the support of Congress, we have been blessed in a situation now to transform our entire information technology system, because that is an important part of information sharing, finding the information, the critical information that has to be shared and also pushing it to the community and pushing it to State and locals, leveraging the Internet, leveraging the technology that is out there. Post that information. Let them have access to it, because they are going to put a tremendous center—and I am very impressed with the testimony here in this 10-state initiative, and they are going to dedicate full-time resources into the intelligence process. That is good for the Nation. That is great.

The FBI has to come through and deliver on feeding their requirements in terms of information and us letting them know what our requirements are so they can collect information. And, again, thank you, Chairman. It is a pleasure to be here.

Mr. GIBBONS. Thank you very much Mr. McCraw.

[The statement of Mr. McCraw follows:]

PREPARED STATEMENT OF STEVEN C. MCCRAW

Good afternoon Chairman Gibbons and members of the Subcommittee. On behalf of the Federal Bureau of ITIvestigation (FBI), I would like to thank you for affording us the opportunity to speak to you today on this very important matter, Information Sharing. First, I would like to publicly acknowledge the outstanding support the FBI receives from the Department of Homeland Security, the Intelligence Community, and our nation's over 17,000 local and state law enforcement agencies. Our ability to share information with all of our partners has been and will continue to be a key factor in neutralizing many threats through a variety of means.

Mr. Chairman, your Subcommittee is evidence that the threat to our homeland is far different than ever before. Worldwide economic, political, social, and technological changes have resulted in a more dispersed, complex, asymmetric threat to our nation. Terrorists, criminals, and foreign intelligence collectors have significantly benefitted from these rapid changes, which have permanently shrunk the world. Yesterday, the most significant threat to the homeland was from nation states that were geographically distant and contained. Today, global networks (terrorism, organized crime, drug trafficking and foreign intelligence operations) are no longer distinct activities, but rather fluid enterprises that pose a significant threat to the security of our homeland. 1As you are aware, Director Mueller is reshaping the FBI to meet these new threats.

The FBI has always been a great collector of information; however, the sharing of information was primarily case oriented rather than a part of an enterprise-wide activity. Prior to 9/11/2001, statutory and other legal restrictions limited to some extent the degree of information sharing between the FBI and our Intelligence Community partners. Thanks to the enactment of the Patriot Act, the FBI now can clearly share information much more robustly than ever before. Moreover, in today's threat environment, cooperation rather than competition must be the guiding principle and the recognition that the benefits of sharing information far exceed the risks. We and our partners must have transparency in our knowledge of terrorist threats to the United States. In fact, it is Director Mueller's view that information sharing is the greatest force multiplier in the defense of our nation. For example, the globalization of crime and terrorism poses unique challenges to local and state law enforcement agencies. Chiefs of Police and Sheriffs need access to information far beyond their jurisdictional boundaries to protect the citizens of their communities. Today, events in Pakistan and Yemen can have a public safety dimension in San Antonio, Texas, that the Chief of Police, the Sheriff, and the Director of the Texas Department of Public Safety must know about in order for them to effectively discharge their responsibilities.

Since 9/11/2001, the FBI has implemented several information sharing initiatives and others are underway. Collectively, when fully operational, these initiatives will provide an integrated system to quickly deliver information to our law enforcement and Intelligence Community partners. All who are involved in the war on terrorism are continuing to work through very real problems, without preventing in any way the full sharing of terrorism threat-related information. We must not only collect and share more, we much collect and share smarter. Collecting and sharing vast amounts of information without any thought being given to the usefulness of the information collected is counterproductive and wastes precious collection resources, while at the same time drowning the end user, whether he or she is a Chief of Police, Department Head, or Intelligence Community Analyst.

The Intelligence process when properly executed ensures that the information shared is useful and meets the needs of the customer. Intelligence has always been a core competency of the FBI and organic to the FBI's investigative mission. The Patriot Act has created new opportunities to strengthen and expand the FBI's Intelligence capability and allowed us to move from thinking about "intelligence as a case" to finding "intelligence in the case" and sharing it widely with our Intelligence and Law Enforcement Partners.

The collection and timely dissemination of the right information to the right people as part of an enterprise-wide business process is so critically important, the Director has elevated intelligence to program status in the FBI and hired a senior intelligence professional from the National Security Agency. Under her leadership, the FBI has embarked on a 10-week program to develop and implement Concepts of Operations for all nine key intelligence functions. We have already completed a concept of operations for dissemination that focuses on both the form and substance of FBI raw intelligence reports. Our aim is to move from individual production processes to a single process that will be imbedded throughout the FBI. One of our first improvements to our already strong Intelligence Program will be to explicitly link the requirements to the raw product and produce metrics to measure our performance against the information requirements of local and state law enforcement agencies, the Department of Homeland Security, the Intelligence Community, and those of DHS officers, our Special Agents, and other Intelligence Community officers assigned to the newly established Terrorist Threat Integration Center (TTIC), in which we, DHS, CIA and others are full partners.

Before I proceed with the remainder of my testimony, I would like to take this opportunity on behalf of every FBI employee to thank you Mr. Chairman, members of the subcommittee and your colleagues for the support you have provided the FBI that is enabling us to overhaul its information technology infrastructure. When com-

pleted, every aspect of FBI operations including the sharing of information will be significantly improved.

The most productive exchange of information occurs at the people level working side by side. Currently, there are 84 Joint Terrorism Task Forces throughout the United States with participation from 25 different Federal gencies and hundreds of local and state law enforcement agencies in the 84 Task Force locations. Every JTTF Officer, Agent, and Analyst has a Top Secret clearance and unfiltered access to all of the information.

The National Joint Terrorism Task Force located in the Strategic Information and Operations Center at FBIHQ is comprised of representatives from 35 different Federal agencies. Like the JTTFs, the NJTTF benefits from the combination of experience, diversity of mission and access to the databases of each member agncy.

Even prior to 9/11/2001, the FBI benefitted from the assignment of Special Agents to the CIA's Counterterrorism Center and the CIA assignment of case officers and analysts to the FBI's Counterterrorism Division. Since 9/11/2001, the exchange of personnel has dramatically increased as has the timely flow of information. The benefits of co-location cannot be overstated. This is why the Administration made the extraordinary decision to co-locate the FBI's Counterterrorism Division, the CIA's Counterterrorism Operations and TTIC in the same facility next year.

The TTIC has already had a positive impact on information sharing throughout the community. As the Subcommittee is aware, TTIC is an interagency joint venture of its partners. The TTIC members include, but are not limited to, the Department of Justice/FBI, DHS, CIA, National Security Agency, National Imagery and Mapping Agency, Defense Intelligence Agency, and the Department of State. Through the input and participation of these partners, TTIC integrates and analyzes terrorist threat-related information, collected domestically and abroad, in order to form the most comprehensive possible threat picture, and disseminate such information to appropriate recipients. TTIC, through its structure, draws on the particular expertise of its participating members, thereby ensuring that the terrorist analytic product takes advantage of, and incorporates, the specialized perspectives of relevant federal agencies. In addition, TTIC will have access to, and will aggressively seek to analyze, information from state and local entities, as well as voluntarily provided data from the private sector. TTIC will work with appropriate partners to ensure that TTIC's products reach not only federal customers, but also state and local, as well as private sector, partners. TTIC provides comprehensive, all-source terrorist threat analysis and assessments to U.S. national leadership. Mr. John Brennan, the Director of the TTIC, and his staff have done a tremendous job in quickly standing up this vital center. The FBI is proud to be full partners in this effort.

I would now like to provide you a quick overview of other FBI information sharing initiatives.

In 2002, the FBI established the position of Reports Officer whose job is to extract pertinent information from FBI investigations and analysis and disseminate it to the widest extent possible. Currently, the FBI has 18 Reports Officers that have already disseminated nearly 2,000 Intelligence Information Reports to the Intelligence Community. We are in the process of hiring 120 more Reports Officers 90 of whom will be assigned to the field, where they will support both local law enforcement and Intelligence Community information needs.

Since 2002, the FBI has sent to approximately 17,000 law enforcement agencies a weekly bulletin concerning terrorism-related information. However, the FBI is not yet satisfied with its ability to provide our law enforcement partners a comprehensive view of the threat. As a result, we are currently establishing an executive briefing capability in the field to ensure senior law enforcement officials receive more detailed threat briefings tailored to their needs.

In addition, senior law enforcement officials need access to classified U.S. Governmnt information and to do so they are required to have a security clearance. As you are aware, security clearances are both costly and time consuming. Nevertheless, since 9/11/2001, the FBI's Security Division has favorably adjudicated over 2,686 security clearances for local and state law enforcement personnel and another 823 are pending approval. This is so important the FBI established an entire Unit to focus solely on the security clearances of local and state law enforcement executives and JTTF members.

Prior to the Winter OlYmpics, Director Mueller mandated that all domestic and international subjects of FBI terrorism investigations be entered into the National Crime Information Center, providing the over 700,000 police officers in the U.S. query access to the names of known and suspected terrorists. This information is also available to Federal law enforcement agencies and the Department of State.

Training must also be considered as an important mechanism for the sharing of essential information. The better we educate ourselves and our colleagues about the

enemy the better we are able to defend against them. All JTTF members receive specialized counterterrorism training; however, local, state, and Federal officers not in the JTTFs also need this type of information including knowledge about the latest trade craft employed by terrorists. We have expanded our counterterrorism training to include another estimated 27,000 local and state officers and are currently evaluating other training initiatives to further increase training opportunities.

An essential component of the FBI's information sharing strategy occurs overseas with our law enforcement allies. Only by sharing information and working directly with law enforcement abroad will we have the opportunity to stop criminal and terrorist threats before they reach our shores. The FBI has 46 offices overseas where we have established solid cop-to-cop information sharing and working relationships, and provided training and forensic support.

The internet provides a cost-effective means to quickly share unclassified information. The FBI's Law Enforcement Online (LEO) provides a secure and easily accessible gateway to this information. Using individual log on accounts, dual certificate authentication, and point to point encryption, LEO will provide a host of information services and enable the FBI to push information over the internet in a cost-effective manner. To further expand its reach, LEO connects to the Regional Information Sharing System (RISS) which is widely used by local and state law enforcement agencies. Furthermore, through LEO, users will soon have access to OSIS.4

Certain information must be immediately brought to the attention of senior local, state, and federal law enforcement officials. The FBI is now implementing a National Alert Notification System which provides us the ability to instantly send text page messages throughout the nation alerting law enforcement agency heads or their designees through their cell phones and two way pagers.

The Criminal Justice Information Services (CJIS) is working with local and state law enforcement to capitalize on pre-existing data agreements to address its crime statistics reporting mission while at the same time provide a national indices that will enable police officers to link subjects and modus operandi throughout the U.S.

Another information gap is the inability to access wide information on suspicious surveillances. The counterterrorism Report System on Suspicious Surveillance (CROSS) was developed by Department of Defense and is being piloted in the National Capitol Region. CROSS will be accessible through LEO and it enables police officers and Agents to report hostile surveillance activity in a Web environment and receive instant notification on similar activity elsewhere in the U.S.4

The St. Louis Gateway project was conceived by the local law enforcement leadership in the St. Louis area to provide law enforcement investigators and analysts easy access to unclassified criminal and terrorism investigative reports from multiple agencies. This initiative will employ link analysis tools and geo-spacial mapping. During the testing phase, previously unknown links between criminal and terrorism reports were identified demonstrating the efficacy of this concept. When successfully completed, this project will be expanded to other parts of the country based upon previously arranged agreements with law enforcement leaders in different areas of the country.

The FBI is also in the process of establishing FBI web pages on Top Secret and Secret Intelligence Community and Department of Defense systems so that it can "post" information on FBI web pages that is easily accessible to the entire community. The FBI also has several ongoing classified information sharing initiatives with its partners in the Intelligence Community that are providing tangible results.

Finally, it is critically important that the FBI leverage the outstanding work that has already been done in the intelligence and information sharing arena. Long before 9/11/2001, the International Association of Chiefs of Police (IACP) were working on intelligence led policing and the information sharing issue. In August 2002, the IACP published a report recommending the creation of a national criminal intelligence sharing plan. As a result, the Global Intelliqence working group comprised of leaders from local, state, and Federal law enforcement agencies was formed to address the goals and objectives outlined in the IACP report. The FBI is essentially a small but determined organization and we recognize that our future success will in large part be as a result of our ability to leverage one of our nation's greatest assets, the over 700,000 dedicated men and women who serve in local and state law enforcement.

Again, thank you for the opportunity to speak to you today and I look forward to any questions you may. have.

Mr. GIBBONS. And we will turn now to Mr. Foresman. Commonwealth of Virginia, thank you and the floor is yours.

STATEMENT OF GEORGE W. FORESMAN, ASSISTANT TO THE GOVERNOR FOR COMMONWEALTH PREPAREDNESS, COMMONWEALTH OF VIRGINIA

Mr. FORESMAN. Thank you. Mr. Chairman, vice chairman, members of the committee, thank you for the opportunity to appear today.

I currently serve as a cabinet ranked State homeland security official in Virginia and was responsible for directing State-level response and recovery actions to both the Pentagon and anthrax attacks that directly impacted the commonwealth in 2001. I am also completing my fifth year as a member of the advisory panel to assess domestic response capabilities for terrorism involving weapons of mass destruction, the Gilmore Commission, created by the Congress in 1999 to advise both this body and the President on strategies to improve America's preparedness for terrorism. I also am a former first responder. My detailed testimony has been submitted, and I will attempt to be brief and within the time constraints.

Since the attacks of September the 11th, America has made great progress in our collective preparedness for emergencies and disasters of all kinds, including terrorism. Much work remains. There is no more fundamental obligation for government than to protect its citizens. Our collective ability to meet that obligation to prevent and deter terrorism and if required, to rapidly respond and recover requires new and innovative thinking coupled with good old fashioned commitment no nowhere is this more evident than in the areas of intelligence and information sharing.

We have merged entire or parts of 22 Federal agencies into a single organization and now named it the Department of Homeland Security. With the goal of improving coordination of effort to make America more secure. The Department of Homeland Security mission continues to evolve. However, one thing is clear. There appears to be ambiguity across the entire Federal Government about the DHS role when it comes to the intelligence sharing responsibility. This is evidenced in almost the daily news articles and my discussions with officials from all levels and areas of government, the media and the private sector.

But this ambiguity about intelligence and information sharing frankly is not limited to the Department of Homeland Security. It extends across and within a multitude of Federal agencies with intelligence responsibilities. It affects how effectively they work with each other, equally important it affects how well they work with local, State and private sector players.

I would highlight three points in my written submission. The problem is not with the people, and clearly the testimony today underscored that, and interestingly enough the discussions during the break further emphasized that for me.

Clearly, there is a commitment on the part of individuals across the Federal agencies to achieve synchronization of effort, but it is clear we are not achieving that as part of a national focus. We have no macro strategic view of how our intelligence and information sharing needs can and should be accomplished with all relevant stakeholders irrespective of the level or function of government. This is a government-wide strategic-wide issue.

The confusion among Federal agencies filters to the State and local level and into the private sector. This confusion is not the fault of any one person, agency or branch of government. It comes from years of ad hoc fixes and changes to many individual components of the Nation's intelligence enterprise without having viewed them as part of a whole.

The result is unintended, but very real patchwork approach that is a threat to the security of the Nation and our ability to move information to relevant officials at the local, State, Federal level.

Second, technology, new statutes or even organizations are not the end-all answer to the problems we face. We need to commit our Nation, that is Federal State and local officials and certain private sector elements, to defining what intelligence needs to be shared and identify existing and new pathways to make it happen.

In short, we need a set of business rules with supporting planning effort. We must then focus on clarifying everyone's expectations and focus on achieving improved movement of information and intelligence among all levels, branches, disciplines, functions, areas of government in key private sector entities.

Third and finally, we must always preserve the democracy and our core civil liberties.

Security at the expense of personal freedoms and rights will accomplish exactly what the 19 hijackers intended. From my way of thinking, for our way of thinking in Virginia and in parting with 49 other States, 6 territories and thousands of Federal officials, we cannot allow this to happen.

I thank you for the opportunity to appear today and I will be happy to take your questions.

Mr. GIBBONS. Thank you very much, Mr. Foresman, for your enlightened comments. They are very helpful indeed.

[The statement of Mr. Foresman follows:]

PREPARED STATEMENT OF GEORGE FORESMAN

Mr. Chairman, Madame Ranking Member and Members of the Committee thank-you for the opportunity to appear today to discuss the issue homeland security related intelligence and information sharing with state and local officials.

Three perspectives inform my comments today. I currently serve as a Cabinet-rank state homeland security official in Virginia and was a senior state emergency management official at the time of the September 11, 2001 attacks and subsequent anthrax incidents. I also am completing my fifth year as a member of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, created by Congress in 1999 to advise this body and the President on strategies to improve America's preparedness for terrorism. Finally, I should note I am a former first responder.

We are approaching several milestones in the next several months. We will soon commemorate the second anniversary of the tragic events of September 11, 2001 and the one-year anniversary of Congress having passed legislation to create the Department of Homeland Security. Congress has already held joint hearings to examine intelligence issues surrounding the attacks and the independent September 11th Commission is expected to deliver its final report in May of next year. I remind you of these to make the point that in the context of having just celebrated our 227th anniversary as a nation, two years is a narrow window in time.

I would like to address three issues to the Committee today.

First, has the flow of information from the federal government to states and communities improved since the creation of the Department of Homeland Security.

Secondly is the quality of information sufficient to support the daily efforts of thousands of local and state officials who are on the front line of making our nation safe and secure.

Finally, I want to offer some perspective as to whether we are we making progress.

The great challenge we face in the post September 11th environment is achieving common definitions of homeland security and intelligence. In response to the extraordinary events of September 11th, we have merged entire or parts of 22 federal agencies into a single organization called the Department of Homeland Security. Their mission continues to evolve reflective of statutory language and the National Strategy for Homeland Security. However, there appears to be great ambiguity about their roles within the entire federal family, especially when it comes to the intelligence sharing responsibilities. This is evidenced in the almost daily news articles about competing intelligence activities within the federal government.

Each day states and communities are confronted with a multitude of sources of so called intelligence information. This is information that may originate at the federal level from within the intelligence, defense, law-enforcement or other federal communities. Some methods for passing information to communities and states were well established prior to the September 11th attacks and worked well, while others are less than efficient. Among the cornerstone arguments articulated in creating the Department of Homeland Security was to provide "one stop shopping" for states, communities and the private sector.

