

**A PROGRESS REPORT ON INFORMATION SHARING  
FOR HOMELAND SECURITY**

---

**HEARING**

BEFORE THE

**SUBCOMMITTEE ON INTELLIGENCE,  
INFORMATION SHARING, AND  
TERRORISM RISK ASSESSMENT**

OF THE

**COMMITTEE ON HOMELAND SECURITY  
HOUSE OF REPRESENTATIVES**

**ONE HUNDRED NINTH CONGRESS**

**FIRST SESSION**

—————  
**JULY 20, 2005**  
—————

**Serial No. 109-33**

---

Printed for the use of the Committee on Homeland Security



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

---

U.S. GOVERNMENT PRINTING OFFICE

27-686 PDF

WASHINGTON : 2007

---

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

## COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

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

---

## SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

ROB SIMMONS, Connecticut, *Chairman*

CURT WELDON, Pennsylvania	ZOE LOFGREN, California
PETER T. KING, New York	LORETTA SANCHEZ, California
MARK E. SOUDER, Indiana	JANE HARMAN, California
DANIEL E. LUNGREN, California	NITA M. LOWEY, New York
JIM GIBBONS, Nevada	SHEILA JACKSON-LEE, Texas
STEVAN PEARCE, New Mexico	BOB ETHERIDGE, North Carolina
BOBBY JINDAL, Louisiana	JAMES R. LANGEVIN, Rhode Island
DAVE G. REICHERT, Washington	KENDRICK B. MEEK, Florida
CHARLIE DENT, Pennsylvania	BENNIE G. THOMPSON, Mississippi ( <i>Ex Officio</i> )
CHRISTOPHER COX, California ( <i>Ex Officio</i> )	

# CONTENTS

	Page
STATEMENTS	
The Honorable Rob Simmons, a Representative in Congress From the State of Connecticut, and Chairman, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment .....	1
The Honorable Zoe Lofgren, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment:	
Oral Statement .....	2
Prepared Statement .....	3
The Honorable Christopher Cox, a Representative in Congress From the State of California, and Chairman, Committee on Homeland Security .....	4
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security .....	6
The Honorable Charlie Dent, a Representative in Congress From the State of Pennsylvania .....	34
The Honorable Bob Etheridge, a Representative in Congress From the State of North Carolina .....	32
The Honorable Peter T. King, a Representative in Congress From the State of New York .....	30
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island .....	35
The Honorable Nita M. Lowey, a Representative in Congress From the State of New York .....	68
The Honorable Daniel E. Lungren, a Representative in Congress From the State of California .....	42
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas .....	39
The Honorable Dave G. Reichert, a Representative in Congress From the State of Washington .....	38
WITNESSES	
PANEL I	
Mr. John Cohen, Senior Homeland Security Policy Advisor, Executive Office of Public Safety, Commonwealth of Massachusetts:	
Oral Statement .....	7
Prepared Statement .....	9
Dr. Lee Colwell, Executive Director, Pegas Research Foundation:	
Oral Statement .....	16
Prepared Statement .....	17
Mr. Gary Edwards, Chief Executive Officer, National Native American, Law Enforcement Association:	
Oral Statement .....	12
Prepared Statement .....	14

IV

PANEL II

Page

Brigadier General Matthew Broderick, Director, Homeland Security Operations Center, Department of Homeland Security:	
Oral Statement .....	48
Prepared Statement .....	50
Mr. Joshua D. Filler, Director, Office of State and Local Government Coordination, Department of Homeland Security:	
Oral Statement .....	56
Prepared Statement .....	58

## **A PROGRESS REPORT ON INFORMATION SHARING FOR HOMELAND SECURITY**

---

**Wednesday, July 20, 2005**

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

The subcommittee met, pursuant to call, at 10:04 a.m., in Room 2257, Rayburn House Office Building, Hon. Rob Simmons [chairman of the subcommittee] presiding.

Present: Representatives Simmons, Cox, Souder, Lungren, Jindal, Reichert, Dent, Thompson, Lofgren, Lowey, Jackson-Lee, Etheridge, and Langevin.

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

The subcommittee is meeting today to hear testimony on the state of homeland security information sharing between the Department of Homeland Security and state and local government entities, and to explore how DHS information-sharing efforts to date can be enhanced.

In order to examine how DHS information-sharing efforts are currently working, and perhaps to explore how they can work better, we are going to hear from two panels: one representing the state, local and tribal perspective, and the other the Department of Homeland Security's perspective. The witnesses on our first panel today are Mr. John Cohen, Senior Homeland Security Policy Adviser for the Commonwealth of Massachusetts; Mr. Gary Edwards, Chief Executive Officer of the National Native American Law Enforcement Association; and Dr. Lee Colwell, Executive Director of the Pegasus Research Foundation.

I thank you all, gentlemen, for being here today.