In my opinion we have not achieved the most fundamental agreement and education concerning what is "homeland security" or "intelligence". Does the term homeland security describe our response to the threat of terrorism or is it something more. Today the Federal Emergency Management Agency is a core element in the Department of Homeland Security Emergency Response and Recovery Directorate. FEMA's role in responding to natural disasters and other emergencies is clear. However, is disseminating precautionary information in advance of a hurricane making landfall a homeland security or an emergency management function. Is the data they utilize from the National Weather Service intelligence in the context of homeland security. If so what "pathways" should it follow in being disseminated to state and local officials. Are the pathways and business rules for moving the data sufficiently clear that critical information is being moved in a timely fashion. Today there appear to be no clear answers to these questions.

The same challenge remains true when we discuss those things that tend to more accurately fit into the category of intelligence. But again, defining intelligence tends to be in the eye of the beholder. Each day law enforcement agencies at all levels of government investigate crimes amassing volumes of data. Is this data intelligence, especially when it may have tangential relationships to the threats we face from our enemies. If the information potentially has direct or indirect relationships to America's war on terrorism is there a well organized structure that provides for the integration, passing and analysis of this data by responsible local, state and federal officials in a comprehensive fashion. I do not believe that is the case.

I offer both of these examples to make the point that the creation of the Department of Homeland Security and its intelligence responsibilities add yet another layer to the communication process between federal agencies and with states, communities, the private sector and citizens. This new layer, especially if it improves and better coordinates the flow of information and intelligence, is not the problem. The major obstacle that we face is adding these new responsibilities without first de-conflicting them with the long-standing communication pathways between the federal government and states and communities. I believe we have unintentionally added confusion because of the ambiguity of the Department of Homeland Security's intelligence function as it relates to other federal agencies as well as state, local and private sector stakeholders.

One would hope that among the successes we might obtain from lessons learned of the events of September 11th is that we must rethink our approach to defining the intelligence enterprise. Between elements of our federal intelligence, law enforcement and defense community's primary responsibilities for components of our "national intelligence enterprise" exist. Throughout history the Congress and Administrations have made adjustments to pieces and parts, usually in response to real and perceived shortcomings, without a seemingly comprehensive analysis of how these individual changes impact on the enterprise as a whole. The result is a patchwork approach that has created often times conflicting responsibilities, ambiguity and further intensified turf between responsible organizations at the federal level.

Furthermore, prior to the events of September 11th, state and local agencies were not viewed by federal agencies as part of America's "national intelligence enterprise". In the aftermath of the attacks leaders proclaimed the critical importance of police officers, firefighters, public health officials and other state and local officials

being key to our war on terrorism. There have been great proclamations about the need to get critical intelligence to those who are on the front lines of keeping our communities and states safe. These same ideals have not been embraced by the rank and file staff in federal agencies. My experience tells me that it is not because of a lack of desire, but rather it again comes back to the ambiguity that exists within the federal intelligence enterprise as it relates to the role of the Department of Homeland Security and what needs to be communicated to local and state agencies.

This is not a criticism of any one federal organization. Rather it points to the larger issue of overall federal coordination. There does not appear to be any overall federal vision and coherent plan across the entire federal government that articulates exactly what we are trying to accomplish in terms of information and intelligence fusion, analysis and sharing, especially related to the involvement of state and local government. My perception is that it does not appear to be clear within and between federal headquarters offices as well as with field personnel on the front lines of moving critical information and to us at the state and local level. In short there is no clear plan and direction.

Let me be clear. These challenges at the federal level are replicated at the state and local level. Agencies and entire disciplines at the state and local level have managed the flow of information and intelligence for years in a manner that best suits their purposes. Law enforcement agencies tend to focus on ensuring the quality of intelligence more for the purpose of prosecution. Public health agencies have a focus that is on preventing the spread of disease and protecting patient confidentiality. Other emergency response agencies use information and intelligence to ensure rapid response to and recovery from emergencies and disasters. Each is legitimate within their individual context. However, when viewed as part of a larger enterprise these current approaches have the potential to create confusion and conflict.

It is clear that state and local level government has a responsibility to effectively integrate information from federal intelligence, defense, law enforcement and other federal communities for its use. A single pathway is not going to work and is not appropriate. Whether it is the threat of terrorist groups, disease outbreak or even a severe storm our continuing focus is on the maintenance of a well-defined set of business rules at the state and local level that outline the pathways for moving information between those who will respond. We are seeking to enhance this in Virginia through the integration of multiple information sources into a single multi-agency center. But our efforts are challenged by the lack of clarity at the federal level among other issues.

My impression is that the Department of Homeland Security is making every attempt to capture significant intelligence currently available at the federal level and, where needed, putting the material in a useable form that can be passed to local, state and private sector organizations. My experience tells me that they are inhibited in their efforts by being a new organization that is still working through start-up, merger and acquisition issues. Furthermore, I get the impression that cooperation of other federal agencies is superficial.

But this misses the larger point of coordination. The Department of Homeland Security's most important function may be to bring the multitude of federal players together with state and local stakeholders are develop a comprehensive approach to defining what is meant by information and intelligence sharing. This must be a priority. The products are not the answer. A clear set of business rules for describing the vertical and horizontal flow of information across the national enterprise—local, state, federal and private sector is the essential first step. This has not yet to my knowledge been done. Technology and methods of protecting classified information can then be applied to meet defined objectives for rapid transfer and protection of critical national security data.

When I began my state career nearly 20 years ago doing contingency plans for nuclear attack there was a two-page description of how information should flow in the aftermath of an attack, taking into account the three levels of government and the multitude of disciplines. I have not seen a similar plan today. Effectively sharing intelligence is less an issue of technology and more good old-fashioned planning and commitment.

The flow of information must be vertical between federal headquarters offices, field and or regional offices, states, communities and the private sector and of course citizens. It is imperative that federal information reflects a coordinated and not conflicting approach, less we add to the confusion. When we evaluate the flow of federal information we see clear disconnects between that received directly from Washington headquarters and what is known by field personnel of the various federal agencies. In Virginia's case our proximity to the District of Columbia and presence of key federal operations necessitates a close working relationship with a wide range of agencies and their field personnel. It remains surprising how many times data

is received from the Department of Homeland Security, or other federal headquarters functions, that is unknown to the its personnel in the field. This again points to an enterprise wide analysis and defining of who needs to get what and how.

More is not necessarily better. Clearly the flow of information increased since the attacks of September 11th. With each passing day more information flows from federal agencies into communities and state agencies. But the simple flow of more information does not equate to better intelligence sharing. I would offer that the almost reactive nature of sharing information may be leading to a well intentioned push by federal agencies that floods state and local officials with often times conflicting data, or so much volume, that reasonable analysis is impossible. This type of visceral reactive approach often adds confusion rather than clarity to the efforts of state and local officials to meet their homeland security responsibilities. Ensuring the quality of information, assignment of priority for its movement and training and education of those who are to receive it remains critical.

We have had mixed experiences with the quality of data received. In one case critical information being passed to us through the Department of Homeland Security was almost immediately attacked by field personnel from another federal agency as being "old news" and, therefore, unreliable having been over taken by events. We were then confronted with the challenge of validating through unofficial channels what had been provided to us to determine if the disagreement was based in "turf" or substance. In another case, the Department of Homeland Security provided us information in advance of Operation Iraqi Freedom concerning potential security concerns on selected sites. This information was passed to local officials but it was clear from discussions with federal field personnel in the affected area that they had not been made aware of these same concerns. Again it posed a vexing question for us as to its authenticity and quality.

Most recently, I am pleased to report, that limited knowledge was made available to state and local law enforcement officials concerning an on-going investigation with alleged terrorism related ties. This occurred within the context of one of our Joint Terrorism Task Forces. But unfortunately the information was not disseminated within the federal agency community and when we inquired with an official at the Department of Homeland Security they seemed unaware of the investigation. These types of events, while understandable given the complexity of the issue, leave significant room for doubt about the quality of any intelligence received.

I would suggest it is to early to make wholesale judgments if the quality of information we are receiving is sufficient. Anecdotal evidence suggests that we have much more work to do and that we must place a premium on ensuring integration between disciplines, organizations, levels of government, the private sector. If the Department of Homeland Security is to be at the forefront of intelligence and information sharing with states and communities several actions will be needed.

First they must continue their efforts to capture and move critical federal information and intelligence to communities and states. This effort must separate they inevitable general information flow and time sensitive intelligence into two distinct categories. Information and intelligence that demands immediate attention must not be sent in the same manner as "good to know" data.

Secondly, a clear set of business rules must be established that defines the movement of information horizontally and vertically across all areas and levels of government and with appropriate private sector elements. Right now each agency, and in some cases elements within agencies, acts very much on their own and there appears to be no centralized authority for ensuring the development of a strategic approach, that takes into account existing pathways, the multitude of disciplines and organizations, the levels of government and the private sector. This must be an effort free of the day-to-day crunches of moving information and with sufficient authority to make it happen. Agencies and organizations need not give up their individual "turf" but rather all of these components must be deigned to operate in harmony. This effort, whether led by the Department of Homeland Security or other federal agency must have the active involvement of knowledgeable local, state and private sector stakeholders. This, I believe, will have profound positive impact on our national intelligence structure including local, state and private sector entities.

Finally, we must begin to educate. There is a fine line between our intelligence and information sharing needs and our desires. I note with interest virtually every day a new technology initiative designed to speed and empower the movement of intelligence and information. While these efforts may reflect the technological opportunities of today, they do not always reflect a comprehensive understanding of the significant policy implications of how information and intelligence is gathered, stored and used, especially as it relates to ordinary law abiding Americans.

More importantly, we find that federal agencies are operating under antiquated assumptions about sharing classified information with state and local officials. There has been only minimal progress in obtaining security clearances for state and local officials. We seem compelled to operate in an environment that seeks to empower restrictions to effectively sharing critical intelligence and information rather than promoting best practice solutions that get needed information and intelligence to those who must act to save lives. Our experience has been that when the chips are down and the crisis is at its highest point the information will be shared irrespective of clearances. But this point is too late. This approach precludes state and local officials from having digested the complexity of information and developed well-formulated response strategies. Right now the release of secure information and intelligence is built upon individuals rather than a well-defined process with auditable standards that lay a clear framework for sharing sensitive information. If we can quickly share sensitive information with our Allies then we can surely find a way to share it with state and local officials who are responsible for keeping our citizens safe and secure.

We cannot underestimate the cultural challenges of having thousands of officials in differing fields change the mentality about the sharing of information and intelligence. But this is essential to our ultimate success. The most significant impediment we face in this regard again goes back to the lack of a clear national strategic approach, one that describes what information needs to be shared and pathways for accomplishing its movement. Virtually every official that I have spoken to understands that they are part of a larger need, but in an absence of a global understanding of the enterprise or their part in it, they find it difficult to adjust their thought process. If I were to point to a major failing to date in our national reaction to the events of September 11th it is that we have not taken the time and energy to train and educate everyone from first responders to elected officials about the critical importance for effectively sharing information and intelligence. We have chosen to think of our enterprise as thousands of separate organizations with a similar intelligence and information requirements rather than a single enterprise with thousands of components. Consequently, each continues to look at its own and not the whole.

I need to underscore that my comments do not mean centralizing all responsibilities in a single agency. But there should be clarity regarding the coordination of information and intelligence flow and better methods for ensuring accountability among federal agencies that needed information is being appropriately shared. Core in our national belief is the preservation of civil liberties. One could argue that current vexing confusion only adds to the dangers we face. Our inability to produce a comprehensive set of business rules about what information should be shared and how, inhibits our ability for appropriate oversight and increases the potential that we may unintentionally undermine our core national values in the name of security. The zeal of securing our nation must not trample on the ideals of living as a democracy with individual rights.

Thank you for the opportunity to appear today and I will be happy to address any questions you may have.

Mr. GIBBONS. And finally, we have gotten to Mr. Daniels who has come a long way and has waited patiently for his opportunity to speak and all the way from Arizona. We want to welcome you to Washington, D.C., and we look forward to your testimony. Mr. Daniels, the floor is yours.

STATEMENT OF DARIN DANIELS, PREPAREDNESS PLANNING AND TRAINING MANAGER, MARICOPA COUNTY, ARIZONA

Mr. DANIELS. Thank you, Mr. Chairman. Mr. Chairman and members of the subcommittee, I thank you for the opportunity to address this committee today. I share the subcommittee's concerns about the preparedness of public agencies charged with protecting the security of our Nation and our communities and offer my comments and insights from the local public health perspective.

The most critical issue in preparedness today relates to the need to share information openly and on a timely basis. This must be done both vertically and horizontally, vertically between governments at the Federal, State and local level and horizontally across

local public and private agencies. Indeed open and timely sharing of information is essential to the ability of State and local medical personnel to respond effectively as a principle line of defense against a disease outbreak, regardless of whether the outbreak is an act of nature or an act of terrorism.

Unfortunately historically, this has not been the case for Maricopa County. Prior to the historic events of September 11th, 2001, communications were, at best, spotty and uncoordinated. Thankfully that has changed for the better. Now with the assistance of Federal funds, Maricopa County has been able to build programs and manpower dedicated to surveillance and response to any emergency situation. At Maricopa County Department of Public Health, we believe the key to successful information sharing is trust, respect and shared goals. These elements are the foundation of the partnerships and cooperative spirit needed to ensure community preparedness.

To that end, we have focused on developing strong partnerships with a wide variety of Federal, State and local agencies, including the fire departments of the cities of Phoenix, Glendale, and Mesa, local hospitals, tribal governments, the Arizona Department of Health Services and the United States Department of Health and Human Services.

As a result of our efforts, we have achieved a high level of interagency cooperation. Examples of this cooperation include shared training and table-top and field exercises. Examples which were the statewide strategic national stockpile exercise, a full-scale chemical and biological table top exercise.

This was made possible through the full cooperation of the four metropolitan medical response system cities in Arizona. These joint exercises have resulted in open lines of communication and more responsive decision making.

At public health, we understand the agencies must work together on an organized regular basis to create and maintain the communication links needed to share information. The Federal MMRS program has enhanced the relationship-building process by bringing together various agencies within the region and fostering their cooperation in creating a sense of inclusiveness among our partners.

These relationships enhance the 24-7 response capabilities locally by allowing leaders and decision makers to know who their partners are prior to any event. Public health has benefitted directly from Arizona's statewide communication system that has been developed to send information through secure and unsecured channels. The secured Internet-based communications network allows sharing of information among local governments and health care facilities. We have focused on changing the dynamics of information sharing.

An example is the sharing of epidemiological disease surveillance information. During the past few months, the public has lived with the threat of sudden acute respiratory syndrome, monkey pox, West Nile virus and the potential threat of smallpox.

Combatting these diseases requires an effective disease surveillance program and the sharing of the results through all vertical and horizontal channels.

The electronic disease surveillance system being developed in cooperation with the State and CDC will be integrated into the statewide health alert network system. This system relies on the cooperation of agencies at State and local level, including county public health departments, hospitals and infection control practitioners.

When this system is fully operational, surveillance data will be collected from these multiple sources, permitting early identification of potential public health threats and coordination of an effective response for disease control.

In conclusion, Maricopa County Department of Public Health is committed to building and maintaining the partnerships and the vertical and horizontal communication links needed to ensure open and timely sharing of information. The funds we have received from the Centers for Disease Control and Prevention through the State of Arizona have improved communications. More importantly, the funding has allowed us to rebuild an infrastructure that has been allowed to deteriorate and to respond more effectively to public health emergencies.

Mr. Chairman, this completes my prepared statement. I thank you for the privilege of addressing the subcommittee, and would be happy to respond at this time to any questions you or any other members have.

Mr. GIBBONS. Mr. Daniels, thank you very much for your testimony as well. Bringing in a perspective from your point of view is just critically important for how this committee learns more and understands more about information sharing.

[The statement of Mr. Daniels follows:]

PREPARED STATEMENT OF DARIN DANIELS

Mr. Chairman and Members of the Subcommittee:

It is an honor and a privilege to address this Subcommittee. My name is Darin Daniels. I am the Preparedness Planning and Training Manager for the BioDefense Preparedness and Response Division of the Maricopa County Department of Public Health, in Phoenix, Arizona. I share your concerns about the preparedness of public agencies charged with protecting the security of our communities and our nation and offer my comments and insight on this matter from the local public health perspective.

The most critical issue in preparedness today relates to the need to share information openly and on a timely basis. This must be done vertically and horizontally—vertically between governments at the federal, state, and local level and horizontally across local public and private agencies. Indeed, open and timely sharing of information is essential to the ability of state and local medical personnel to respond effectively as a principal line of defense against a disease outbreak, regardless of whether the outbreak is an act of nature or an act of terrorism.

The state of Arizona has 5.6 million people, most of whom reside in either Maricopa or Pima County. Maricopa County, located in the central part of the state, has 3.3 million people or about 60 percent of the state's population. The majority of the county lives in the Phoenix metropolitan area which is the state's population, economic, and political center. Pima County, located in the southern part of the state, has about 1 million people, the majority living in the Tucson metropolitan area.

Arizona has the distinction of having four cities that are part of the Metropolitan Medical Response System (MMRS), which was created in 1996. These cities are Mesa, Glendale, Phoenix, and Tucson. Maricopa County Department of Public Health, which established its BioDefense Preparedness and Response Division one year ago, is active partner with these MMRS cities and other public and private agencies in building a high quality emergency medical response system.

Unfortunately, however, partnerships and good communication have not always been the case in Maricopa County. Prior to the historic events of September 11, 2001, communications were at best spotty and uncoordinated. An incident occurred

in late 1997 that demonstrates this point. An aircraft returning from Mexico arrived at Sky Harbor Airport with 28 very sick passengers. The airport emergency medical staff responded properly, and all the ill passengers were triaged and transported to local hospitals. There was a large failure in communications as no call was placed to Public Health. Without notifying Public Health and properly screening passengers on that flight, a very infectious and contagious disease could have been transmitted to the next city by that aircraft and its unknowing passengers. Thankfully, that has changed for the better. Now, with the assistance of federal funds, Maricopa County has been able to build programs and manpower dedicated to surveillance and response to any emergency situation.

At Maricopa County Department of Public Health, we believe information sharing—vertically between governments and horizontally across local public and private agencies—requires three things:

- Trust that information will be shared appropriately and without impediments;
- Mutual respect between individuals and the organizations they represent; and
- Shared commitment to the goals of preparedness and protecting the public.

These three elements are the foundation of the partnerships and cooperative spirit needed to ensure community preparedness. To that end, we have focused on building and maintaining strong partnerships with a wide variety of federal, state, and local agencies—including the fire departments of the cities of Mesa, Glendale, and Phoenix, local hospitals, tribal governments, Arizona Department of Health Services, and the U.S. Department of Health and Human Services.

As a result of our efforts, we have achieved a high level of interagency cooperation, reinforcing the fundamental concepts of emergency response and incident and consequence management. Examples of cooperation include shared training, tabletop drills, and field exercises; these are illustrated by the following:

- Joint incident management systems training is provided regularly to Maricopa County Department of Public Health, MMRS cities, law enforcement, fire departments, emergency medical response, emergency management, hospitals, and public schools. Since many agencies function as secondary responders, the MMRS cities have brought valuable information to the table, expanding the understanding of the secondary responder agencies.
- A statewide Strategic National Stockpile exercise was held in November 2002. This event incorporated training, tabletop drills, and field activities and provided an opportunity for the different levels of government to interact and coordinate vertically and horizontally. The exercise involved the state's two largest counties (Maricopa and Pima), and included Maricopa County Department of Public Health, Pima County Health Department, Arizona Department of Health Services, Arizona Department of Emergency Management, the Tucson MMRS, the Mesa MMRS, the Mesa public school system, the Red Cross, and other private and volunteer agencies. This exercise provided the participating agencies with a hands-on experience in a real-time multi-agency emergency response situation.
- The city of Glendale sponsored a full-scale chemical exercise to replicate the interagency response capabilities that would be needed in the event of a deliberate release of sarin with an explosive device. Communication between the hospitals and the Department of Public Health was evident at the outset of the exercise; information sharing from the infection control practitioners and the Department of Public Health reinforced the routine communications that occur regularly.
- The city of Glendale also sponsored a biological tabletop drill with the Maricopa County Department of Public Health to test leadership actions and the responses to the decision-making process. . The benefits of this joint exercise were opened lines of communication and more responsive decision-making.

With all exercises, we learned many lessons and our systems were tested on many levels. The most important lesson learned from these exercises is that some agencies communicated well with one another, but others did not—either they did not receive needed information or did not know where to send it. As a result, Maricopa County Department of Public Health and its partner agencies now have a better understanding of the role of various agencies in incident management and what information must be communicated. This understanding is key to the information sharing and relationship building that is now on-going in Maricopa County and throughout the state.

Maricopa County Department of Public health has also benefited directly from Arizona's statewide redundant communication system that has been developed to send information through secure and unsecured channels. The secured Internet-based communications network, developed by Arizona Department of Health Services as part of the Health Alert Network, enhances the notification and information sharing process used by local agencies and healthcare facilities. This system will provide security, secure messaging, a public health directory, and some data translation while

serving as the gateway for a statewide system with direct access by local health departments. In addition, the MMRS notification network is a system that provides immediate notification of events to the necessary agencies at a moment's notice. This system has the capability to provide critical information and directives for a collaborative and coordinated response regardless of the event.

The technical side of communication would not be effective without a strong connection between the users of the system, and the federal MMRS program has enhanced that connection. Advisory committees, subcommittees, task forces, and planning groups have served to build a response network and good relationships among public and private agencies by creating a sense of inclusiveness. These networks enhance the local 24/7 response capabilities by allowing leaders and decision-makers to know who their partners are prior to an event. These systems, alone or combined, allow for the exchange of information vertically and horizontally.

In partnership with the state, we have worked aggressively to change the dynamics of information sharing, based in part on a new understanding and respect for roles and responsibilities. An example is the sharing of epidemiological disease surveillance information.. Epidemiological investigations and disease surveillance conducted by the Maricopa County Department of Public Health have only recently received the attention they deserve. A prior lack of understanding of the critical nature of this work resulted in diminished resources and reduced capacity within the public health system. As the role of surveillance has become better understood, public and private agencies have better acknowledged how this everyday function protects the public from the silent invasion of diseases. This is evidenced in new support for epidemiology and surveillance.

Recent events have shown the importance of open and timely information sharing between agencies. During the past few months, the public has lived with the threat of Sudden Acute Respiratory Syndrome (SARS), monkeypox, West Nile virus, and the potential threat of smallpox. Combating these diseases requires an effective disease surveillance program and the sharing of results through vertical and horizontal channels. The electronic disease surveillance system being developed in cooperation with the state and CDC will be integrated into the statewide Health Alert Network system. This system relies on the cooperation of agencies at the state and local level, including county public health departments, hospitals, and infection control practitioners. When this system is fully operational, surveillance data will be collected from these multiple sources permitting early identification of potential public health threats and coordination of an effective response for disease control.

In conclusion, preparedness for a terrorism event requires solid partnerships and open, timely communication. Maricopa County Department of Public Health is committed to building and maintaining the communication links needed vertically between federal, state, and local government and horizontally across public and private agencies. The funds we have received from the Centers for Disease Control and Prevention through the state of Arizona have improved communications. More importantly, the funding has allowed us to rebuild an infrastructure that had been allowed to deteriorate and to respond more effectively to public health emergencies.

Mr. GIBBONS. What I am going to do now is turn to the members of the committee for 5 minutes each for questioning and I will do so in the order of their arrival with one exception. I am going to turn now to the chairman of the full committee and yield my 5 minutes to Chairman Cox so that he may have the first round of questioning. Mr. Cox.

Mr. COX. Thank you very much, Mr. Chairman. Welcome again to our witnesses. Thank you very much for your participation on this panel. Mr. Parrish, thank you again for coming twice this week. I would like to begin with Mr. Foresman and Mr. Daniels, because I think you might be able to help us with questions we have about how the Washington system is working in disseminating information. When you get threat information, this question is for both of you, for example, concerning change in the threat level, where exactly does that come from in each of your cases?

Mr. FORESMAN. Mr. Cox, I would like to be able to say that it has been the same every time it has happened, but even as recently as in the last 24 hours we had yet a new process which was used to communicate information to us. Typically we find our best

notification coming directly through the Department of Homeland Security into the Governor's office into the Homeland Security function.

Mr. COX. How does that work? Who is contacting you from—.

Mr. FORESMAN. Typically what is happening is the watch center is making notification to us of a conference call in the case of something that is a nationwide alert and we are doing it in conference call fashion. In the case of specific intelligence relating to the Commonwealth of Virginia we typically will receive a call from the Secret Service and they will then be the relayer of critical intelligence from the Department of Homeland Security to our office which creates a little bit of a conundrum because frequently we get that information prior to the Joint Terrorism Task Forces having it over at the FBI.

Mr. COX. Do you have any contact with the Under Secretary for Information Analysis, or with the Directorate for Information Analysis and Infrastructure Protection?

Mr. FORESMAN. No, sir. Typically the direct relationship has been through the Office of State and Local Coordination up to this point.

Mr. COX. Okay. Mr. Daniels.

Mr. DANIELS. Mr. Cox, the information that we receive in Maricopa County comes directly from the Arizona Department of Health Services and we actually have a very good relationship with our State partners as well as our local Federal representatives.

Mr. COX. So you don't have any contact directly with the Federal Government when it comes to threat advisories?

Mr. DANIELS. We have limited contact with the Federal Government.

Mr. COX. I ask these questions because the Homeland Security Act gives the Department of Homeland Security Under Secretary for IAIP primary responsibility for public advisories related to threats to homeland security, and it requires that he provide specific warning information and advice to State and local government agencies and authorities as well as the private sector and the public. And, Mr. Parrish, I wonder if you could explain why that isn't happening exactly that way.

Mr. PARRISH. Sir, if I may, let me just explain a little bit about the organizational structure. Certainly the State and local advisor to the Secretary is a separate position. Within the Operation Center of Homeland Security there is a desk which is part of the operation center that is titled State and Local. The operations center belongs to the Under Secretary for Information Analysis and Infrastructure Protection. The message, the report, the information that is received by the Commonwealth of Virginia is coming from the operation center in the form of a document that is prepared in the Information Analysis and Infrastructure Protection Directorate, so I think it is a little bit of just an organizational understanding of how the process works.

Mr. COX. I want to jump to something that is very topical. It is in the news today. I am not going to rely on this open hearing for purpose of the questioning on an Associated Press and New York Times account of the 9/11 report that you are all aware is now released. One of the things we have learned in this report is that NSA intercepts that were in hindsight relevant to what happened

on September 11 were not translated, not only were they not disseminated but they weren't translated, and I wonder, Mr. Lago, if you can address that question. I know you are not here to represent NSA. But this is not the first time this has been a problem. In another capacity at another select committee chairmanship I ran into this problem of untranslated intercepts that were materially relevant to things that we cared about, and part of it was we didn't have the trained linguists, we didn't have the translators. Is this still a problem?

Mr. LAGO. Sir, there is always going to be a problem for that skill set. There is a finite number of people who can perform that service and there is a large body of us trying to go after these individuals. We have a number of programs in place. We are better than we were then. To get into more detail we would have to take this for the record and get back to you in another session, and we would be happy to do that.

Mr. COX. And let's quickly switch to dissemination. This stark example that for that reason made the news was an illustration of both failure to translate and failure to disseminate. But let's assume that it had been translated and now the only remaining problem is that we didn't disseminate it, and that of course is one of the reasons we formed the Homeland Security Department. We want to make sure that we have shared all of this information. At CIA, at FBI, how far along are we to building IT systems that will permit the Department of Homeland Security to have access to what you have got and how much are we reliant today still on people flagging information that DHS might be interested in? We have a statutory system that contemplates that it is all shared. We have real life and we are getting there in real life, but how far along are we?

Mr. LAGO. Yes, sir. First of all, if it wasn't translated it would not be disseminated. I mean that is just a given.

Mr. COX. I didn't ask that question but I am not sure that needs to be the case. We have a lot of resources in the Federal Government and, you know, to the extent that for years now, and at least in my oversight experience it has been years, we keep bumping into the same problem. I wouldn't want to foreclose an agency giving up ownership of something that it doesn't have the resources to translate. But that is not the question I asked you.

Mr. LAGO. Yes, sir. We have developed a couple of parallel processes to share information with the Department of Homeland Security. One, if you will, is a push process where the information is in mass pushed over to the Department and they hold their hands out with a system try to catch it and put it in the proper bins. The second, which is probably going to be more beneficial in the long run, is the pull capability where the analysts and the Department can pull the information. We have given—we are giving analysts in Homeland Security access to CIA source, a database that they can pull from. They have the same user profile capability as the CIA analysts and they can go in and pull information, it is a more manageable process. They are both up and running as we are defining the profiles and we are providing the clearances for the analysts. They will have the same access that the CIA analysts have who work in the Directorate of Intelligence.

Mr. COX. Mr. McCraw.

Mr. MCCRAW. Yes, sir. From—I can't give you the exact date when Trilogy will be fully implemented, because I am new on the design, and one of the exciting things about the design is the investigative data warehouse of XML tagging of data, and the normalization of data. We can actually take all the information that is legally allowable and, with the protocols that Mr. Lago pointed out, push that information not just to the CIA, but also the Department of Homeland, because sometimes they don't know what information it is that they want, but actually provide them investigative data, investigative reports, 302s, things that can go back, all of that stuff we are allowed to and push it to it. Moreover, you know, often it is the FISA take or it is the stuff that has been translated and sometimes not been translated and be able to get multi-media and to be able to allow, you know, them access to that as well is also part of the Trilogy buildout, and of course it is exciting for anybody that has been in the FBI as long as I have and having to do without and to be able to have that capability and then maximize, to actually pushing information, giving information out is also exciting because it certainly does—what we are moving to is a more customer concentric type of model where we are actually, you know, putting performance metrics on how well we are doing and pushing information out.

Mr. COX. I thank you, Mr. Chairman. These are important questions, but as much as I would like to pursue them beyond the time allotted I think I should yield in favor of the other members and seek possible questions on a second round. I think that is as long as I can talk before getting the chairman's attention.

Mr. GIBBONS. Thank you very much, Mr. Cox.

Mr. COX. Thank you, Mr. Chairman.

Mr. GIBBONS. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman, and, gentlemen, I want to thank you for being here today for your testimony. If I could, I would like to start with Mr. Parrish.

And just so you know, one of my very first meetings with Secretary Ridge I had the opportunity to introduce him to a regional information sharing network that is used in Rhode Island and surrounding States known as RISSNET, and it is ostensibly a tool that law enforcement uses to securely share information about criminal activity. Information that is going to be on RISSNET doesn't rise to the level of the information that would be on, for example, BCI or NCIC records, but it ostensibly is an intelligence sharing network among law enforcement. And I provided the Secretary with a pretty detailed memo on what the system is, and I also provided a copy to Chairman Gibbons and I note that he has had an opportunity to review it.

I guess if I could, Mr. Parrish, I would just ask you, I would like to know—actually I do know that you briefly mentioned the RISSNET system during Tuesday's hearing in response to a question from Mr. Etheridge about the Department's efforts to provide information to and gather information from State and local first responders, and I have to say that I am a very big fan of RISSNET and I am excited about the demonstration project that is going on between RISSNET and the Department of Homeland Security. And

I guess if you could provide my colleagues with a description as you understand RISSNET to be and the ways in which DHS is working with the network, I would be interested to hear about what has been learned from the partnership thus far because I believe that RISSNET could be an excellent model for regional cooperation across the country. And I would just like to hear your thoughts on that.

Mr. PARRISH. Congressman, I am indebted to you then for bringing that to the Secretary's attention. I think the RISKNET program does offer a capability that we are excited about in the pilot program. In April of this year the Global Intelligence Working Group met here in Virginia, in Alexandria I believe, and my predecessor Paul Redmond spoke to that group. That is comprised of numerous organizations throughout the law enforcement community, International Association of Chiefs of Police, Sheriffs Association, major city police chiefs, a wide audience of the law enforcement community across the country. One of the things we discussed in that, I should say that Paul Redmond discussed along with the FBIs in attendance was the RISSNET program, and as we got into that, looking at could we develop a pilot program that might enhance the information both from the Department of Homeland Security as well as getting the information back, as Mr. Kallstrom said earlier, the listening posts, the eyes and the ears that are out there 24/7 across this great country.

So we have a pilot program beginning and we are going to start with—any time you do a pilot we want to start a little small and not get too large. But essentially we are going to connect with the nuclear power facilities in six States. What we will get from that then is a potential surveillance operation that may come in and, as you indicated, RISSNET provides—it is not a classified system but it is a secure Internet program. It also has a great backbone that we look upon possibly building a Web-based site which would be password protected of which now IAIP could then put out its daily intelligence bulletin that would go across the country to all of its subscribers. I think the significance about RISSNET is that it reaches out in addition to your major metropolitan areas, but more critically to your small rural areas, areas that sometimes are overlooked when we get into some of these big programs. So your small police departments that may not be on a system would be able to get this critical information.

So again, sir, we appreciate you bringing that to our attention and we look forward to this pilot program. We hope to turn a switch August 15. I am not big on long, elaborated tests. I want to see quick results and then let's move on with this and hoping we will have that program, the pilot over with by the first of October, to press on. And again, sir, we thank you for your bringing that to our attention.

Mr. LANGEVIN. Thank you. I appreciate your comments and I look forward to monitoring the program to see how it progresses. I know that our first responders across the country are hungry, are anxious to be as connected with the Department of Homeland Security and both share and receive as much information as possible, and it is obviously going to be critical to the success of the Department of Homeland Security and ultimately our ability to protect

the country from terrorists. So thank you for the work that you are doing and I look forward to working with you.

Mr. PARRISH. Thank you, sir. We will certainly get back to you and keep you informed on the pilot program.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Mr. GIBBONS. Thank you, Mr. Langevin. Turn now to Mr. Sweeney of New York.

Mr. SWEENEY. Thank you, Mr. Chairman, and let me note that Mr. Kallstrom is staying here for as long as he can, running the risk of not being able to get back home because of flight pattern problems. Jim, if you need a place to stay tonight you are always welcome at my place. And I will get the questions to you as quickly as I can.

We have had a lot of discussion, in particular leading up to this hearing, about the horizontal system. It is a great challenge. I salute you folks for all of your work. It is what the President talked about when he talked about the need for America to remain vigilant, and I think some of the work that you have done is the best example of the successes we have had. I want to talk a little bit more about the vertical system, and therefore I will start with my friend Mr. Kallstrom. And as it relates to your idea about the Northeast Regional Consortium, it sounds to me to be a very solid proposition that offers us great opportunity on this dual track to really try to expedite the kind of dissemination and a two-way process. I am wondering if you have ever asked Secretary Ridge to obtain DOD authority to let individuals who have DOD clearances use them once a State has given individuals a formal need to know authorization for the purposes of homeland and maybe just very quickly tell us what the status—what the response you are getting from DHS on the idea.

Mr. KALLSTROM. Well, yes, sir, we have. First off let me say our number one priority is the same as everyone else here, and that is to stop the next event. Clearly it is important to clean it up if it happens. And that has to all happen. But I believe that we could, together, have a much higher percentage of chance of stopping the next event. We have worked greatly with Governor Ridge when he was the adviser to the President and now that he is the Security Secretary. I can't—we have had hundreds of meetings on this issue. He has been very supportive. But like this big aircraft carrier we are trying to turn around in this country, now that we are all pretty much awake as to what we have to do, it is going to take some time. We have got a lot of this put together. What hasn't been put together in fact, the recess you took to vote I think was incredibly important, because we solved about 90 percent of our problems right here while you were voting, at least at his level.

Mr. SWEENEY. We might keep you here a little longer.

Mr. KALLSTROM. But there has been great cooperation. The Department has only been stood up for what, two or 3 months or whatever it is. So I think now we are in the position to connect the pipes to the States in the test bed or in a regional or however we want to do it. I can tell you the cops are ready to play a role, and a focused role, a role that is sensitive to our privacy, the privacy that we fight and die for in this country. But they are ready to play an important role and we have the hooks and the wires hooked up

in New York State to do that. And what we really need to do now is have that pipe and have that ability to pick up the phone and talk to people that are in the know about actions that we are seeing in front of our eyes and some training that we can give. And I think, you know, in the next few months if we can put this together we will add another whole layer of protection for our society.

Mr. SWEENEY. Is there interest among the other States? Has there been an exchange of ideas among States?

Mr. KALLSTROM. Well, the 10-State consortium is just totally, totally interested in doing this. We sent a letter to Governor Ridge signed by all 10 States, and I would guess if we talked to 50 States, the 50 States would all be interested in having, you know, a better hookup, a better arrangement so that we can vet and train and be better eyes and ears.