The ability to share relevant terrorist-related information is key to preventing future attacks. In the wake of the terrible bombings in London on July 7, we are reminded that prevention is of paramount importance. The department is working diligently to ensure that structures and policies are put into place to give our intelligence and law enforcement entities the tools they need to prevent terrorist attacks. We have established within the DHS the Information Analysis and Infrastructure Protection Directorate.

We have created or supported an agreement, a memorandum of understanding on information sharing requiring all federal law enforcement, intelligence and homeland security agencies, to share

terrorist-related information. We have established the Terrorist Threat Integration Center, the Terrorist Screening Center, and most recently the National Counterterrorism Center, in order to better coordinate and share information. And so on and so on and so forth.

The department's Homeland Security Operations Centers serves as the nation's nerve center for information sharing, as a point of fusion for homeland security-related terrorist threat information. There are advisories and bulletins concerning threats to homeland security, and they manage the homeland security information network which is deployed to over 260 sites across the country. While the department is working to increase the federal government's ability to share information, there are also a variety of efforts underway across the nation at state, local and tribal levels.

I had the honor and the privilege of serving for over 35 years in the U.S. Army before my retirement a few years ago. For over 35 of those years, I was in military intelligence. I also had the experience of serving for 10 years as a CIA officer for most of those years under cover, actually for all of those years under cover, and for most of those years overseas. The culture of the intelligence community in my experience over those 35 years, the culture of the intelligence community is not to share. Sharing goes against the culture of the intelligence community. They want to protect sensitive sources and methods. They want to keep secrets. So there is a reluctance to share information. We understand that. Those of us who have served in the intelligence community understand that.

So the idea of intelligence information sharing, intelligence information sharing, is in many respects an oxymoron. It is kind of like jumbo shrimp, government efficiency. I could do a few more, but I do not want to offend anybody. So what we are talking about today is something new and different, but it is critically important if we are to prevent another 9/11. It is critically important if we are to protect our people and to provide for their homeland security.

So that is why we are pleased to offer this hearing today and to hear from our witnesses.

At this point, I would like to yield to my friend and colleague, the very distinguished ranking member of the Intelligence Subcommittee, Ms. Lofgren of California.

Ms. LOFGREN. Thank you, Mr. Chairman.

I will submit my full statement for the record, but I would like to note that I think this important hearing is timely. We need to be concerned about the sharing of information within intelligence agencies, but also perhaps even more importantly with agencies who are not intelligence agencies, our local and state police officials.

We have more than 18,000 state and local and tribal law enforcement agencies across the United States, more than 800,000 law enforcement officers. These officers have intimate knowledge of the communities they serve, and they develop close relationships with the citizens they protect. They are in a unique position to track down terrorist-related information, to understand and develop prevention information, but they need to be our partners, our intelligence partners in order to do that effectively.

I think we need to figure out how to get the police officer on the street the information that he or she needs to identify terrorist and to foil their plans. There are multiple efforts underway at all levels of government to meet the challenge, but there are some common principles I think that should govern the work. First, there should be agreement on what law enforcement needs to know. In my mind, I think they need to know the threats to specific locations, events, and specific infrastructure sectors. They need to know methods used by terrorist to plan, support and carry out attacks, and the individuals and/or organizations involved in terrorism-related activity.

Second, there needs to be agreement on why law enforcement needs to know this information. It needs to know it so it can guide efforts to prevent terrorist attacks. We do not want to respond. We want to prevent. And also to develop protective and continuity measures and emergency response plans. We need to design training programs and exercises. We need to select equipment and technology to be acquired for these efforts, and we need to develop budget and staffing plans in a coordinated and strategic way.

Finally, there should be agreement that the potential solution might not come from the top down. To the extent that state, local and tribal law enforcement agencies have developed successful methods and means of sharing information, consideration should be given to adapting these home-grown sharing approaches regionally and even nationally.

So I am glad to be here today. I look forward to the witnesses. As I mentioned to the Chairman, I do have to step out for a meeting with the Democratic Leader at 10:30, but I will be back shortly after that meeting. Our wonderful ranking member, who has spent an enormous time on this, certainly is here. I am grateful to him for his expertise and attention to this effort.

I yield back. Thank you.

#### TALKING POINTS FOR RANKING MEMBER ZOE LOFGREN

I am pleased that this Subcommittee is turning its attention once again to the critical issue of information sharing.

In view of the recent devastating terrorist attacks in London, the question of how we promote effective information sharing in order to discover terrorist threats and to avert them could not be more timely.

Like Mr. Thompson, I have long been concerned about how and to what extent intelligence information is being shared—not only among the CIA, the FBI, and the Intelligence Community generally, but also (and perhaps most importantly) with state, local, and tribal law enforcement authorities.

#### ***The Role of Local Law Enforcement***

As the September 11th attacks demonstrated, local law enforcement officers will likely be among the first responders to any future terrorist attack. Such officers should not be limited, however, to a merely responsive role. Instead, they can and should play a vital part in the investigation and prevention of terrorist attacks.