Mr. SWEENEY. Mr. Foresman, I was interested in something you said just a second ago that typically primarily that the information on threats comes from DHS and that was actually good news, I think, for those of us here. And I am wondering, Mr. Parrish, Mr. Lago and Mr. McCraw, and maybe Mr. McCraw the most, by virtue of sort of the interaction with general law enforcement and such, have you developed similar kinds of models, or are you in the process of developing models that, you know, relate to that issue of the vertical transference and I am interested in your response and your thoughts on the Northeast Consortium.

Mr. MCCRAW. Well, first of all, my thoughts. I think it is outstanding. In fact the more of groups that set up intelligence components in those types of arrangements, fantastic. The Bureau's job has been strictly to address local and State law enforcement and feed them intelligence and we have done it in a number of ways. We are not satisfied that we have met our obligation to provide them the type of information that they need to do their jobs, and we have got a number of initiatives that I detailed in my testimony. But I am convinced that when we take this as the whole and look at it from an integrated standpoint it will do the job.

Now we have to, you know, we have to make it—you know obviously not treat it as just a by-product of what we do, but actually make it a core function and have performance metrics and talk to the customer and treat, you know, individuals like Mr. Kallstrom and treat others that are involved in the State and local law enforcement as customers, whether it is a briefing program, whether we are pushing information, whether it is LEO, whether it is RiskNet, which finally surprisingly we have actually for good government's sake combined or provided connectivity between LEO and RiskNet so that customer on RiskNet has access to the same information, and I can assure you in week seven of our concept of operations it will become an enterprisewide activity.

Mr. SWEENEY. Let me thank you. I have to go preside over the House. Let me say I am glad we were productive, at least bringing you together. I look toward to working with each of you and all of you and I thank you for your service. I thank the chairman.

Mr. GIBBONS. Thank you, Mr. Sweeney. And Ms. Lowey.

Mrs. LOWEY. I am delighted to welcome the panel, and I guess Mr. Kallstrom is the man of the hour. We are two New Yorkers here today and thank you so much for appearing before us. And I

apologize, we are all running from one hearing to another. But I would like to pick up on where our Chair Chris Cox left off and I think because I have 5 minutes, and I know you are a quick study, I am going to just go through a series of questions and then if you can respond to the whole issue I would be most appreciative, Jim. That would be great.

One of the questions was, number one, who provides you with information about terrorist threats? The Department of Homeland Security, the FBI, another agency? And if you receive the information from both, can you determine what types of information are being channeled through DHS or the FBI? And is it a problem to receive—I don't want you to take notes, but I think you can kind of get it as I am going down. Is it a problem to receive terrorism information from the Federal Government through more than one channel?

Following up on that—.

Mr. KALLSTROM. No, it is not.

Mrs. LOWEY. Then we can go back to the other, and if you can compare as you are talking about this. Can you compare the status of information sharing prior to the passage of the Homeland Security Act to the present situation? Has anything changed? Do you have a sense that the information you receive from the Federal Government is coordinated? Do you ever receive conflicting information from different Federal agencies? If you care to provide some examples, you certainly can. And how do you do deal with it, and has the Information Analysis Office ever contacted you to coordinate training for your employees regarding information sharing? Has another Federal agency provided such training?

Maybe I will stop at that point. You get what I am trying to say.

Mr. KALLSTROM. We work a lot together so>

Mrs. LOWEY. Well, I appreciate it.

Mr. KALLSTROM. We love getting information from multiple sources. We would like it by the wheelbarrow full. I have to congratulate the Federal Government and maybe it is a function of the fact that I spent my whole life in the FBI and have personal relationships and have maintained a security clearance. But the CIA, for instance, has been incredibly responsive.

George Tenet sent someone to New York—maybe I shouldn't say that—but for the sole purpose of sharing information with us, and it couldn't be better.

Mrs. LOWEY. On a regular basis?

Mr. KALLSTROM. On a regular basis. Of course it doesn't solve the bigger problem, but the cooperation has been great. The people trying to, you know, hook up the wires in a system that isn't quite organized yet the way it needs to be. Everyone is interested in doing that. The three FBI task forces in New York State have been great in sharing information about their investigations although they don't have, in my view, the bigger picture that they need. So we have had those great relationships. What I—and Homeland Security has been great. I mean since they have been stood up, since Bill Parrish has been over there, Frank Libutti is a 20-year friend of mine back from the Marine Corps, we talk almost every day. And we talk about the issues, the priorities that were faced. So I think the intent, the human heart throb intent emotion to fix this

thing is there. What we have to do now with the help of Congress is figure out a way of more systematically and routinely and real time—I mean, yes, there is a need to go to a Web site and look at stuff and that is all part of training. But I need a cop on the Taconic Parkway tonight that has got a car pulled over with a potential terrorist in it. We don't know. But for whatever reason his suspicion has been raised as we trained him to be a more observant person. I want that person to call a center in New York State, or if he is in Boston to call a center, you know, in Massachusetts or whatever State, and to put that information into the center which is connected to Washington, all these guys and others that aren't here, and get some real information in the center about the, you know, how important it is that we have this guy on the side of the road. Do we let him go, do we bring him in, do we do something else because of the information that we have so we can make better decisions. And then the flip side of that is in New York State we have got 75,000 cops, and you know a lot of them. They talk to you all the time in Westchester.

Mrs. LOWEY. I was going to let you finish the sentence because if you could expand on that, because I hear that over and over again.

Mr. KALLSTROM. Right. And there is about less than 1 percent of them that are part of the three terrorist task forces and that is through no fault—I mean that's the amount of local police, State police, local police we have on the task forces. I ran the one in New York City for 4 years, and it is a very effective, it is a fabulous thing to do. The problem is the other 74,750 that are on the streets were not effectively using their eyes and ears.

So we need to train them. We need to enable them. We need a system so we can communicate, you know, right from the street down to Washington and from Washington back again in the counterterrorism business only. You know we are not looking to make cops a new band of intelligence gatherers at political events or any of that stuff. I am talking about countering terrorism. And we can do this. They are ready to do it. In New York State we have hooked up all the cops. We have secure communications with every police chief, every sheriff in the State, and so we are ready. We have got the pipe. And now we want Washington to organize themselves so we can talk to them and, yes, we need archived information. Yes, we need stuff that we can go to Web sites and find stuff. But we also need to pick up the phone and talk to someone that has access to all this information so we can make better decisions.

I see the State center as being sort of a tangent to Washington, sort of their guys in the State that are trained, have the right security clearances, understand the sensitivities of this information, understand the legal rules of how we store information, how it is retrievable and we can let cops without top secret clearances, without secret clearances communicate with us with real time information. And guess what? We can all be safer because we have got 700,000 more pairs of eyes and ears out there that are being more effective to protect us against the next act.

So, you know, I don't know if I answered your question.

Mrs. LOWEY. You sure did, Jim.

Mr. KALLSTROM. But that is what we are trying to do.

Mrs. LOWEY. You sure did. And rather than my going through more questions I really want to pursue that for a minute, because you know I have been meeting with the police, the firefighters, everybody. Now, I heard that a year ago. I heard it 6 months ago. I am hearing it now. We just appropriated on our committee, on which Sweeney and I—well, we all, many of us serve, $39 billion for Homeland Security. The gentleman—I forgot his name—who appeared before us was telling me on the interoperability issue, which is a little different from the issue you are presenting, that they are going out with an RFP within a year. We will get the equipment so everyone can talk to each other. And I said great. Are you going to have a buyback program because my guys aren't waiting for you to go out with the RFP 6 months from now, a year from now. You will get back the information. How—.

Mr. KALLSTROM. Just give us some secure phones.

Mrs. LOWEY. Well, how can we be of help to, I mean, the problem—you and I have talked. This is an issue we have been hearing a long time. Charlie Cole in Yonkers is still complaining about this. How can we help you?

Mr. KALLSTROM. Congresswoman, I think we are on the verge of making this happen. I think, you know, the Homeland Security Act I think that the House Intelligence Appropriations Act of 2004, with some work, it needs a little bit of work, is a good vehicle for authorizing this type of exchange if we need authorization. I don't see any legal impediments to doing this. I just think we need to get everyone down here to hook this thing up. And if we start off at, you know, if our engine can go 10,000 RPM and we start off at 2000 RPM, that is okay. We can make this thing work and we can develop it along the way. And I think we are ready to go. I really do.

Now, are all the States, have they done what New York state has? I don't know. But I mean we are willing in our 10-State consortium—I don't know if you were here when I talked about that. We got all the New England States and New Jersey, Pennsylvania, Delaware and New York, that have formed a group just to share information. They are ready to go and they are ready to use a regional center for this very reason. So I think this is not that hard to do. I think we just have to get everybody in the same room and do it.

Mrs. LOWEY. I am probably out of time, but I just—I see the red light. I just wanted to thank you very much and thank you all and hope with the efforts of all you good people you can push us and help us move this forward so a year from now we are not still talking about how we can get it through.

Mr. KALLSTROM. Yeah, and money would be helpful at some point.

Mr. GIBBONS. Thank you very much, Ms. Lowey.

Mr. Meek.

Mr. MEEK. Thank you, Mr. Chairman. Like I started out in the opening statement, I am glad to be here today because I have been wearing many hats over there the last couple of years in Florida. We followed New York as relates to passing Homeland Security legislation in the legislature there. Also, in my past I have been a first responder, and now I have had an opportunity to serve with

these very fine men and women in the Congress. I have been in a lot of circles where folks are saying that they are sharing information and we are all getting along and we are all hugging and carrying on and saying good things about one another.

But I think, like I said at the beginning, of some of the events that have recently taken place in the area of intelligence. Is it good or is it bad? Who is sharing it with what and who said what? I watched Director Tenet's body taken from the Senate intelligence chairman over in the Senate, thrown from the train as it relates to who gave what bad. Neither here or there, no one will ever know the prevention that all of you provide every day of being able to seek and find out and inform law enforcement agencies on what they need to know as it relates to potential terrorists in this country. But also I want to direct my question towards the fact that what are we doing as it relates to individuals, especially as it relates to State and local law enforcement and even the FBI who—what I may call home grown terrorists those individuals that are in the heartland and in Miami and in Chicago and these individuals that prey upon us not being prepared? I don't know how they play into this bigger role. Many Americans feel that our counterterrorism efforts are targeted towards individuals from the Middle East or targeted from individuals that may be from a country or a state outside of our homeland here that may bring about a threat to our country. And I think that it is important because when it comes down to homeland security, unfortunately, and folks from New York here, I want to apologize for the events that took place in the city yesterday, but automatically the thought that it was a terrorist attack. So I want to find out how does that play into the role of some of you that are sitting at the table, number one. Number two, as it relates to the front line guy or gal that is in the patrol car like the Oklahoma situation, it was an officer pulling an individual over. How are they getting that information because I guarantee you this committee room may not be full today, but let something happen and someone knew something and someone else didn't know it, and I guarantee you could get members who don't even serve on this committee trying to get into this room because they are looking at who is going to be at the lynching at high noon the next day because they don't want the burden to be on them.

So I am saying a lot, but I want to make sure that we are actually talking. I take some comfort in the fact that y'all were able to complete some business while we were on the floor voting, but I want to know outside, and the people that serve under you, is there real communications, you feel comfortable with those communications? Because I don't believe that is something that we can legislate, to be honest with you. We can try, but I don't believe that is something that we can legislate. Historically in law enforcement or any sense of power or even here in the Congress, there is some information that even we don't share with one another, but in this case it is imperative.

Mr. PARRISH. Let me if I could just open up because in your opening remarks you made a very relevant and germane statement when you said that the information that is provided to the State and local authorities must be relevant. One of the things that we

do in the Information Analysis Directorate is we take in volumes of intelligence at the very sensitive level. In reviewing that with our counterparts at the CIA, at the Terrorist Threat Interrogation Center or the FBI, what we are looking for is getting something that is relevant in the hands of a police officer on the street and working with the FBI to get that information to him, something that is relevant to a private sector to enhance their security posture at either a chemical facility or a shopping mall. The intelligence that we get sometimes is very general in nature. What we try to do is to take a look at it and pull out what can be actionable intelligence to get out there to the people to look at.

One of the initiatives I have now is to draw upon the successes of our country's great Americans wearing a uniform serving in the military and the captured individuals involved with terrorist organizations from Afghanistan. Also the FBI has made numerous arrests and the CIA has seized many. Our allies in some other countries have picked up significant members of the al Qaeda leadership organization. What the IA is doing right now is reaching out to the CIA, to the FBI and coming together to sit down and analyze the intelligence that is being pulled from these individuals. What I want to be able to do is to assess the capabilities of the threat that they say they have to take down a bridge, to take down a tall building. What were the skill sets taught in the training camps? Did they in fact really have that capability? Did they really analyze and take a look at the amount of resources required to do that? Those to me are the nuggets of information that we can get out to our State, local, and private sector when we put out a threat against a bridge, against a tall building, against an apartment complex. Help them prioritize the expenditure of their minimum resources they have in a prioritization of how to expend that. Working with the FBI, again, their information is getting out to the State and local law enforcement entities. Our customer base is a little bit different, but yet it is important we get that information out there.

So we are taking a very close look at this very sensitive, classified information. We must realize we have to protect sources and we are sensitive to that. But we want to get that down to the level that a police officer on the street, a Wackenhut security guard actually understands what this means to him or her in the performance of their duties. And I think probably, Steve, I would turn it to you.

Mr. MCCRAW. Yeah. I think that is a very astute observation. We must be mindful, you know, prior to 9/11 that Oklahoma City took more lives on American soil than any other international terrorist act and that Eric Robert Rudolph was caught by a State and local officer, a local officer in Andrews, or in fact Murphy, North Carolina and not by the Federal Government. You know, point in case why you want to leverage those opportunities. The FBI still has domestic terrorism. The JTTF still works domestic terrorism. We still are focused on the Phineas Priesthood, the Aryan Brotherhood, the ALF, ELF and the myriad of other domestic terrorist organizations that have been documented that are out there that are active and in conducting day-to-day investigations on those. And it has to be

done that way and we have to be mindful and we have to infiltrate them as well to prevent the next act of terrorism.

So I think that is an outstanding point. And again you do it the same way, you know, working relationships, cop to cops, and what is good for international terrorism in terms of information sharing that the FBI is doing and adopting is also the same for domestic terrorism. It has to be shared to the widest extent possible. And thank you.

Mr. MEEK. Mr. Chairman, just a closing comment. I know that I am out of time, but I just want to say I think we have two choices here, one, to work together in times of prevention and when the waters are calm, and to work together but somewhat be suspicious of one another in a time of crisis. And after 9/11 a lot happened. This Congress moved in an unprecedented way in passing legislation, authorizing dollars, flying and having special meetings and joint sessions. And I think it is important that we do everything we can do and while the waters are calm to get—pay justice to that individual out in the patrol car, at the same time pay justice to those individuals in State agencies that are trying to do the best they can do to be able to make things happen. And I know that the FBI, CIA, you know, after the joint commission and the 9/11 report and all of that from out of this Congress, from Mr. Porter Goss' committee, that you are now working together. We are all better now. We want to make sure that we get better.

One of you made the comment—I am sorry I had to step out for a minute—of the fact that we are better now than we were 6 months ago and hopefully we will be better as we move along. We hope that that is the case. Please let us know if there is anything that we can do to make sure that the line of communications are there. But I think only the people in the law enforcement and prevention agencies that are out there, even within the Department, can even move better than we can because we can't legislate that. That is something that just has to come together on behalf of our country.

Thank you, Mr. Chairman.

Mr. COX. [Presiding.] I thank the gentleman. Chairman recognizes himself for 5 minutes. I want to talk about clearances.

Mr. Foresman, Mr. Daniels, are you finding that the people at the local level are able to get clearances in a timely fashion?

Mr. FORESMAN. No, sir.

Mr. COX. What has been your direct experience?

Mr. FORESMAN. We have had a multitude of direct experiences and, Mr. Chairman, I would also like to say I don't think clearances are as much the issue as developing an auditable process to share information much the same way we do with our allies on a day-to-day basis because we don't clear our allies to get classified information but we do have an auditable process that allows us to share it with them. But having said that, I think the big challenge that we run into is just the length of time that it takes to clear individuals. We happen to have one-term governors in the Commonwealth of Virginia. We started this process, I had a clearance previous to coming into this Cabinet position. Others who are in this office did not. We are just now getting the first of what are supposed to be seven or eight clearances. We have not cleared our

Chief of Staff. We do have a clearance for the Governor. We are doing the Governors much the same way that we do Members of Congress.

Mr. COX. How long did it take the Governor to get cleared?

Mr. FORESMAN. Interestingly enough, Mr. Chairman, we suggested at a hearing up here on the Hill, and this is a prime example of where Congress stepped up to the plate, that if you as Members of Congress could receive classified information by signing a nondisclosure agreement certainly Governors could as well, and DHS moved rapidly to get the Governors to sign nondisclosure agreements.

Mr. COX. And that was all it took?

Mr. FORESMAN. That was all it took.

Mr. COX. But, now, with respect to the seven or eight clearances that are coming to the floor as we speak, how long has that process taken?

Mr. FORESMAN. We have been in the process for over a year, Mr. Chairman. And again, the issue is if you look across the universe of people who have a need to know information in Virginia, it is in the hundreds if not thousands. And the simple fact is developing a process to clear all of those individuals may not be as important as developing a process to sanitize information as appropriate and to rapidly get it into their hands in a form and fashion that they can act on it quickly. Because with even the simple turnover, if it is taking a year or 18 months to clear an individual, we could theoretically start a state police superintendent today and in 18 months have to start over again because he or she has left the job.

Mr. COX. Now, when Secretary Ridge was in California we had a discussion with the California law enforcement officials in Los Angeles. It was suggested, and nobody objected to the notion, that we could democratize the process a bit, share the workload. Obviously it is a Federal function to clear people, but there isn't any reason in the world that we cannot rely on the manpower in the States to do some of this work. If you have got requirements, if not in the hundreds then possibly over a thousand people that have a need to know in Virginia, need to know something, and it would be useful to have access to information at those levels, then surely the Virginia State police or Virginia law enforcement can do some of the knocking on doors and interviewing and so on that comprises a large part of this burden. Has anybody suggested to you that we have a joint Federal-State arrangement for clearances?

Mr. FORESMAN. Mr. Chairman, we have actually suggested that on a number of occasions, but I think what we are finding now is that the background can be done quickly, whether we are using retired FBI agents or other Federal law enforcement personnel, State law enforcement personnel. But then we have to adjudicate the clearances once the background information has been done by the Federal agencies. But this points to a larger issue, Mr. Chairman, that if I get a clearance through the Department of Defense, is it going to be recognized through the Federal Bureau of Investigation and is it going to be recognized by the CIA and is it going to be recognized by the Department of Homeland Security, and I will tell you the simple answer is today still no.