They are in a unique position to do this.

More than 18,000 state, local, and tribal law enforcement agencies across the United States—comprising more than 800,000 law enforcement officers—have intimate knowledge of the communities they serve and accordingly have developed close relationships with the citizens they protect.

These relationships provide officers with the ability to effectively track down terrorist-related information.

Officers on their day-to-day patrols interacting with the members of their communities can—if properly trained in what to look for and what questions to ask—be valuable sources of information and intelligence for the national homeland security effort.

In order to make use of this capability, however, it is essential for federal, state, and local law enforcement agencies to develop an efficient and comprehensive system for the timely sharing, analysis, and dissemination of specific and actionable intelligence information.

In other words, we need to figure out how to get the police officer on the street the information that he or she needs to identify terrorists and to foil their plans.

***The Information Locals Need and Why They Need It***

I am aware that multiple efforts are underway at all levels of government to meet this challenge. While the extent of integration among these efforts is unclear, I believe several common principles should govern this work:

*First*, there should be agreement on what local law enforcement needs to know. In my mind, it needs to know: (1) the threats to specific locations, events, and specific infrastructure sectors; (2) the methods used by terrorists to plan, support, and carry out attacks; and (3) the individuals and/or organizations involved in terrorism-related activity.

*Second*, there should be agreement on why law enforcement needs to know this information. In my mind, it needs to know it so it can: (1) guide efforts to prevent terrorist attacks; (2) develop protective and continuity measures and emergency response plans; (3) design training programs and exercises; (4) select equipment and technology to be acquired for these efforts; and (5) develop budget and staffing plans.

*Third*, there should be agreement that potential solution might not come from the top down. To the extent state, local and/or tribal law enforcement agencies have developed successful means and methods of sharing information, consideration should be given to adapting these “home grown” sharing approaches regionally and even nationally.

***Conclusion***

I am very glad that we have represented here today such a wide range of voices and expertise on information sharing. I look forward to your testimony and to hearing your ideas on how to create a workable information sharing environment.

Mr. SIMMONS. I thank the distinguished ranking member of the Intelligence Subcommittee for her observations. I also thank her for partnering on this hearing here today.

The chair now recognizes the chairman of the full committee, the distinguished gentleman from California, Mr. Cox, for any opening statement he might wish to make.

Mr. COX. Thank you very much, Mr. Chairman. I want to thank you and the ranking member. A progress report on information sharing on homeland security is a welcome thing. I think it is an indispensable part of this committee’s oversight responsibilities.

This morning, we begin by hearing from state, local and tribal government officials. That is unconventional only because we in Washington have a tendency to focus our attention on executive branch agencies, on the federal government. A homeland security enterprise properly conceived calls for a different approach.

I suppose that state, local and tribal governments are in theory equal partners, and that is the premise of this hearing. They are supposed to be equal partners with the federal government in a joint enterprise. So they must be, if potential terrorist attacks are to be prevented across this country in the future.

The federal government, even the Department of Homeland Security, is not everywhere. State, local and tribal governments, by contrast, are. It has been well over 2 years since the attorney general, the director of central intelligence, and the secretary of homeland security signed their memorandum of understanding on information sharing, committing intelligence, law enforcement and homeland security agencies alike to certain core principles. That MOU called for specific actions to implement the Homeland Security Act.

It contained the following plain statement: "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 attacks. Delay in providing such information risks frustrating efforts to meet these critical responsibilities and could result in preventable attacks against U.S. persons and interests failing to be preempted, prevented or disrupted."

We on this committee often stressed that preventing terrorist attacks must be our overriding priority, and we, like every commission and blue ribbon panel that has looked into these matters, understand that the failure promptly to share all pertinent information was the single preeminent factor in the government's failure to prevent the 9/11 attacks. It was in fact 2 years ago almost to the day that, in opening a select committee hearing on this same topic, I noted that if it is true that the tragedy of the 9/11 attacks teaches information and good intelligence is the lifeblood of homeland security, then it is also true that the information must move and must circulate. Sadly, that has not always happened.

That was my assessment of the state of affairs in 2003, in July. Two year later, I think it is fair to expect real progress, and that is why we are here today. We want to be reassured that DHS in particular has engaged its nonfederal government counterparts as equal partners in the homeland security enterprise. We want to know that there are now mutually satisfactory mechanisms to enable the two-way communication, the two-way flow of information, to and from DHS and its state, local and tribal government partners that this enterprise contemplates. That, in itself, would be real progress.

So, Mr. Chairman, I want to focus as we move forward with this hearing on what I think it would be realistic to expect, and at the same time, what would be unrealistic to expect. I think it might be unrealistic to expect state, local and tribal governments' preventive efforts to be very effective if they are not routinely informed by the relevant predictive intelligence that the federal government produces. Nor would the federal government be serving its non-federal customers well if it merely passes on a welter of raw information, or by speaking to those customers with an inconsistent analytic voice, a problem this committee addressed squarely in passing the department's initial authorization act, H.R. 1817, overwhelmingly just 2 months ago.