Mr. COX. And so the seven clearances that you have gotten or about to get are valid where and invalid where?

Mr. FORESMAN. It depends. It is in the eye of the beholder, Mr. Chairman. And again that is not an indictment of the fact that we have got a very diffused enterprise across the Federal Government in how we manage the clearance process in much the same way that we have a very diffused enterprise in terms of how we manage the flow and the movement of intelligence and information horizontally or vertically.

Mr. COX. For your purposes and for purposes of the clearances that we are using as examples in this question, who is the Federal agency with which you are dealing?

Mr. FORESMAN. It has transformed over a period of time because in one case, and this is actually a little bit interesting, DHS is on the front of seven of them. For a period of time before the merger and acquisition went through it was the Federal Emergency Management Agency. Those individuals who were associated with our Joint Terrorism Task Forces it is being done through the Federal Bureau of Investigation. Those individuals with—that have to work closely on DOD installations across the Commonwealth on response issues, it is being done by DOD. And the most recent is the U.S. department of Transportation Office of Pipeline Safety is currently in the process of doing some folks.

Mr. COX. Mr. Parrish, let me ask you that. You may not know or you may know precisely the answer to this question. But does the Secretary or his delegate within the Department have the authority to grant clearances to State and local officials?

Mr. PARRISH. Sir, I will get you a definite answer back to you. We do work the process with Secret Service to coordinate the issuances of clearances. We are looking at that. With regard to Mr. Foresman's comments of different Federal agencies granting clearances, my experience holding a Top Secret/SCI for as long as I can remember, when I was in the military, I worked in the counter drug business with the FBI and DEA. All of that was honored as well as with the CIA, so that is one I think we need to get back to Mr. Foresman and the Commonwealth on, and we will follow up on that.

I would like to say if I could, I think Mr. Foresman is exactly right. It is the process of information sharing that goes back to what I commented to Congressman Meek, is one of the things that IA is doing right now, is taking a look at this sensitive information to see what is relevant, what really could a State and local authority do with this piece of information when it is analyzed and assessed. Some of this intelligence at the very sensitive level is so general that it is really when they get it they say what does this mean to me, Patrolman Smith, in Topeka, Kansas. One the things we have in IA's initiative as we are following up is to get a training program to train the intelligence analysts within State and local communities so that when they do get this intelligence they know what the method of looking at it as well as following up and going back and asking for what we call RFIs, requests for information, additional requirements that they may have germane to their mission. The other piece we are looking at is a fellowship program within our, Fusion cell. It will probably become the information fu-

sion cell within IA where we will have DHS law enforcement personnel from the Customs and Border Patrol, Immigration and Customs enforcement, but also a fellowship to bring in analysis from Stat/Local Agencies from around the country to spend perhaps 2 weeks in our operations, than having just rather the fusion cell looking at this intelligence at the classified secret level. We would get them interim secret clearances to come in there to be able to understand our operations. Part of the problem when we deal with this information is analysts have to understand when they look at a report "they must ask themselves what is it that I know and who needs to know it." And that is the essence of information sharing, is getting people trained to understand what it is they are looking at, understand who needs to get this information.

Mr. COX. I want to take us back, although I certainly think that your point about information sharing as against clearances is a transcendent one, is the purpose of today's hearing fact in fact. I want to take us back to this clearance question, because the question that I asked, I don't know the answer to either, a moment ago, about whether the Secretary or his delegate has the authority to grant clearances to the State and local officials. The reason I don't know the answer is that the best we have been able to come up with on the committee is the President's executive order of January 23 of this year, which gives to you, gives to the Secretary—I will read the categories of people: The Secretary of Homeland Security, the Deputy Secretary of Homeland Security, the Under Secretary for Information Analysis Information Protection and the Assistant Secretary for Information Analysis, Department of Homeland Security, each shall be considered a senior official of the Intelligence Community for purposes of Executive Order 12–333, and then you know, on and on. And then it goes on to say that specifically you have the authority to recognize and give effect to and make clearance and access determinations pursuant to Executive Order 12–968 back in 1995 with respect to all employees of the Department of Homeland Security, all applicants for employment at the Department of Homeland Security and all people in the private sector. It doesn't say anything about State and local governments. Now this is an EO and it is not perfect, obviously, but I don't know whether that loophole or that gap is filled somewhere else, whether you think you have the statutory or executive authority to do this. But surely we would like the Department of Homeland Security to be able to address the problem of clearances among State and local law enforcement, public health officials, and the harmonization of those clearances for Federal purposes because we are trying to share here. That is the main purpose of Homeland Security, and it remains a puzzlement to you as you sit here at this hearing and to me as chairman and to our staff, and so it probably requires a little bit of work.

Mr. McCraw.

Mr. MCCRAW. Mr. Chairman, if you don't mind, from the local and State law enforcement standpoint the FBI has taken on that responsibility. In fact, if it is not working well, I mean we are the ones that need to be held accountable as it relates to local and State law enforcement specifically and we—I know we have made a number of gains under Assistant Director Senser's leadership. We

stood up a unit just specifically to address State and local law enforcement clearances, and I know close to 3,000 have been cleared and another 800 are in background right now. We see for a secret clearance we can make it as quick right now, in terms of setup, 60 days for a secret clearance. And as most of the gentlemen know at this table, the secret clearance will get you to where you need to be most of the time and top secret takes much longer obviously for the JTTFs.

Mr. COX. Would the support of State and local law enforcement assets and resources help speed up the FBI process?

Mr. MCCRAW. I think we are in good shape right now. There are some things that can't go any faster. You can't force it through even with more people, Chairman. However, when we can make that 60-day to 90-day window for the secret clearance for State and locals and the chiefs of police, that works real well. And they have been very vocal. The chiefs of police are not very shy about letting us know when we are falling down on that, on getting their clearances through. And so the good news is it is one clearance for all. I mean whether you are in the Homeland Security, the agency, the military or if you are a Governor given a clearance, that counts across the board. It doesn't matter who got it for you.

Mr. COX. Mr.Markey.

Mr. MARKEY. Thank you, Mr. Chairman. Mr. Lago, the now declassified National Intelligence Estimate said that if we didn't attack Saddam then it is unlikely that he would use biological, chemical, nuclear materials, but if we did attack and we destabilized the government that there would be a significant increase in the likelihood that he would align with al Qaeda, he would align with other terrorist groups. In view of the fact that we have yet to find the chemical, biological, nuclear materials that were reported to be there before our attack upon that country and that the scenario which the National Intelligence Estimate is most concerned about is now in place; that is, that he is not in government, is he telling you, you are not authorized to this question that—have you changed now your recommendation, for example, Mr. Daniels, over here? Have you told him to be on the alert for biological, chemical, and nuclear materials that might be in the hands of al Qaeda?

Mr. LAGO. Congressman, we should be on the alert today regardless of the information—.

Mr. MARKEY. Have you notified Mr. Daniels that he should be on higher alert because the scenario in the national intelligence estimate has now unfolded?

Mr. LAGO. No, sir.

Mr. MARKEY. You have not. Why is that?

Mr. LAGO. Congressman, again, we should be on the alert for those attacks today. We have no specific information, no specific actionable information—.

Mr. MARKEY. The national intelligence estimate said that there would be a significant increase in the threat if we went in and we did—.

Mr. LAGO. Sir, I understand that. We have no specific actionable information to pass on to Mr. Daniels today.

Mr. MARKEY. You do not. So has there been a change in the national intelligence estimate now in terms of what the threat is that

is posed to our country? Was that wrong? Was the information prior to the war wrong?

Mr. LAGO. Sir, I—.

Mr. MARKEY. You can answer.

Mr. LAGO. I am not an expert in this field. I will take that back for the record and we can get back to you.

Mr. MARKEY. I think America has a right to know whether or not the national intelligence estimate on that subject was correct; and if it wasn't, then they probably should say that the Intelligence Community has changed its mind, that there is no heightened risk now that the uranium, the biological and chemical materials are not accounted for.

Mr. LAGO. Sir, as I said, I will take that back for the record.

Mr. MARKEY. Because it seems to me that was the major justification for the war.

Colonel Parrish, I am interested in finding out the process by which the Homeland Security Department's information analysis and infrastructure protection unit operates under various scenarios. As you know, 22 percent of all cargo is transported on passenger planes and isn't physically screened at all. In fact, packages and mail weighing less than 16 ounces aren't even subject to the Bush administration's flawed known shipper program which relies on the shipper's paperwork as a guarantee that the cargo was safe. It just goes right on the passenger plane unscreened.

As you know, Pan Am Flight 103, which exploded over Lockerbie, was brought down with a small quantity of plastic explosives in an unscreened bag. Richard Reid had 10 ounces of plastic explosives.

So let me ask you these questions, if I may, Mr. Parrish. If IAIP received intelligence indicating that there was a credible threat that the terrorist was planning to use the security holes in the cargo screening program to use plastic explosives to blow up a passenger plane, who would IAIP inform?

Mr. PARRISH. Sir, for intelligence received on that information, we work very closely with the Transportation Security Administration with that regard. At the same time, if there is indication of potential smuggling operations to move those materials in across the borders of our country, this information is conveyed to the Customs and Border Protection.

Mr. MARKEY. So would you inform FBI?

Mr. PARRISH. Sir, that would be done in coordination with the FBI. Again, the FBI is represented within IAIP at our headquarters.

Mr. MARKEY. If the CIA receives intelligence about a terrorist threat against a commercial airline using an explosive device in the cargo, who would you inform, Mr. Lago?

Mr. LAGO. Sir, we would use the same mechanism that is set up to inform all members of the community to pass information to the Bureau, to pass information to the Department so they can pass information to the channels that have been established for the necessary individuals to be notified.

Mr. MARKEY. Would you pass it directly to homeland security automatically?

Mr. LAGO. Absolutely.

Mr. MARKEY. If you were instructed by your CIA supervisors not to share that information, what would you do?

Mr. LAGO. Sir, that is a hypothetical. I have never been asked not to share information like that. I imagine if I was, I would share it.

Mr. MARKEY. Mr. McCraw, if the FBI received intelligence about an explosive threat against a commercial airline using an explosive device in the cargo, who would you inform?

Mr. MCCRAW. All involved parties, including homeland security, the Agency, the entire Intelligence Community, and certainly the local and State law enforcement officials in that area that have a vested interest in that geography.

Mr. MARKEY. So you automatically, under the law, have to deliver it directly to Homeland Security?

Mr. MCCRAW. Well, I don't know the law, but from the FBI's standpoint, we are going to, whether the law says we are going to or not. We are absolutely going to. In fact, the example used in such specificity, I can absolutely guarantee you that that information would get out to all those individuals, and under that scenario, probably the head of the airline company as well.

Mr. MARKEY. If IAIP received intelligence about an Al Qaeda potential attack against U.S. nuclear facilities, who would IAIP give that information to?

Mr. PARRISH. That piece of intelligence that comes in would go to the Nuclear Regulatory Commission, which is responsible for the security of the nuclear facilities. At the same time, sir, we would reach out to the private sector within that geographic region. Certainly at the same time all of those communities, if we could narrow down the location, reach out to the governors and the State and local authorities within that region. First would be the Nuclear Regulatory Commission responsible for the security of the nuclear facility to enhance their security posture.

Mr. MARKEY. Would you give it to TTIC as well simultaneously?

Mr. PARRISH. Yes, sir. That information—and that scenario you present would be coming in simultaneously to all those organizations. They would be assessing it at the same time as IA.

Mr. MARKEY. So there would be no additional screening of the information after you were passing it on to the NRC? If the NRC asks you not to pass it on to others until they had time to investigate, would you wait or would you automatically give it to TTIC and to the FBI and to others?

Mr. PARRISH. No, sir. That would be automatic.

Mr. MARKEY. You would give it to the governors automatically even if the NRC said wait?

Mr. PARRISH. No, sir. That would go out to the State and local authorities as well in a timely fashion. The relationship we have with the NRC, I do not see that as a realistic scenario.

Mr. MARKEY. And finally, if I may, on the question of staffers, Mr. McCraw, how many FBI staffers are qualified to administer polygraph tests in Arabic?

Mr. MCCRAW. I don't have that answer for you, but I will find out. Not nearly enough.

Mr. MARKEY. Are we talking about ten or 100?

Mr. MCCRAW. I don't know. I know it is not 100.

Mr. MARKEY. You really don't know the answer to that?

Mr. MCCRAW. I absolutely don't know it.

Mr. MARKEY. How about you, Mr. Lago? How many are trained to conduct those kinds of polygraph tests in Arabic?

Mr. LAGO. Sir, I don't know the answer to that question. We will take it for the record and get back to you.

Mr. MARKEY. And has there been a damage assessment done to determine how costly our failure to collect information from walk-ins and other sources pre9–11 from Arab sources was in protecting Americans from terrorist attacks? Either one of you. Have you guys done an assessment of that, going through the volume of information. I know that a lot of information was never actually translated, and I am just wondering have you done an assessment now in retrospect of how serious that was as a whole in our intelligence gathering that all of that information remained untranslated?

Mr. LAGO. Sir, we will take that for the record.

Mr. MARKEY. Mr. McCraw?

Mr. MCCRAW. Obviously we didn't have enough sources to prevent the act, which clearly that is the basis we do all damage now is prevention of the act, not in terms of what we figured it out after the fact, Mr. Markey.

Mr. MARKEY. You haven't determined after the fact that you actually didn't have enough people who can actually speak Arabic in order to actually read all of the translations or to translate all of the information that was being gathered?

Mr. MCCRAW. As it relates to the translations, that has occurred on that. I thought you meant, more importantly, the walk-ins, whether we had source coverage, whether we have infiltrated the particular cells, and the answer is clearly we know right now we did not.

Mr. MARKEY. Thank you, Mr. Chairman.

Mr. COX. Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman. One of the things that has been always puzzling to me is why we have had such a difficulty coming up with a single consolidated watchlist. I know the General Accounting Office recently issued a report, and they say we have 12 different terrorist watchlists maintained by nine different Federal agencies. If any of you disagree, please advise me, but I think everyone agrees that we should work from one watchlist. But it appears that there is some confusion about who is supposed to be creating this consolidated, single watchlist.

I noted that in July of 2002, the President's national strategy for homeland security stated that the FBI would establish a consolidated terrorist watchlist. Then in February of 2003, the White House issued the fact sheet on the Terrorist Threat Integration Center, and it stated that the center would maintain a database of known and suspected terrorists. And finally, in April of this year, the General Accounting Office report indicated that the Department of Homeland Security had taken the responsibility for creating the consolidated watchlist.

Who among you can tell me who is supposed to create the consolidated watchlist, whose responsibility is it: the FBI, the Terrorist Threat Integration Center, or the Department of Homeland

Security? It seems totally unacceptable that we can't solve what would appear to be a simple problem.

Mr. Parrish, do you want to start?

Mr. PARRISH. Yes, sir. First, there is the term "watchlist," and then the term "database." The multiple databases that existed by the independent agencies—they had those databases based on their mission of their organization. From these databases, then you could produce the watchlists of the names of the individuals that you were looking for or to be aware of.

The Terrorist Threat Integration Center is in the process now of developing the identities tracking database, which will be, if I could I guess, describe as the mother of all databases as we talked about over at TTIC, of integrating all of these databases of the Federal agencies into a single database.

Obviously that is resource-intensive. When you start integrating this to maintain this database, one of the things we learned is that people's names got on lists early on, and there needs to be a mechanism to get their names off once it is proven that individuals are not associated with the terrorist nexus.

But when you take a look at the resources that are out there to bring these databases together, and once that is done, then the concept of a national watchlist center, which is really kind of the switchboard that people would call into to be able to determine if an individual they have in front of them is someone that they need to be concerned about. This will really fall into alignment with the discussion that Mr. Kallstrom is talking about in these regional operation centers that we are talking about.

Using that scenario, when this process is in effect, when that patrolman out there in Lackawanna pulls someone over and calls back into that regional operations center of New York and says, I have in front of me a certain individual by the following name, that center calls into the National Watchlist Center—which currently is under review right now regarding should it reside in the Department of Homeland Security under our umbrella, or is it more appropriate in the FBI, we hope to come to a rapid decision on that in working with the White House. But under that scenario, then this National Watchlist Center would pull that name from this integrated tracking database to say here is the background on this individual.

Now, what that does then is give that patrolman on the street a little bit more information of what he should be looking for. Again, to be consistent with the privacy laws, but he may now be able to take a look and gain a little bit more information about this individual that allows us to take a look at connecting the dots.

So the database, you are right, sir, it requires the integration. We are looking at databases from State Department and TOPOFF. We are looking at Treasury Enforcement Communication Systems and their database and the FBI database. You are exactly right, but I think there is a process in place, and we are moving fast on this to be able to get this up and running.

Mr. TURNER. It just seems to me that in the short term, untilthere is a National Watchlist Center, set up in the manner that you suggested, that there should be some entity that you create that everybody goes to. We should be capable of at least having

having the same terrorists on all the watchlists. And apparently we don't do that. So I am not sure when you talk about the local patrolman on the beat; I guess he goes to the FBI watchlist. I guess that is where he turns, I would assume. I don't know.

Mr. PARRISH. His initial entry point would be—and I will let Mr. McCraw talk about that, but as he goes in, it would be through the national criminal index computer system. You are right.

If I could, even though it seems there is a disparity here with the databases, there are success stories. You all may recall reading in the paper of an individual by the name of Omar Shishani in Detroit, and I will quickly tell you in January of 2002, when the FBI called me from one of the document exploitation centers and said I have a roster here of about 150 names that was found in the terrorist training camp in Kabul, would you be interested in it? And I said, sure. Bring it over.

As we looked at it, very generic names, Al Hindi the Indian, Mohammed the Egyptian, Omar Shishani, the Chechnyan. I said, let's put it in the TECS computer system, the Treasury Enforcement Computer System, with a footnote on the bottom that says, "name associated with terrorist training camp," and as you know how that system works, we then do our advanced passenger information system sweeps on all international flights coming into the United States.

In July of 2000, a flight coming in from Tokyo to Detroit ran through that sweep, and on it appeared Omar Shishani. No date of birth, no passport number, but on the bottom was "name associated with terrorist training camp." An astute Customs inspector pulled him aside in a secondary and opened his suitcase, and we found $12 million of counterfeit checks with an individual who has a long history of association with the Russian Mafia and some of the terrorist activities in Chechnya.

So there are systems that are working in place. You are right, sir, we need to integrate these databases to become more efficient, and I think the plan is in place to make this happen.