So today we look forward to hearing that information sharing has progressed. We hope to hear how the structural reforms engendered by the secretary's second-stage review will further consolidate and enhance that progress. Where, by contrast, shortcomings emerge, I am confident that this committee will continue to lead in the effort to ensure that a failure adequately to share information can never again be cited as the reason a terrorist attack could succeed.

Thank you, Mr. Chairman.

Mr. SIMMONS. I thank the chairman for his comments.

I agree completely that I suppose our worst nightmare is a situation where there might be another successful attack in the homeland, and we learn as part of the process of an after-action report that there was information available that simply was not shared with the people that need it. That is our goal, to avoid that type of a situation from occurring.

The chair now recognizes the distinguished ranking member of the full committee, the gentleman from Mississippi, Mr. Thompson, for any comments he would like to make.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Like my colleagues, I look forward to the testimony of both panels.

I would like to give a special welcome to Dr. Colwell from the Pegasus Foundation. He just happens to be from my district and doing good work.

But nonetheless, Mr. Chairman, this hearing is a very important hearing. The tragic attacks in London 2 weeks ago demonstrated to all of us once again that terrorists think nothing of killing innocent people in their war against open democratic societies. Terrorists are not only foreign infiltrators, but homegrown radicals that blend easily into the various societies that they have come to despise.

What I found so shocking about London, beyond the senseless carnage, was the fact that neither the British nor our own intelligence services saw the attacks coming. We at last addressed information sharing in depth in the 108th Congress, prior to the issuance of the 9/11 Commission report. In this report, the commission called for major reforms in the intelligence community organization of practices, including the development of a decentralized network for information sharing. It made clear that improving border security, preparing first-responders, and security critical infrastructure is not enough. We will not be safe unless we are effectively sharing information about terrorists and their plans.

Information sharing, however, means much more than getting the CIA, the FBI and other members of the federal intelligence community to talk to each other. It also means improving information sharing with the law enforcement officer in the street. This includes reaching out to the law enforcement in rural and small communities. Ninety-percent of the law enforcement agencies within the United States serve communities of less than 25,000 people. Over 75 percent of police departments across the nation, moreover, serve communities of less than 10,000 residents. As the 9/11 Commission demonstrated, it is in these localities that law enforcement will first encounter the next group of terrorists.

Indeed, it was the local police officers who stopped three of the 9/11 hijackers for routine traffic violations in the weeks and months prior to the September 11 attacks. The rest, the right-wing extremists like Timothy McVeigh and Eric Rudolph in rural jurisdictions, further highlight the often critical role that law enforcement in these areas plays in the apprehension of terrorists.

Rural America is likewise home to much of the nation's critical infrastructure, including agriculture, food production facilities, dams, nuclear power plants and portions of electric grids. For all of these reasons, I am very interested in how information sharing

is working and how it is developing for the benefit of small and rural communities. While much of our homeland security attention has been focused on large cities and urban areas like New York, Washington, Chicago and Los Angeles, and rightfully so, it is critical that we also ensure that our small communities and towns are looped into information-sharing networks.

Mr. Chairman, I look forward to the testimony of our witnesses, particularly on their views on information sharing in rural America.

I yield back.

Mr. SIMMONS. I thank the ranking member for his comments.

Other members of the committee are reminded that opening statements may be submitted for the record.

Mr. SIMMONS. Now, I would like to call the first panel: Mr. John Cohen, senior homeland security policy advisor for the Commonwealth of Massachusetts; Mr. Gary Edwards, chief executive officer of the National Native American Law Enforcement Association; and Dr. Lee Colwell, executive director for the Pegasus Research Foundation.

Gentleman, if you don't mind testifying in that order, we have a 5-minute clock that will give you a green light, a yellow light, and a red light. I think anybody who has been involved with any form of law enforcement understands that the yellow light does not mean slow down, it means speed up. And the red light means stop. We would encourage you to summarize your testimony because we have copies in our books and can probably read faster than you can speak. So we encourage that you summarize, stick to the 5-minute rule so that we will have an opportunity to ask questions and interact.

That being said, I would ask Mr. Cohen to lead off. Mr. Cohen?

**STATEMENT OF JOHN COHEN, SENIOR HOMELAND SECURITY  
POLICY ADVISOR, EXECUTIVE OFFICE OF PUBLIC SAFETY,  
COMMONWEALTH OF MASSACHUSETTS**

Mr. COHEN. Thank you, Mr. Chairman, Chairman Cox, members of the committee. I appreciate the opportunity to appear before you today.