Mr. TURNER. I think that is an excellent example of why we need watchlists. You mention Omar Shishani and how putting him on the list resulted in something positive occurring. But, my question would be was Omar Shishani on everybody's watchlist, the 12 different watchlists that are maintained by apparently nine different agencies?

Mr. MCCRAW. Congressman, I can go ahead and try to answer your question. First of all, as important it is to improve it—and there is a plan in place and TTIC is going to play an important part of that plan, the situation is not as bad as it appears on the face. First of all, there is really two actual lists, and everything else are extracts thereof. The no-fly list is an extract of information provided either by the FBI or the intel community that is either maintained in tipoff or vigtoff, which is a file system within NCIC. Is that perfect? No. Clearly there needs to be and they are working towards it, and Mr. Parrish talked about the plans in place for a watchlist center, and I think appropriately briefed you in terms of where we are going.

Tipoff right now will be incorporated into TTIC, and they will take over that particular responsibility. And all of that information

will go into that particular place, and one of the plans in which needs to happen—although the FBI subjects now appear in NCIC for access to over 600,000 state police officers, that information in tipoff is under review that will also be included so that that state police officer has access not just in terms of the FBI subjects, but in terms of the collective wisdom or about bad guys involved in terrorism by the Intelligence Community and the FBI.

Mr. TURNER. Mr. Foresman, you might want to weigh in on this. You are down there at the local level. Where would you call if you were trying to identify someone and wanted to look at a watchlist? Where do you go?

Mr. FORESMAN. Congressman, this is probably a bad day to ask me this question, because we just spent the last week trying to get someone off of a watchlist only to find out it wasn't an FBI watchlist but someone else's watchlist that really wasn't a watchlist, and I think that part of the issue here is definitional in nature and centralizing in nature.

Right now we would probably go to the Joint Terrorism Task Force through the Bureau as the basis for doing that, but I think what is more important is if I have a trooper who is sitting on the Capital Beltway around Washington who stops a vehicle, he has no way to query the system today, and I think when we critically talk about the 700,000 law enforcement personnel, those at the local level, those at the State level, Federal law enforcement personnel, the bottom line is the beat cop on the street is not having access to the information to be able to do a rapid check against it.

And while I understand that we are certainly making progress towards planning for integration, I remain fundamentally concerned we don't understand what we are designing, because we haven't really mapped out the larger strategic picture as of yet.

Mr. TURNER. Thank you. Thank you, Mr. Chairman.

Mr. COX. Ms. McCarthy.

Ms. MCCARTHY. Thank you very much, Mr. Chairman. Thank you very much, panelists, for sharing your thoughts with us once again today.

Mr. COX. Would you yield for just a moment?

Ms. MCCARTHY. Of course.

Mr. COX. I would like to ask unanimous consent to include my opening statement in the record, and I believe you wanted to make a similar request.

Ms. MCCARTHY. I would like to make that request, Mr. Chairman, that my opening remarks be placed in the record as well.

Mr. COX. Does any other member wish to make a similar request?

Mr. TURNER. I will make a similar request, Mr. Chairman.

Mr. COX. Without objection, the opening statements of all members shall be included in the record. Thank you for yielding.

Ms. MCCARTHY. Thank you, Mr. Chairman.

Mr. Foresman, I very much appreciate your experience at the local and State level, and I testify there is confusion in the movement of information from the Federal Government to the State and the local level, and I wondered if you could share some examples with us and ideas on what needs to be done to clear that up. I know from my own experience with local responders, they are expe-

riencing that in Missouri as well. And I know, Mr. Parrish, based on your testimony and your comments yesterday, and today that you are very sensitive to this need, but the sources aren't quite there yet to enable the training and other things that need to go on.

But Mr. Foresman, if you would speak to that. I know in your testimony you indicated there does not appear to be any overall Federal vision and coherent plan across the entire Federal Government that articulates exactly what we are trying to accomplish in terms of information and intelligence fusion, analysis and sharing, especially related to the involvement of State and local governments.

How should the Department of Homeland Security and TTIC and any other agency optimize information sharing? Because I am quite concerned and agree with all of you that the people who are going to carry this out are at the State and local level. The knowledge is here in Washington, but the people on the front lines, those homeland security police and fire and ambulance drivers and others are out there all over America. And how best do we get the information to them that they need so they can do the job when called upon?

Mr. FORESMAN. Well, I will come back and do the two examples last and maybe address the latter part of your question first with your indulgence.

I think this is very much an issue of empowering the Department of Homeland Security with clear authority and responsibility for bringing all the relevant stakeholders to the table in crafting a national vision, one that includes all those Federal agencies with component pieces in the intelligence enterprise as well as the local stakeholders and the relevant private sector partners.

There have been a plethora of efforts, both through the Bureau, through the Central Intelligence Agency and through the Department of Homeland Security, but they still lack that overarching strategic national focus, and I think very much so that whether it is the Department of Homeland Security or any other Federal agency, we very much need to lock ourselves in the room and actually as we talked about earlier, about another 3 hours' worth of break and we may have solved about everything here today.

But I think it is critically important that we sit in the room and define expectations, do the education, define the business rules for sharing information that allows the Bureau to protect that information that it feels like it needs to protect, the Agency, State and local governments. There is certain information that State and local governments have that should, because of the provisions of Congress, not be warehouseable at the Federal level. And we all recognize all those things, but we have not sat everybody down and created that vertical and horizontal picture in the most macro of sense.

The specific examples I would cite, I would like to go back to the fact that we are very much early in this process of this post September 11th environment, but I still—and the challenge—I have a great deal of faith in the people sitting at this table, whether it is my counterparts in Arizona or New York or the Federal agencies that we work with, but remember, I am just one person and I have

to work with a plethora of local officials, whether they are law enforcement, public health, I have to work with elected officials.

The two examples that come to mind is the Department of Homeland Security in advance of operation Iraqi Freedom was quite active in providing threat information to all of the States and specific threat information to the Commonwealth of Virginia. They provided that information in rapid fashion and form, and when we attempted to do that level of local level collaboration as we brought our local stakeholders to the table, I will tell you that the level of zeal of security of certain sites was not necessarily represented in the field agents of the various Federal agencies in the affected area, and so we were faced with the conundrum and a legitimate conundrum of a police chief saying what do they know in Richmond that the field offices don't know, or what do they know in Washington and so what is the quality of the intelligence.

A second example actually goes back prior to that when we had some credible information that we were dealing with with regard to the Commonwealth of Virginia and to DHS's credit, they went to great pains to get that information to us rapidly and succinctly. They were good about making sure that all those folks that need to be briefed were briefed.

The problem end is again that there was good agreement between the principals, i.e., those folks who now make up the TTIC, the Bureau, headquarters in DHS, headquarters offices about the information; but, again, when it went down to the field, the response that we got from the field personnel was that this is old information. This has already been vetted. We sent it to Washington. Someone got excited about something that they shouldn't have gotten excited about.

Well, from my standpoint, I am left with the challenge of articulating to a governor and to local officials is this credible quality information that you should act upon and do certain measures? I think in large part, those were early incidentals in this process, and things are beginning to improve, but just as we talked about a number of regional initiatives across the northeast, things that we are doing in Virginia, things that are going on within Federal agencies, who is the air traffic controller for all of these different things, and how are we making sure that we are making this whole effort operate in harmony and in a synchronized fashion?

Mr. PARRISH. If I could just add, one of the things, an initiative of Under Secretary Libutti is we need to go out and hear from our customer base in a follow-up to Congressman Markey's scenarios that he presented. For example, I know that you have interest with regard to water supplies. On June 23rd, we put out an extensive threat advisory to all States with regard to water safety—water supply threats with some protective measures on what they should be looking for to handle that.

It will be valuable for us to get the feedback from Mr. Foresman's office, how did the Commonwealth—how do they use that? Was it valuable to them? Was it a good product? What else, additional information?

To Congressman Markey's scenarios, as I mentioned it had other day, the morning following the attack on Riyadh as I was sitting at TTIC looking at the sensitive intelligence traffic going back to

TTIC and to the CIA, I said I needed a downgraded product at the unclassified level. IA began writing protective measures against this new tactic and technique employed by Al Qaeda in those attacks.

Again, a lengthy document that assessed and analyzed the actual tactics and techniques employed against an installation, breaking through the fence, assault teams coming in, we took that intelligence, got it unclassified the same day, and we put out a product that gave protective measures to State, local and private sectors on things they should consider in enhancing their security posture.

So we put products out there like that to the State and locals, but we need feedback to see if that is relevant to them, is it useful to them. So, again, it is an initiative of the Under Secretary. We are going to get out there and find out exactly has needed.

Ms. MCCARTHY. Anyone else wish to comment? I thank you, Mr. Chairman, and I thank the panel.

Mr. COX. Thank you. I want to take the opportunity, Mr. Kallstrom, to ask you prospectively about how the Counterterrorism Center that you describe in your testimony might operate when it opens in August and thereafter.

Specifically we heard from Mr. Lago that a CIA source is an IT solution that deliberates finished intelligence products. Is this something that you would expect to take advantage of at that center?

Mr. KALLSTROM. Sir, I think we would see the center as sort of the filter or the go-between between all the collaborative agencies in Washington and internationally, for that matter. To the myriad of people in the State, probably the law enforcement people first, and then there is obviously other people that need to know things. And we would be in a position at that center, because we would have trained the people, they would have the proper clearances—and I must just divert and tell you something in my view of 28 years in the FBI, I see virtually no reason for but a handful of people in any State to have a top secret clearance, by the way, because the only reason it is top secret is the information is not anything that anyone needs to know. It is—secret is adequate. But the center would then take the information through collaborative efforts between the people in the center in Washington, discussions, phone discussions, summary reports, different types of intelligence that is put out periodically, and we would then put that into real words and real action for the cops in a different form to educate them as to what they should be looking for, what indications might be, what warnings might be so that their eyes and ears work better. That is one thing.

The second thing is a point someone made here earlier, I think the gentleman from Texas. A police officer is someone on the side of the road that for whatever reason his level of suspicion is raised. Maybe there is a hidden NCIC, but maybe just because he presents some documentation that looks a little strange or maybe this thing is in plain view or whatever the reason, that police officer just radios in to the center in New York who has connectivity with Washington and says, I have this guy and maybe there is a code word for an all sources check, please give a check on that, and then instantaneously within minutes, you know, our people in New York

who are sort of an extension of Homeland Security/FBI/CIA, are looking at databases to see if this person is of any interest. And then the center and Washington together craft what we want that officer to do without divulging the sensitive information. Hold the guy? Let him go? Delay him? You know, whatever it is, make note of whatever is in plain view, blah, blah, blah. And that is how we see the process working.

The other point I want to make is I think it is imperative on the part of all of us, particularly in Washington, to break this issue of the protection of us as a people into two categories. Category one, those things we need to do to stop the next event, to not have another event happen on the soil of this country or against American interests elsewhere. Number two, if it does happen, clean up the mess. And those things obviously we have to be prepared. Our first responders need the right equipment. We need the right protocols. They need information. But it is critically important to do a dozen things—maybe it is 14. Maybe it is 10—to add the State and local resources to this problem, this challenge of not having another event happen, and I think we can easily do it, ladies and gentlemen. I think we can do it. I think we need to focus on it, though, and not combine all this stuff into one big pot and call it homeland security. I think we have to talk about those issues we do to stop the event and those issues we do to mitigate if an event happens. I think we would have clearer direction and clearer solutions to it if we looked at it that simple way.

Mr. COX. Well, I couldn't agree with you more on that point.

Mr. Lago, when you described a CIA source in your testimony, you had reference to sharing with DHS. Is that system something that on a classified or unclassified basis State and local governments can tap into?

Mr. LAGO. Today, no. We have nothing in place today. There are some issues that you would have to work, you will have to work on, on getting the CIA process that close with the State and local processes, but as Mr. Kallstrom said—and I think I would echo that—the first thing you need is to be able to translate the needs, the requirements needs on both sides. We could put a box out there and we could give a person a couple weeks training, but I would suggest that it has taken—it probably takes us 4 to 6 years to train an analyst to be proficient in doing the modeling and using the tool to the best of their ability. We have tried to come and work our way around that relationship. We have deployed a CIA officer to New York. We are fairly proud of the information flow that has gone both ways because of that. It clearly has given us more insight into their specific requirements. And quite frankly, we spoke different languages when we started this relationship, today we have an individual to help translate.

Now, does that mean to say that we couldn't put some kind of a system in that would allow them the access to those things or maybe send an analyst to help them? There are other ways of doing it. But I am not sure that just sending a system to them would help most of the States.

Does that answer your question?

Mr. COX. Well, it certainly raises an important aspect of the question, which is that there is judgment involved in determining

what is reasonably likely to require onward passage to State, local, and so on, law enforcement and intelligence.

The MOU obviously contemplates this and states that information that is classified or otherwise subjected to restricted dissemination but which reasonably appears likely to require onward passage to State, local or private sector officials, the public or other law enforcement officials goes to DHS with accompanying high-content tear lines suitable for onward passage at the unclassified level. That would certainly—and run a lot of the tougher problems that we have just been talking about.

And the question is whether there is an IT solution to that or whether this—how is this being done? Is it being done literally with tear lines where pieces of paper are being faxed, or how does this work?

Mr. PARRISH. Sir, if I could on the access, the CIA source, CT link, some of those systems, IA has access to that with our analysts. As I say, we go into those systems daily. We receive that information. We analyze those pieces of intelligence to say what do I have here and who needs to know it, what State and local authorities need this, is this regionally oriented to the Northeast sector? Do we need to get that to California?

We then go back in through the process to get that tear line if required, and then that information is provided to us. Now, oftentimes we will go back and say we need more information, that this tear line does not meet the needs of our constituents, and we have had success with that with the CIA to go back and get that.

Then—and going back to the concept of RISSNET as we implement this, this will be a secure Internet system not at the classified level but it will be password protected. We envision this to be posted on a Web site or we will send it directly via e-mail up to that operations center in New York to convey this information to them.

So that is our job. That is our mission in IA to make sure that we are pushing the IC, the Intelligence Community for every piece of information that is there that is classified sensitive at a level that we deem essential to get out into the hands of the State and locals, and right now the system is working. We are working it with TTIC, reaching back through CTC, and I am here to say that so far, Parrish has never been told no.

Mr. COX. Mr. Kallstrom.

Mr. KALLSTROM. If I can just add one thought to close the loop on it. You know, I think we have a very good vehicle in place now to stop the next attack, and that is the terrorist task forces that comprise all the Federal agencies and some select State and local police. There is just not enough people on these task forces to know what they don't know, and the missing piece as we talked about earlier I think before you came in was we need to find a way from the—I am talking about prevention now. We need to find a way to let State and local resources be more effective eyes and ears for those task forces so we can broaden their knowledge base of what is going on in our communities, our towns, our neighborhoods, you know, some little town up on the northern border where maybe some terrorists are living. The targets may be in New York. They may be in Washington. They may be a few other places. The terrorists aren't necessarily there.

So I think we will go a long way. I think the Federal Government appears to be fairly well coordinated now. We have got problems with these watch lists. We have got problems with computers, but if we can figure out a way of harnessing the State and local assets, the law enforcement assets and other assets to be more effective lookouts, watchdogs or listening posts for the task forces we already have, I think we will make a geometric leap in the ability to protect our society.

Mr. COX. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. If I could, another question for Mr. Parrish. I have to admit that many of us I think were surprised when the TTIC was created, because I think many of us had expected and wanted to have that type of an entity, that function performed by the Information Analysis Directorate, but at this point I think many of us are just withholding judgment as to whether that is going to work and we will take a wait and see attitude.

I am concerned, though, and just want to touch on the topic of the type of information again that you are receiving, and I know this has been discussed, but I want to look at it again. Are you receiving the raw intelligence or mainly the analyzed product? And if you are receiving analyzed product rather than the raw intelligence, are you concerned that something might be missed that you would have picked up on had your analysts looked at—had direct access to the raw intelligence? And do you feel that the TTIC analysts are looking for the same things that you would be at the Information Analysis Directorate?

Mr. PARRISH. Yes, sir, and I recognize your concern. First, again, as we mentioned the other day, is that we are a part of TTIC, the Department of Homeland Security. IAIP is a partnership with TTIC. We have Department of Homeland Security analysts, the IAIP analysts working in TTIC that come there with an operational understanding, I should say—or rather, an understanding of the operational environment of the Department of Homeland Security. A TSA analyst is located there. A Customs and Border Protection analyst is there, and Immigration and Customs Enforcement.

So they are looking at all of that raw intelligence, all of that information that is filtering through TTIC that is coming from the entire Intelligence Community, looking at it through the lenses of what is relevant to the Department of Homeland Security from the standpoint of what is needed for the State and local and private sector.

We are also receiving that information within IA, and we do conduct independent assessments on that intelligence to identify if in fact there are credible threats that we need to get out to the private sector, which is State and local.

Mr. LANGEVIN. The raw intelligence as well as analyzed intelligence?

Mr. PARRISH. Yes, sir. Again as I said the other day, you know what you know. I know that we are getting reports. Again, I have analysts from those agencies of the IC that have access to their systems within IAIP, members of the NSA, from the CIA. So at this point in time, I think your assessment is right, is that TTIC is a force multiplier right now. It is doing what the administration

intended. At the same time IAIP is certainly in compliance with those 19 functions of the Homeland Security Act, of which we are charged.

Mr. LANGEVIN. Well, thank you. We will be monitoring its progress, and I certainly would hope that you will share with this committee if you have concerns that that arrangement is not working.

Mr. PARRISH. Sir, if it is not working, I will be right back here to tell you.

Mr. LANGEVIN. I yield back. Thank you.

Ms. MCCARTHY. [Presiding] the Chair recognizes Mr. Markey.

Mr. MARKEY. Thank you. Thank the Chair very much. Back to you, Mr. Lago, if I could. Back in October 7th, 3 days before the Congress voted on the resolution authorizing the President to go to the UN and then to use force if necessary, the President said in that speech to the American people and to the Congress at that time—he said that—he said, we have learned that Iraq has trained Al Qaeda members in bomb making and poisons and deadly gases and we know that after September 11th Saddam Hussein's regime gleefully celebrated the terrorist attack on America. Iraq could decide on any given day to provide a biological or chemical weapon to a terrorist group or individual terrorists. Alliance with terrorists could allow the Iraq regime to attack America without ever leaving fingerprints.

Then in the State of the Union Address that the President delivered this year, which laid out the case for why we might have to go to war against Saddam Hussein, the President said to the American people as he was concluding the State of the Union address, he says, evidence from intelligence sources, secret communications and statements by people now in custody reveal that Saddam Hussein aids and protects terrorists, including members of Al Qaeda; secretly and without fingerprints he could provide one of his weapons to terrorists or help them develop their own.

I am continuing the President's State of the Union Address. This is how he is concluding now. Before September 11th, many in the world believed that Saddam Hussein could be contained, but chemical agents, lethal viruses and shadowy terrorist networks are not easily contained. Imagine those 19 hijackers with other weapons and other plans, at this time armed by Saddam Hussein. It would take only one vial, one canister, one crate slipped into this country to bring a day of horror like none we have ever known. We will do everything in our power to make sure that that day never comes.

Now, we know that on Friday a senior White House official—and we know who that is. We just won't say his name. We know he doesn't want his name mentioned—said that in response to the questions about the National Intelligence Estimate that was revealed on Friday that he publicly released, showed that—and I will read this now from the National Intelligence Estimate: Saddam if sufficiently desperate might decide that only an organization such as al Qaeda, already engaged in a life or death struggle against the United States, could perpetrate the type of terrorist attack that he would hope to conduct. It went on to say that Hussein might decide to take the extreme step of assisting al Qaeda in a terrorist attack

against the United States if it, quote, would be his last chance to exact vengeance or by taking a large number of victims with him.

So thus far the intelligence assessment that Hussein might be a potentially bigger threat now than before the United States attacked has yet to be retracted if he wasn't captured and if these materials went into the hands of al Qaeda.

That being the case, Mr. Lago, again, it is hard for me to understand why a warning hasn't been passed on to Mr. Daniels, Mr. Foresman and others to be on high alert, given the fact that al Qaeda has not been yet captured in that country and the materials are at large, none of them have yet been identified. Can you explain to me why we are not now giving warnings that reflect the National Intelligence Estimate that was used by the President both on October 7th and in the State of the Union as a justification for me?

I voted for that resolution, Mr. Lago. So I was relying on the President's holding out. So why isn't it now being communicated to the public that this risk is real, since we haven't identified either al Qaeda or the terrorists which the CIA said was there?

Mr. Lago.

Mr. LAGO. Congressman, again, we do not have specific threat information. If we were to give warnings on every piece of general information that we have, we would be warning people 24 hours a day, 7 days a week. We need specific actionable information to put out those warnings. We don't want to be in a position of spooking people, and we do that without specific actionable intelligence.

Mr. MARKEY. I understand what you are saying, but doesn't this intelligence reflect a greatly heightened sense of concern which we should have? Now we have—the basic intelligence said he is more dangerous if we attack in terms of these materials, and he feels desperate, which obviously he does, and these materials would then be much more likely to be put into the hands of al Qaeda and other terrorist groups.

Mr. LAGO. Congressman, again, to warn—we are at an elevated level of warning today. To warn specific events, we have to have actionable intelligence. We do not have specific actionable intelligence.

Mr. MARKEY. Mr. Kallstrom.

Mr. KALLSTROM. I can only speak from New York State, but we are at a high level of alert. New York City is still at Orange. We have done numerous things throughout the State, which I don't want to discuss here, but involving sensors, involving special precautions around special sites. So Congressman, we actually are, and just before we went into Iraq, we went up to Orange, as I am sure you remember.

In the New York State, we really have not come down much from that from the standpoint of the potential of somebody actually doing that, so we have taken it very, very seriously, and we continue to.

Mr. MARKEY. See, the problem that I have, Mr. Kallstrom, is this, is that I agree with this conclusion, and of course the reason that I voted for the resolution was that I am from Boston. They took over the two planes in Boston. It was Bostonians who were on those two planes, and now the Bush administration is opposing

any attempts to screen cargo that comes onto planes coming out of Logan Airport, and if this biological or chemical or nuclear material tied to an explosive is out there at heightened risk and the administration is still opposing the screening of cargo going onto passenger planes, then that means that the entire intelligence assessment before October 10th, when we voted here in Congress, was wrong and that the information the President was communicating in the State of the Union was in fact wrong.

Then the question is was it knowingly wrong, or was it just very bad information which the President was relying upon? But I know that people in my district are still relying upon these representations by the President based upon CIA and other intelligence agencies, but you can't have it both ways. You can't say that it is a greater risk and then at the same time you are saying the very planes that the President said would be at greater threat if 19 terrorists had these greater weapons aren't going to screen the cargo that is going on passenger planes. You can't have it both ways. It is either one or the other, and the very fact that you don't have the specific threat yet doesn't mean that there isn't a plan in place.

You know, we still haven't found anybody in Boston helping those terrorists that killed all those people from my district. They haven't found anybody even helping them yet. So wouldn't it be wise for us, Mr. Lago, to take the precaution of screening all cargo that goes on planes that have passengers on them in the United States given the President's representation?

Mr. LAGO. Congressman Markey, I am not an expert in that area. I do think it is wise for us to be at the elevated state of alert. I do think it is wise for us all to take precautions. Again, if we don't have specific actionable information—.

Mr. MARKEY. I understand that, but I am saying to you—.

Mr. COX. [Presiding.] The gentleman's time has expired, but let him answer the question.

Mr. LAGO. There is—.

Mr. MARKEY. —if you wait until that point in time, you are going to have a recurrence of September 11th in Boston, okay. That is all I am saying to you. They will put the cargo on the same planes, maybe with the same number on the flight and send it off. We don't screen cargo for biological, chemical or nuclear materials that would go on in the cargo to find an explosive.

Mr. LAGO. Sir, again, that is out of the scope of my expertise—we don't screen domestic cargo at the CIA, sir. I can't answer that question.

Mr. MARKEY. I understand, but I think your analysis before that the President relied upon is either accurate or inaccurate. I hope the President used accurate information. If he did, there is a natural consequence of that to passengers on domestic planes.

Mr. COX. Mr.Turner.

Mr. TURNER. Thank you, Mr. Chairman. Mr. Parrish, you have been with us several times. You know where the sentiment of this committee is with regard to the role that the new department should play in information, collection and analysis. I think it is fair to say, at least on the part of the chairman and I, that we have a view based on the reading of the Homeland Security Act that your role is very broad, and I certainly appreciate the fact that we

are at a somewhat early stage in the evolution of these relationship. I am glad when I hear Mr. Kallstrom talking about the relationship that he has with the Department. It is based on in many cases longtime friendships with Mr. Libutti, and those kinds of things are important. But with a country as large as we have, we have got to create a system that works for everybody, including Mr. Foresman. I see him shaking his head down there.

And I guess what I hope is that at some point we will be able to arrive at such a system, and I hope it is sooner rather than later, because I think it is important to our security.

Just a minute ago I was listening to you talk about your relationship to teinnst the threat integration center. You said we have analysts there, and of course when I hear that—and I think my chairman shares this view—I mean, we think maybe those analysts are supposed to be at your shop and what is happening in terms of information flow at TTIC is supposed to be coming to your shop at DHS.

You made a comment that you are pushing the agencies for every bit of information when the Homeland Security Act by its very words really shouldn't require you to have to push anybody for information. The statute says you are to get it whether you ask for it or not, and you said a moment ago that when you have made these requests you have never been told no. Under the Homeland Security Act, nobody has the right to ever tell you no, and so I think that we can get there. If somebody says no, no, we went down the wrong road, the Congress passed this legislation, and it gave you this authority, but that was a mistake, then I hope at some point somebody would come to us and say we need to change the law. Because we all come to this table from different perspectives, and many of you have worked on behalf of the people of America for many, many years and you do an outstanding job. We like to think that we come to this table with the same motivation, and our job is oversight, and our job is to read the statute that we pass and see if it is being complied with. I guess many of the frustrations that we probably exchange back and forth relates to that different perspective, because I know each of you are doing the very best you can to get to the desired goal, and that is making America more secure. But I hope you will work with us, because if what we put in the statute is wrong, we need to hear that from you as well. I would welcome your comment with respect to that if you feel I am off base with regard to that observation, I would welcome it now.

Mr. PARRISH. No, sir. I do not think you are off base. As I said the day before yesterday, it is not a push-pull system at this point. It is still a pull system, but I am telling you that it is working and it is getting much better. In my short tenure as the Acting Assistant Secretary, I have received phone calls from members of the Intelligence Community that have said I need to make sure that you got this message.

Again, we are standing up. Some of the IT connectivity is not there. We have the work-around because we have representatives from the other communities. I can tell you that I worked very late last night on some things, and the system was working very well,

and it continued to work this morning when I got back into work at 6 o'clock to follow up on where we ended last night.

Let the record show, sir, that when I am told no and if I ever am told no, I will be back to this committee to let you know that I was told no. The law is very clear. Under Secretary Libutti has made that very clear to his counterparts within the Intelligence Community, but at this point in time I have to admit I have seen nothing but cooperation from—again, there are personalities involved in this, and I have established some strong relationships with senior leadership in the FBI, senior leadership at the CIA, at the National Security Agency and other agencies which I meet with on a weekly basis, and the system is working right now.

I think the legislation that this Congress passed is on target. I think the list of the 19 functions of which we are held responsible for, we are implementing those functions, and I think that legislation as it is written right now is going to be the things that Mr. Kallstrom has alluded to in the preventive measures to stop a terrorist attack.

Mr. TURNER. Well, let me thank all of you for your patience with us today and for your time. I know it has been a long day. You had to wait for us to go through a series of votes, and we had lengthy questions, even though perhaps we haven't been as well attended in the subcommittee as the panel has, but you have been very generous with your answers to our questions. And, again, each of us greatly appreciates your dedication to our country, your deep sense of patriotism and your devotion to the task that we know is important to the future of the country.

Thank you so much.

Mr. COX. Thank you. I want to join my ranking member in thanking each of you, Mr. Daniels, Mr. Foresman, Mr. Kallstrom, Mr. McCraw, Mr. Lago, Mr. Parrish, for your extended duty today. We have benefitted greatly, not only from the time and the resources that you have committed to this hearing but from the fact that you have been here together so that we could learn jointly from your presentation.

I think you have inferred from our questions today that the kind of commitment, the full commitment to information sharing that Congress intended in the Homeland Security Act, in our view at least, requires enormous changes in the way the government at all levels does its business, and it may require, for example, that agencies be willing to give up ownership and control of information that they generate and through IT permit not only sharing that information but also its augmentation by government at all levels in a networked environment.

These are things that are under construction. It is work in progress. It is a new way of looking at the world, but I think that protecting the American people from attack necessitates these things in this if not strange new world in which we live, difficult new world in which we live. So what you are doing seems to be exactly the right thing. The fact that you are doing it together is more important still.

We are going to cut you loose. We know some of you have to go, and, again, thank you very much for your extended stay today. It

has been enormously beneficial to this committee. This hearing is adjourned.

[Whereupon, at 6:32 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS AND RESPONSES FOR THE RECORD

RESPONSES TO QUESTIONS FOR THE RECORD BY WILLAM PARRISH, ACTING ASSISTANT SECRETARY FOR INFORMATION ANALYSIS, DEPARTMENT OF HOMELAND SECURITY FROM THE SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM HEARING TITLED "IMPROVEMENTS TO DEPARTMENT OF HOMELAND SECURITY INFORMATION SHARING CAPABILITIES" HELD ON JULY 24, 2003

Status of Information Analysis Office

Section 201 of the Homeland Security Act requires the Information Analysis and Infrastructure Protection (IAIP) Directorate to disseminate information analyzed by the Department within the Department, to other Federal government agencies, state and local governments, and the private sector, in order to assist in the prevention of, or response to, terrorist attacks against the United States.

Question: **1. How many products, and what types of products, has IAIP disseminated to other parts of the Department as of today? To other federal government agencies? To state and local governments? To the private sector? Do you consider this number to be adequate? If not, when will you be able to disseminate the desired number of products?**

Response: Information Analysis and Infrastructure Protection has disseminated 46 products to other federal government agencies, 48 to state and local governments, and 41 to the private sector. Procedure dictates that a draft of a bulletin or advisory is vetted through twelve internal DHS divisions, as well as through outside sources, for approval. Once the product has been vetted, it is then disseminated to DHS. At no point has the necessary information or a needed product not been distributed. The figures above, therefore, accurately represent the number desired.

Question: **2. How frequently does IAIP disseminate intelligence products? Can you give some examples of the products? Will you provide them to the Subcommittee?**

Response: The Homeland Security Information Summary (HSIS) is briefed and distributed electronically daily to DHS leadership and component intelligence chiefs, as well as to selected members of the intelligence community. Additionally, IAIP compiles the information received from DHS operational elements into the Homeland Security Intelligence Report (HSIR) or into a restricted version (the HSIR–R). IAIP also produces a Spot Report in advance of the daily report when it is necessary to begin processing critical material immediately. Lastly, IAIP produces the Secretary's Morning Brief, a daily compilation of in-depth analytical perspectives on significant recent, and developing, issues affecting homeland security and DHS. Although some products have been provided to Congress in the past, DHS, Office of Legislative Affairs is developing a more formal and automatic process to pass appropriate level products to a variety of committees in Congress. These products will be provided to the Committee as appropriate to their level of classification.

Terrorist Threat Integration Center (TTIC)

During the joint hearing held on Tuesday on the Terrorist Threat Integration Center, you testified that you hope to have about 150 analysts in your office by next year. Mr. Brennan, the Director of TTIC, testified that TTIC will have about 300 analysts when fully staffed.

Question: **3. Will 150 analysts be adequate to carry out all the missions of the Information Analysis office? How did you determine what the correct number should be? How does that mission compare to the Terrorist Threat Integration Center, which will have 300 analysts when fully staffed? If TTIC will have 300, how can IA only have 150 in light of its broad mission?**

Response: Yes. One hundred and fifty analysts is an adequate number to carry out the missions of Information Analysis. The number was determined by Information Analysis Division Chiefs based on years of experience in the Intelligence Community. The missions of TTIC and Information Analysis differ in that IA deals only in intelligence that involves threats to the Homeland. TTIC deals in all threat-related information and therefore has more information flowing in on a daily basis.

Information Analysis also has the added benefit of analysts in other DHS component entities that pass threat-related information to IA.

At the hearing on TTIC on July 22, Mr. Brennan testified that an agency, such as the CIA, that has threat information provides it to both TTIC and the Information Analysis office of DHS simultaneously.

Question: **4. Can you explain what happens at that point? What does your office do with the information that is distinct from what TTIC does?**
Response: Information that comes into Information Analysis is independently analyzed and assembled with all domestic threat-related information flowing into the Department. This information is matched with known capabilities and vulnerabilities to produce an overall threat picture that allows IA to issue warning products to other federal government agencies, state and local governments and the private sector. TTIC receives all domestic and international threat-related information and sends reports to IA regarding domestically relevant intelligence, particularly to support its critical infrastructure protection responsibilities. TTIC does not communicate with anyone outside of the Intelligence Community.

Question: **5. After TTIC and the Information Analysis office both process the information, what happens then? What is the "output" of the Information Analysis office? Who receives this output? How is it different from what the TTIC would do with the same information?**
Response: The "output" of the Information Analysis office is the afore-mentioned warning and intelligence products, based on information from DHS entities and members of the Intelligence Community. IA differs from TTIC in that all IA products deal solely in threats to the Homeland while TTIC deals in the overall threat picture. IA delivers its "output" to other federal government agencies, state and local governments and the private sector. TTIC does not communicate with the public.

Responsibilities of the Information Analysis Office

The Information Analysis office, in particular its Information & Warnings Division, is responsible for administering the Homeland Security Advisory System. Many state and local officials have complained that there is little guidance accompanying changes in the threat level.

Question: **6. Can you describe, specifically, what guidance the Information Analysis office provided to state and local officials during the recent changes in the threat level form yellow to orange and back to yellow? Did the office recommend that state and local officials take any specific actions other than be at a higher state of alert?**
Response: When the threat level was changed from yellow to orange on May 20, 2003, specific protective measures were included in the Advisory that was widely disseminated. Upon deciding to lower the alert level back to yellow on May 30, 2003, DHS/IAIP distributed a product that included an overview of the existing situation and suggested that those receiving the product maintain surveillance of critical locations, assess emergency plans, and provide a visible presence as a viable form of deterrence. The report detailed such actions as the use of random or rolling patrol operations and encouraged individuals to report information concerning suspicious or criminal activity to law enforcement. Specific suggestions regarding what type of threat exists, recommended increased security measures, and as many details regarding suspicious activity as can be reported continue to be included in products issued by IA.

Question: **7. Who do you believe your "customers" are? Do you intend to develop intelligence products tailored to each type of "customer" of the Information Analysis office?**
Response: Information Analysis is dedicated to sharing information with the Intelligence Community, TTIC, DHS entities, and to serving other federal government agencies, state and local governments and the private sector as is relevant. Information Analysis, through these bodies and through its cooperation with other DHS entities, consequently serves the public at large.

Question: **8. Have you met with the officials and agencies that are your "customers" to determine what information they need from your office and in what form?**
Response: Information Analysis receives feedback on its communication with its "customers" through a variety of channels. The State and Local and Private Sector Directorates within the Department of Homeland Security convey the feedback they

receive from their components and IA is in regular communication with the federal government agencies and Intelligence Community members it works with.

In your testimony, you discussed that DHS has operational personnel, such as Border Patrol and Customs inspectors, who are in positions to collect information that could be useful to the rest of the Department and the government as a whole.

Question: **9. What systems are in place for regular reporting from those on the front lines to IAIP? Do the personnel on the front lines know what they should report? Can you give some examples of information that has been collected by Border Patrol or Customs that has been reported to IAIP and shared with other agencies?**

Response: The operational personnel within DHS entities such as Border and Transportation Security operate through their own intelligence components. IA receives threat information from these components. Personnel on the front lines diligently observe and report intelligence and threat-related information such as suspicious activity at the nation's borders and suspect names discovered through daily activity.

You testified that there is work being done on a national watchlist center, and that there has not been a final decision on whether it would be at the Department or the FBI.

Question: **10. What is the time line for this process? When will the national watchlist be in place? What agencies are working on the problem?**

The Terrorist Screening Center, now in existence, is a central point at which the Terrorist Screening Database (TSDB) will be consolidated and administered. TSC operations were phased in and became operational 1 December 2003. The TSC, a multi-agency effort, involves the expertise of the FBI, DHS, and State Department.

RESPONSES TO QUESTIONS FROM STEVEN C. MCCRAW, ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

1. The FBI has been criticized in the past for its unwillingness to share information. The March, 2003 Memorandum of Understanding between the Attorney General, the Director of Central Intelligence and the Secretary of Homeland Security provides that the FBI is to provide Electronic Communications (ECs) and interview summaries known as "302s"?