Recently, the homeland security advisers from a vast majority of the states came together under the umbrella of the National Governors Association. There was clear consensus among that group that at the end of the day this is the most important issue facing us as we try to better protect our communities or be prepared to respond should an attack occur, because again at the end of the day, everything we do as it relates to homeland security, whether it is response planning, recovery planning, critical infrastructure protection and resiliency initiatives, or prevention activities, depends on accurate and credible information about those who want to attack us, the targets they intend to attack, and how they wish to carry out those attacks.

If I had to describe to you, well, since I am here I am describing to you, where we are today as a nation with regard to this, I would have to tell you that we have made great progress over the past 2 years, but we are still not where we should be or must be if we

are going to be effective in protecting our communities from future attack.

Governor Mitt Romney of Massachusetts has chaired for the last 1 1/2 years a working group comprised of state and local officials. My friend, Mr. Edwards, was a participant in that process, where we looked at the role that state, local, tribal entities and the private sector should play in supporting our prevention efforts and most importantly, the role they should play in efforts to gather, analyze, share and use homeland security-related intelligence. So much of what I am about to say to you and much of what was contained in my written testimony that was submitted are the results of those efforts.

Today, from an information-sharing perspective, we still depend on a national system that can best be described as a patchwork of ad-hoc processes, protocols and technical capabilities that still require state and local officials to develop strong interpersonal relationships with representatives from key federal agencies. Particularly in times of critical threat evaluation or emergency situation, we depend more on those interpersonal relationships than on a solid, well-defined, institutionalized infrastructure to support intelligence and information sharing.

The Department of Homeland Security and the FBI are doing a much better job at providing state, local and tribal entities an integrated intelligence product. But at the same time, we still receive from both those entities large quantities of nonactionable intelligence and information, which actually comes to us at times with a caveat that this information has been deemed noncredible, of course facilitating us to ask the question, why is it being sent to us in the first place?

Even though the Department of Homeland Security and the Federal Bureau of Investigation are doing a much better job of integrating the product that they send out to state and local entities, we still receive considerable amounts of intelligence and information from other federal entities who clearly are not collaborating with the FBI and the Department of Homeland Security prior to sending that information out, and at times we receive information that is conflicting or cannot be verified from some of the key intelligence sources that we rely on to do our planning.

There still is no national plan that provides clear guidelines for how state, federal, local and tribal entities and the private sector should work together to gather, analyze, disseminate and share homeland security-related intelligence, recognizing that it is a complex issue because much of this information is protected by privacy and other types of guidelines that restrict the inappropriate disclosure of that information.

There remains an over-emphasis at the federal level on providing classified information and intelligence to state and local entities. There is an over-emphasis on trying to create closer linkages or actually draw state and local entities into the intelligence community. This is a significant issue because at the end of the day if I am going to be effective in protecting our local communities, working with our local, tribal and private sector entities to be prepared to respond, I need to share critical intelligence with them. If it is provided to me in a classified format and I have to share it with

people who do not have appropriate clearances in order to do my job, I am put in the position of either not doing what I need to do to be effective, or violating the law.

The emphasis should be on the federal community coming together and providing unclassified intelligence and information to state and local authorities. Clearly, there are times when they will need to share classified information. We should put the infrastructure in place to do that, but the rule should be unclassified information.

There is some good news. There is a greater level of sophistication at the state and local level with regard to their role in this whole intelligence cycle. You are seeing the emergence of intelligence fusion centers in most of our major cities and states. Unfortunately, a lot of money was spent over the past several years by state and local governments in establishing these centers without any clear guidelines. The Homeland Security Advisory Council, working with the Global Justice Information Sharing Working Group, has developed those guidelines. We are working with DHS and the FBI and the Justice Department to send those out.

I just would leave the committee, since my light is red, with two final thoughts. As everybody pointed out, state and local entities are important gatherers of intelligence, but that does not mean that we should act as spies or practice tradecraft of the intelligence community. We should be focusing on taking that information which we gather in our day-to-day crime control and other delivery of emergency and non-emergency services, and being better able to determine when there is a linkage with terrorism, as opposed to asking us to carry out the function of an intelligence agency.

Secondly, I would just re-emphasize that as consumers of intelligence, we need this intelligence to guide prevention efforts, but also response, recovery and continuity planning. It guides everything we do at the state and local level as it relates to homeland security.

Thank you, Mr. Chairman.

[The statement of Mr. Cohen follows:]

PREPARED STATEMENT OF JOHN D. COHEN

Mr. Chairman, members of the Subcommittee good morning. My name is John Cohen and I currently serve as the Senior Homeland Security Policy Advisor to the Commonwealth of Massachusetts. In that capacity, I am a direct advisor to the Governor of Massachusetts Mitt Romney and the Secretary of the Executive Office of Public Safety Edward Flynn. I appreciate the opportunity to be here with you today.

The hearing today is entitled "A Progress Report on Information Sharing for Homeland Security"—and for state, local and tribal governments there truly is no more important issue because at the end of the day, the efficacy of our prevention, response, and recovery efforts all depend upon the effective collection, analysis, sharing, and use of timely and accurate intelligence about those who wish to attack us, the targets they intend to attack and the methods they intend to use.

Terrorism-related intelligence is not solely utilized by or derived through the efforts of the Intelligence Community. The attacks of 9/11 and the recent bombings in London taught us that today our enemy may not always be overseas—he or she may live in our local communities—and engaged in criminal and/or other suspicious activity as they plan attacks on targets within the United States and its territories. Intelligence and/or information regarding possible attacks—possessed by federal authorities must be provided in a timely manner to state, tribal, local and key private sector entities to support information-driven efforts to protect our communities. Furthermore, information that may forewarn of a future attack may initially come to

the attention of authorities through local crime control activities or by reports made by the general public.

The Intelligence Community plays a critical role in managing the flow of terrorism-related intelligence among critical stakeholders. But, until recently, the manner in which our modern day Intelligence Community operated and the mindset it operated under for the most part was established during the Cold War and designed to confront foreign-based, state-sponsored adversaries. Efforts are underway to restructure the Intelligence Community so that it can better meet the challenges of the post 9/11 world. This restructuring must include defining the appropriate roles for state, tribal, local, and private sector entities in the collection, analysis, dissemination and use of this intelligence and information—and how those efforts should be coordinated with those of the Federal Government. This debate represents an historic opportunity to enhance existing information sharing between all levels of government—and—the threat to the nation demands that we proceed expeditiously. But—we must also proceed thoughtfully and consider all of the civil liberty and financial implications before asking state, tribal, local and private sector entities to take on new responsibilities.

#### **BACKGROUND**

In an open society, it is impossible to protect against every possible type of attack. While all appropriate steps should be taken to protect and secure our society and we should continue our efforts to have a robust response effort, the key to protecting America is to prevent another attack. To be fiscally prudent and operationally effective, prevention efforts must be intelligence-driven, adaptable, multifaceted, prioritized, and designed to effectively support efforts to:

- **Identify and target for arrest**, prosecution, incarceration, and/or other enforcement actions, such as deportation, people who have been determined to be supporting, planning, and/or intending to carry out an attack.
- **Protect potential targets from being attacked**—this means enhancing the physical security of high-risk targets to reduce their attractiveness to potential attackers and ensuring the continuity of critical services to minimize the impact of an attack at a single or multiple locations.
- **Disrupt the ability of terrorists to plan and conduct operations**—State, local, and tribal entities can effectively disrupt the ability of terrorists to operate according to their plan and force them to change their methods of operation, thereby exposing them to potential discovery by disrupting their financial support networks and implementing—in an unpredictable manner—aggressive protective measures such as counter-surveillance of potential targets and directed patrol.

**The key to prevention is intelligence.** We have spent billions in America since 9/11 on response—it is time now to put equal and greater attention on the challenge of preventing future attacks. We need to get our intelligence operations functioning at the level needed for the threats we now face. While the federal government clearly has primary responsibility for intelligence, the state and local governments must play a major role. We are the eyes and ears on the front lines in the homeland. And while this doesn't mean that state and local authorities should begin spying on the public, it does mean that in the course of our day-to-day duties we gather information that may have a nexus with a terrorist threat and this information needs to be organized, analyzed and distributed to those who can act on it. Information sharing between federal, state, local, tribal and private sector entities has improved since the attacks of 9/11, but it is still not as effective as it should be—and must be—if we are going to protect our communities from future attack.

Over the past year, state, tribal and local officials have worked to better define the role state and locals should play in intelligence gathering and information sharing. We have also thought about what we need from the federal government if we are to play our role successfully. In June 2004, with the concurrence of then DHS Secretary Tom Ridge, Massachusetts Governor Mitt Romney established the Homeland Security Advisory Council (HSAC) Intelligence and Information Sharing Working Group (Working Group) to review the roles, responsibilities, and requirements of state and local government entities as related to the collection, analysis and dissemination of terrorism-related intelligence information. The Governor established the Working Group in recognition that while there seemed to be general agreement at all levels of government that the sharing of terrorism-related intelligence/information is vital to our nation's efforts to detect, prevent, and effectively respond to acts of terrorism here at home, it is still somewhat unclear what state and local

entities should be doing as a part of a national effort in this regard.<sup>1</sup>

In December 2004, the HSAC Intelligence and Information Sharing Working Group issued a report that included a number of findings and recommendations intended to better define what state, tribal and local governments should be doing as part of our nation's efforts to collect, analyze, disseminate and use terrorism-related intelligence (a summary of that report is included as an attachment to this testimony). At that time, the Working Group reported that almost every state is establishing an "information fusion center"—a location where homeland security-related information can be collected and analyzed. But the Working Group also found that there was no common definition of fusion nor were there standards to guide the states in doing so. The Working Group was asked by Secretary Ridge to develop a list of functional attributes for use as a guide by state, tribal and local entities as they seek to establish statewide and urban area "fusion centers."