Question: **Is the FBI currently providing ECs and 302s to the Department of Homeland Security? If not, why not?**

Response: The Federal Bureau of Investigation (FBI) is sharing a very large amount of information and intelligence with the Department of Homeland Security (DHS), primarily through electronic cable message traffic. The FBI also provides information and intelligence through Electronic Communications (BCs) and FD–302s when these documents can independently fulfill a Request for Information (RFI) without revealing protected sources or methods. In either instance, the intelligence contained in FBI documents/ communications is made available to DHS, as provided for in the Memorandum of Understanding (MOU). To further assist in the flow of information, two FBI Supervisory Special Agents have been posted to DHS since April 2003.

Due to the internal structure of DHS, a determination was made to create two parallel RFI channels to ensure the proper sharing of information. The first channel was the RFI process for "emergent threat" information. Because of the time sensitivity of this type of RFI, the system calls for direct connectivity between the DHS Homeland Security Operations Center (HSOC) and the FBI Counterterrorism Watch. The majority of these RFIs are either by telephone or by facsimile. The HSOC now assigns a tracking number to all RFIs.

The Director of the HSOC has initiated a program whereby a DHS Senior Watch Officer (SWO) is detailed to the Counterterrorism Watch on a 90-day rotating basis. The SWO educates the Counterterrorism Watch on the mission and needs of the HSOC and, by learning how the Counterterrorism Watch defines and manages emergent threat matters, is additionally able to serve as the "eyes and ears" of the HSOC.

The second channel of information sharing is the method by which all requests for nonemergent (i.e., routine) information, such as investigative updates and analytical products, are processed. Procedurally, these requests are collected and sent via cable from the DHS Information Management and Requirements Division (IMRD) to FBI

Headquarters (FBIHQ), where they are received by the Executive Staff of the Counterterrorism Division. Responses are sent by FBIHQ via cable back to IMRD for dissemination to the request's originator.

In addition to these RFI processes, information sharing initiatives have included numerous briefings and meetings both at DHS and the FBI, including weekly Intelligence briefings at the FBI's Strategic Information and Operations Center where DHS selects the topic to be covered and the FBI's Counterterrorism Division provides the briefer. The FBI provides to DHS virtually all of its terrorism analytical products that are disseminated externally.

2. The same Memorandum of Understanding indicates that the TTIC and the FBI's Joint Terrorism Task Forces (JTTFs) will have a role in the information sharing.

Question: **Can you explain what the current roles of TTIC and JTTFs are? Does the FBI share information directly with the Department of Homeland Security, or only through the TTIC and JTTFs?**

Response: The mission of the Terrorist Threat Integration Center (TTIC) is to enable full integration of terrorist threat information and analysis. It is a multi-agency joint venture that integrates and analyzes terrorist threat-related information collected domestically and abroad, and disseminates information and analysis to appropriate recipients. TTIC sponsors a website that increasingly includes products tailored to the needs of state and local officials and private industry, so that DHS and the FBI (who are the designated conduits of information to these entities) can readily pass this information along.

The 84 Joint Terrorism Task Forces (JTTFs) are the United States Government's primary counterterrorism operational entities throughout the United States. The JTTFs team FBI Agents with state and local law enforcement officials, as well as representatives of DHS and other federal agencies, to coordinate counterterrorism investigations and share information. The JTTFs investigate and follow up operationally on leads provided by the Foreign Terrorist Tracking Task Force, the FBI, and other intelligence agencies. The JTTFs also serve as conduits of state and local law enforcement information to the FBI.

In accordance with the Homeland Security Act of November 2002 and other statutory requirements and interagency agreements, the FBI furnishes information directly to the Department of Homeland Security, as discussed in response to Question 1.

3. Your office in the FBI is a new one, and was created as a response to the criticism of the FBI's weaknesses in analysis.

Question: **Can you explain the role of your office in relation to the Information Analysis and Infrastructure Protection Directorate of DHS, and the TTIC? For instance, if a FBI field office has terrorism information, is it reported to your office and then in turn to DHS and TTIC?**

Response: The Office of Intelligence (OI) is the program manager for the FBI-wide Intelligence Program. As such, the OI manages intelligence requirements, collection tasking, information sharing policy, standards, the analytic cadre, and oversight of the FBI's distributed intelligence production mission. The core principle of the FBI Intelligence program is the integration of intelligence with FBI counterterrorism, counterintelligence, cyber, and criminal operations. The actual intelligence production mission takes place within those FBI investigative programs and in all operational divisions both at Headquarters and in the Field. The OI ensures that intelligence production is accomplished against a common set of priorities and according to a common set of protocols and policies regarding analysis and dissemination. Additionally, the OI develops training and certification standards for intelligence professionals, both analysts and agents.

The FBI produces two types of intelligence: 1) raw intelligence in response to intelligence requirements from the National Security and Homeland Security Councils; and 2) assessments to support FBI operations and those of our partners in the larger National Security Community, to include our state, local, and tribal law enforcement partners. Both raw intelligence and assessment reports are passed from 01 elements embedded in HQ divisions and the field to our customers according to a common set of standards and policies.

TIIC is an intelligence analysis organization with two core functions. First, it directs the work of raw intelligence producers like the FBI by identifying gaps in our knowledge and issuing requirements for intelligence collection and production with

respect to key threat areas. Second, it produces all-source threat analyses for the larger National Security Community. The OI ensures that TIIC intelligence requirements are tasked to FBI collectors and that assessments requested by TIIC are produced in a timely fashion. In addition, the OI manages the FBI analytic cadre embedded in TTIC. FBI analysts bring the authorities and intelligence information produced by the FBI directly to TTIC by virtue of their access to FBI systems and databases from TTIC space. In this way, the FBI is able to apply all its information to TTIC's mission of providing consolidated terrorist threat information to the National Security Community.

The Information Analysis and Infrastructure Protection (IAIP) component of DHS is an information and analysis organization with two core functions. First, it overlays threat information from all producers in the United States and proposes countermeasures. Second, through its participation in the larger national intelligence requirements process, it directs raw intelligence producers to provide information based on its analysis of vulnerabilities in the U.S. infrastructure. In addition, like the FBI's OI, DHS IAIP provides a full range of intelligence support to DHS leadership and manages the collection, processing, analysis, and dissemination of DHS information from its operational components (Coast Guard, Secret Service, Transportation Security Administration, Immigration and Customs Enforcemnt, and Customs and Border Protection). DHS has assigned to the FBI a senior representative, who is attached to the FBI's OI. That assignment ensures that all information required by DHS is passed to it expeditiously by the FBI.

4. The FBI has long established relationships with state and local law enforcement. The hearing held on July 22 indicated that state and local officials are receiving information from both the Department of Homeland Security and through the JTTFs.

Question: **What determines whether a piece of .information from the federal government is shared through DHS or the JTTFs? Are there any protocols or guidance?**

Response: The JTTFs are the operational and investigative arms of the United States Government in the war on terrorism. Because of this responsibility, the FBI is tasked with dissemination of information on terrorism (including operational and investigative information, as wellas general threat information) to the JTTFs, which utilize the information to conduct investigations and/or cover leads. This information is provided through the JTTF structure to state and local JTTF members who possess the appropriate security clearances. In addition, FBIHQ distributes weekly intelligence bulletins to all law enforcement officials through the National Law Enforcement Telecommunications System, the Law Enforcement Online program, the Regional Information Sharing System, and the National Electronic Alert System. The Special Agent in Charge of each FBI field office is tasked with further disseminating general terrorism threat information to members of the state and local law enforcement community through established methods. These methods may include regularly scheduled briefings, working groups, newsletters, e-mails, and similar vehicles. Terrorism threat information is shared on a daily basis between the FBI and DHS.

DHS passes threat information on to their state Homeland Security Directors, who are charged with notifying first responders in each state. Because many of these first responders are members of the law enforcement community, they often receive information from both the FBI and DHS.

There is close coordination between the FBI and DHS in the dissemination of terrorism intelligence information. All weekly FBI Intelligence Bulletins are reviewed by DHS prior to release by the FBI. The FBI and DHS have also agreed to protocols requiring coordination of changes made to the Homeland Security threat level. The sharing of information on terrorism intelligence was formalized in the March 2003 MOU referenced above.

5. You testified at the hearing that the FBI still has responsibility for "domestic terrorism."

Question: **Can you define the term "domestic terrorism"? For matters that fall in that definition of ″domestic terrorism,″ is the FBI the only agency with responsibilities? Does DHS have any role?**

Response: As codified at 18 U.S.c. section 2331(5), the term "domestic terrorism" means activities that:

(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;

(B) appear to be intended
(i) to intimidate or coerce a civilian population;
(ii) to influence the policy of a government by intimidationor coercion; or
(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
(C) occur primarily within the territorial jurisdiction of the United States.

While the overall role of the FBI in coordinating the Federal Government's response to a terrorist incident has changed pursuant to Homeland Security Presidential Directive 5 (2/28/03), the FBI still maintains responsibilities regarding domestic terrorism. DHS has assumed responsibility to coordinate the Federal Government's overall response to domestic terrorism incidents, including a major terrorist attack on U.S. soil. The FBI's role in domestic terrorism concentrates on criminal investigative and counterterrorism intelligence missions, tactical resolution of terrorist-related incidents, and the coordination of the law enforcement community's response to a terrorist incident. The creation of DHS in no way alters the FBI's chain of command. The Attorney General continues to have the lead responsibility for criminal investigation of terrorist acts and terrorist threats. The FBI continues to be the lead law enforcement agency to detect, prevent, preempt, and disrupt terrorist acts against the United States. While active coordination with DHS will be maintained, the FBI's investigative role in domestic terrorism will be preserved.

FOLLOW-UP QUESTIONS FOR JAMES K. KALLSTROM FROM CHAIRMAN GIBBONS

Question: **1. Who provides you with information about terrorist threats? Is it the Department of Homeland Security, the FBI, or another agency? If you receive information from both, can you determine what types of information are being channeled through DHS or the FBI? Is it a problem to receive terrorism information from the federal government through more than one channel?**

Answer: 1. The NYS Office of Public Security (OPS) receives terrorism threat-related information from a variety of federal sources. DHS and FBI supply frequent informational bulletins regarding current and historical terrorist trends, potential targets for terrorism (in general terms), potential indicators for terrorism, suggested protective measures for critical infrastructure, etc. DHS and FBI normally coordinate the dissemination of such information; both agencies contribute to the content and therefore a specific bulletin/advisory is only disseminated through one channel. In addition, DHS distributes related press releases, scripts of counter-terrorism related testimonies, and daily incident reports indicating possible terrorist activity nationwide.

As discussed in my testimony, shortly after September 11th 2001, OPS created 16 Counter-Terrorism Zones for the purpose of facilitating the dissemination of terror-related information and best practices, while promoting cooperation and collaboration among local, county and state law enforcement agencies on a regional basis. OPS also created the Counter-Terrorism Network, a secure, stand-alone system to distribute counter-terrorism and threat-based information and intelligence. Through these developed methodologies of information sharing, OPS disseminates the above-mentioned advisories from DHS and other federal agencies, as well as information generated by our office and other state and local agencies. Therefore, statewide law enforcement is uniformly kept abreast of current terrorist trends and indicators, enabling them to play a more effective role in the prevention of acts of terror in our state and country.

Our office also maintains contacts at other federal agencies, such as the CIA and the DOD, as well as other state homeland security offices and law enforcement agencies, and therefore may receive threat information in a less formal manner (i.e. phone call, fax, etc.) All information classified above ″Law Enforcement Sensitive″ is generally relayed in person or over a secure phone line.

Our office attends meetings and conferences with international intelligence and law enforcement agencies in effort to share information across national borders. We maintain contact with Canadian, British, German and other foreign counterparts.

Question: **2. Can you compare the status of information sharing prior to the passage of the Homeland Security Act to the present situation? What, if anything, has changed?**

Answer: 2. Information sharing between federal, state and local governments has improved significantly since the passage of the Homeland Security Act. The Depart-

ment of Homeland Security hosts bi-weekly regional conference calls with state homeland security representatives, touching base on local, national and international terrorism issues. DHS formalized a method of sharing terrorism information on a continual and frequent basis by distributing information bulletins and advisories (see AI) to our office so we may further disseminate information to appropriate law enforcement agencies and private sector constituents within New York State.

In addition, state and local representatives are invited to attend FBI-Joint Terrorism Task Force (JTTF) meetings held weekly to share and discuss current general and specific threat posture items of concern.

The creation of DHS has sparked the creation of federal information sharing centers like the Terrorism Threat Integration Center (TTIC) and the Terrorism Screening Center (TSC). TTIC, designed to serve as a depot and analytical center for all collected foreign and domestic intelligence, will facilitate the flow of raw and analyzed intelligence between federal, state and local law enforcement and intelligence communities. The TSC is designed to allow a state or local law enforcement officer to access federal watch list information in "real time" when he/she comes in contact with a suspicious individual during routine traffic stops, etc. This process can potentially help police officers intercept a terrorist and prevent the next attack.

However, these federal systems of improved information sharing will be effective only if the process does indeed work in "real time" and is unhampered by bureaucracy and interagency cultural differences. In reality, information sharing is often hindered between agencies due to nonequivalence of security clearance levels. Additionally, some federal agencies classify information, which is received at an unclassified level from foreign sources, thus rendering it difficult for us to further ascertain credibility or corroboration with the help of our federal intelligence agencies.

New York State and the nine other states comprising the Northeast Homeland Security Agreement have advanced a feasible system of "one-stop shopping" to enable the realtime dissemination of relevant counter-terrorism information to law enforcement. As outlined in my testimony, the Northeast Homeland Security Agreement has proposed the implementation of this information-sharing pilot program to the Department of Homeland Security. The currently operational Upstate New York Regional Intelligence Center (UNYRIC) will serve as the central hub of intelligence gathering, analysis and dissemination between law enforcement agencies in these northeastern states. This facilitated flow of counterterrorism information will enable state and locals to assist the efforts of the JTTF's. The proposal has been detailed and pending with the DHS since November 2003. It is our view that the conception and approval of this Northeast Regional information-sharing center, rather than federal intelligence centers, will better serve law enforcement personnel in New York State and the surrounding region. Finally, sensitive threat information and information regarding threat level changes is often prematurely released to the media. This makes it difficult for our office to share such information in a controlled and secure environment, leading law enforcement to discredit the intelligence community's ability to handle and effectively disseminate sensitive information from the federal to local level.

Question **3. Can you describe what happened when the threat level was raised or lowered in recent months? How did you find out about the change in the threat level? What guidance did you receive from the Department of Homeland Security at the time the threat levels changed?**

Answer: 3. The national and New York State alert levels were recently elevated to Orange on December 21,2003. That day, the Department of Homeland Security held several conference calls with our office and other state homeland security representatives. Secretary Ridge and other intelligence community (IC) representatives shared information regarding current threat posture, including intelligence indicators requiring the US to raise its terrorism alert level. Implementing Operation Liberty Shield at the federal level was discussed on the call, thus providing guidance to states for implementing their own deployment plans. The conference call and subsequent DHS advisory provided detailed information on the types of critical infrastructure terrorist groups may attempt to target and supplied guidance on the steps state and local law enforcement should take in protecting such targets.

When the alert level was lowered to yellow on January 9,2004, DHS conducted another conference call with state homeland security representatives to explain the lowering of the alert level and suggested reducing resources and security personnel deployed at strategic locals during Orange Alert.

Question: **4. Do you have a sense that the information you receive from the Federal Government is coordinated? Do you ever receive conflicting information from different Federal agencies? If so, what examples can you provide to the committee?**

Answer: 4. Since its inception, OPS has received information from a wide variety of federal agencies. This information usually appears to have been discussed among the various IC agencies prior to its dissemination to state and local authorities and there is clearly some consensus as to the threat/analysis/credibility of the information.

However, on occasion, our office has been in receipt of information from one federal agency that has clearly not been coordinated with other appropriate federal agencies prior to dissemination. There has been occasions where federal agencies are completely unaware of this information or if it was aware, it had assessed the credibility of the source or analyzed the intelligence in a drastically different manner. On occasion, we have had federal agencies contact our office for information when it would have been more appropriate to reach out directly to another IC agency.

Question: **5. If you run across information during your duties that could indicate potential terrorist activity, where would you report that information at the federal level? Is it the FBI? Do you know if the FBI shares that information with the DHS or with any other federal agencies?**

Answer: 5. OPS does not have an investigative arm thus the office reports all terrorist threat related info to relevant counter-terrorism agencies. For example, if intelligence reporting indicates an imminent threat, OPS would immediately contact 911 and then the relevant federal, state and local agencies.

If the threat does not appear imminent, information is distributed based on jurisdiction. OPS reports information related to New York City to the New York City Terrorism Tip Line–(888) NYC-SAFE that is handled out of the Upstate New York Regional Intelligence Center (UNYRIC). UNYRIC, based in Latham, New York, serves as a regional center to facilitate the collection, analysis. and dissemination of criminal and terrorist intelligence.

If the information is specific to another part of New York State, OPS reports information to the New York State Terrorism Tip Line—(866) SAFE-NYS. Both the New York City and the New York State Police evaluate the information and based on initial investigations, either choose to conduct further in-house investigations or pass the intelligence to the FBI Joint Terrorism Task Force (JTTF). On occasion, our office has passed information directly to the JTTF's when it appears very specific in nature to indicate federal jurisdiction.

When OPS has been in receipt of threat information pertaining to other states, we have reported said information to the state's respective homeland security office and/or appropriate law enforcement agencies at the federal, state or local level.

Question: **6. Has the Information Analysis office ever contacted you to coordinate training for your employees regarding information sharing? If no, does another federal agency provide such training?**

Answer: 6. Neither the DHS' Information Analysis Office nor any other DHS division has contacted OPS with regard to training our employees or providing training to other relevant officials within New York State. OPS has and will continue to orchestrate and offer counter-terrorism training for state and local law enforcement officers and first responders throughout New York State. Our office has taken the approach that continuing education is essential in this field and has implemented many programs in this regard. OPS welcomes educational and training initiatives provided by DHS and other relevant agencies for both our own staff and other relevant personnel involved in the war on terror.

Our office encourages DHS to utilize the resources available in the departments under its command and within the agencies of the Intelligence Community to coordinate training in a variety of areas. New York can benefit from additional training in; analytical skills, the creation of threat matrixes, data mining, first response, chem/bio-terrorism, radiological terrorism, infrastructure protection, general aviation threats/security, fraudulent documents, etc.