On 4/28/05, the Governor formally presented to the HSAC guidelines to support establishing a state-based, nationwide fusion capacity—recognizing that every level of government and the private sector has a role in the fusion process (a copy of the April report is included as an attachment to this testimony).

### INFORMATION FUSION

The process that has become known as "information fusion" represents the organizing principle that supports an effective national homeland security intelligence capacity. The Working Group defined the term "fusion" as the overarching process of managing the flow of information and intelligence across levels and sectors of government and the private sector to support the rapid identification of emerging terrorism-related threats and other circumstances requiring intervention by government and private sector authorities. It is a key part of our nation's homeland security efforts because it supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. It means more than the one-time collection of law enforcement and/or terrorism-related intelligence information and it goes beyond establishing an intelligence center or creating a computer network. It is a clearly defined and ongoing process that involves the blending of information from:

- The intelligence and information management systems used to support the core missions of individual Federal, state, tribal and local government entities;
- The general public; and
- Private sector entities.

The Working Group report acknowledges that the way in which individual jurisdictions and regions implement the fusion process will vary taking into account their specific needs, capabilities and resources. The Working Group's report lists a number of factors critical to an effective intelligence/information fusion process—these include:

- Common terminology used by all stakeholders;
- Up-to-date awareness of the global and domestic threats;
- An understanding of the linkages between terrorism and non-terrorism related information so that we can recognize "precursors" or "indicators" of an emerging threat;
- Intelligence and information requirements that prioritize and guide planning, collection, analysis, dissemination and re-evaluation efforts;
- Understanding and elimination of impediments to information collection and sharing;
- Extensive and continuous interaction with the private sector and with the public at-large;
- A commitment to ensure aggressive oversight and accountability so as to protect against the infringement of constitutional protections and civil liberties.

The Working Group recommended that minimally, each state should establish and maintain an analytic center to facilitate the fusion process—Each major urban area (as defined by the UASI program) may want to establish a similar capacity **ensuring that it is interlinked with the fusion process established by the state.** Additionally, there needs to be some consideration of where these fusion centers link into the federal system.

Secretary Chertoff—as well as a numerous other federal, state, local and private sector entities—have been briefed on the efforts and findings of the Working Group.

<sup>1</sup>The Intelligence and Information Sharing Working Group was comprised of state, tribal, local and private sector officials representing various disciplines. The Working Group worked closely with members of the Global Justice Information Sharing Working Group—a Department of Justice sponsored advisory committee comprised of state and local law enforcement officials. Representatives from the Department of Homeland Security, the Department of Justice and the Federal Bureau of Investigation actively participated in all of the Working Group's efforts.

Information contained in both reports have been incorporated into the guidelines and other materials being developed by the Department of Homeland Security that are intended to support efforts by state, tribal and local governments to enhance their capacity to prevent, respond to and manage the consequences of a terrorist attack.

#### **CONCLUSION**

The initial report of the HSAC Intelligence and Information Sharing Working Group outlines the roles state and locals should play in intelligence gathering and information sharing, and it also outlines what we need from the federal government if we are to play our role successfully. This report has been given serious consideration by the White House and by DHS as they write preparedness standards for state and local governments, and I hope that the federal government will also consider the critical role of state and locals in intelligence as they restructure the federal intelligence environment.

The follow-up report on standards for fusions centers in the states comes at a time when most states have one or more fusion centers under development. For this reason, and recognizing that it is ineffective to demand that the same structure be used in every state or large urban area, we have focused instead on the process that should take place in a fusion center—what are the inputs and outputs needed for a state's fusion operation to be effective.

Equally important is the report's recommendation that the federal government recognize that states are establishing a fusion process and that the federal government needs to take this into account as they restructure the federal environment. We have made clear what we need from the federal government in order to be effective in our role—and we will focus in the states on putting together the fusion operations on the ground that can ensure we have a robust intelligence operation working at every level throughout our country.

Mr. SIMMONS. Thank you very much for that testimony. Congratulations, you finished at the red light. Good going.

Mr. Gary Edwards, we look forward to your testimony, sir.

#### **STATEMENT OF GARY EDWARDS, CHIEF EXECUTIVE OFFICER, NATIONAL NATIVE AMERICAN LAW ENFORCEMENT ASSOCIATION**

Mr. EDWARDS. Thank you, Mr. Chairman, Mr. Vice Chairman and distinguished members of the committee. My name is Gary Edwards. I am the chief executive officer of the National Native American Law Enforcement Association, also known as NNALEA.

I am honored and pleased to appear before this committee and the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment to discuss the progress of information sharing for homeland security. Thank you for this opportunity to address you.

I ask that my written testimony be entered into the record.

Mr. SIMMONS. Without objection.

Mr. EDWARDS. NNALEA is a nonprofit public service organization formed in 1993. Among other things, we provide a media for the exchange of ideas and new techniques, establish networks for training collaboration, technical assistance, information sharing and investigative assistance between federal, tribal, state and local governments and agencies and the private sector.

We have conducted 12 national training conferences, and this year we are going to be conducting our 13th national training conference on November 15 through 17, 2005, in Las Vegas, Nevada. We are sure that some of the hot topics will be homeland security and information sharing. You are all invited to attend.

In my capacity as the chief executive officer of the National Native American Law Enforcement Association, I serve on a number of advisory committees, task forces and working groups for the De-

partment of Homeland Security and the Department of Justice. It is my opinion that the progress of information sharing for homeland security can be best understood by comparing today's information sharing for homeland security with that of the past.

Prior to the formation and efforts of the Department of Homeland Security, information sharing on issues relating to the security of our homeland was handled in patches, wherein the federal departments, states, tribes, localities and the private sector would largely engage in information sharing for homeland security independently and through limited coordination. There was not a master weaver, so to speak, to achieve a seamless fusion of all the patches.

The result was, in the past, although there was some information sharing, there was no comprehensive plans, no centralized coordination, no seamless functionality of information sharing for homeland security. With the formation of the Department of Homeland Security, the information sharing to secure our homeland was finally given its much needed master weaver.

Presently, the Department of Homeland Security has placed a great focus on information sharing for homeland security. Secretary Chertoff stated, "The ability to share information with our international, state, tribal, local partners, the private sector, law enforcement and first responders is absolutely critical to our success."

The Department of Homeland Security has employed a national approach engaging national agencies such as the National Congress of American Indians and the National Native American Law Enforcement Association, among numerous others, to work toward achieving information sharing goals such as the integration among public and private stakeholders of the roles and responsibilities for the security of our homeland: seamless functionality for information sharing, establishment of effective partnerships for information sharing, information sharing pertaining to prevention, protection, all-hazards response and recovery, establishment of comprehensive information sharing, centralized coordination of information sharing, promotion of greater situational awareness, and the fusion and sharing of a richer intelligence base.

For example, NNALEA, the National Congress of American Indians and the Department of Homeland Security are currently conducting a tribal border security pilot program. The tribal border security pilot program is cutting edge and provides the Indian tribes located on or near the international borders of the United States with the opportunity to advance their respective tribe's ability to deal with threats or acts of terrorism, national disasters and other national emergencies, while also advancing Indian Country and national homeland security.

In one phase, we used tribal border security pilot program tools to collect capabilities and information such as emergency management and public works, law enforcement, border security, detention facilities, emergency fire response, emergency medical responders, facilities, critical infrastructure, and environment and public safety communications and interoperability. The tribal border security presents this information to the Department of Homeland Security, which may use it in assessing the as-is environment of homeland security on our borders, as well as the homeland security capabili-

ties, preparedness and assessments for the participation of tribes, among other uses.

We must thank the 40 tribes for sharing this information with the Department of Homeland Security. It shows their vigilance in the protection of our nation.

In the future, as we look to information sharing and homeland security progress, we must look at integration of information sharing systems between federal, state, tribal and local governments and agencies, as well as the private sector.

This integration can be achieved through the following: the federal government clearly defining what type of intelligence and information is needed; the removal of barriers like long-awaited security clearances; the empowerment of local and tribal law enforcement to collect intelligence; the creation of a legal structure for intelligence gathering and information sharing that law enforcement officers feel comfortable in; the removal of any legal impediments that prevent law enforcement's ability to gather legitimate information at the state, tribal and local levels without spying on people, and all the while protecting the constitutional and human rights of American citizens; the continued establishment of coordinated intelligence and information fusion centers; the development of clear, open interoperable communications and information-sharing policies that require two-way information sharing between the federal departments, states, tribes, local entities and the private sector because top-down information sharing is an ineffective and inefficient method that creates untimely critical information sharing; the development of innovative means to build and maintain a personal relationship across our great homeland for personal relationships are the time-tested catalyst for information sharing; and the provision for funding for much-needed equipment, technology training, accreditation, certification, personnel pay parity and so forth to allow governments and agencies of different means to be able to achieve seamless information sharing for homeland security.

As Winston Churchill once said, "Give us the tools and we will finish the job."

Thank you again for this opportunity to speak, and I will answer any questions you may have for me.

[The statement of Mr. Edwards follows:]

PREPARED STATEMENT OF GARY L. EDWARDS

***Introduction***

Mr. Chairman, Mr. Vice-Chairman and distinguished members of the Committee, my name is Gary Edwards and I am the Chief Executive Officer of the National Native American Law Enforcement Association ("NNALEA"). I am honored and pleased to appear before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment to discuss the progress of information sharing for Homeland Security. Thank you for this opportunity to address you today.

***Background on NNALEA***

As many of you may be aware, NNALEA is a non-profit public service organization founded in 1993, which among other things, provides a media for the exchange of ideas and new techniques, and establishes networks for training, collaboration, technical assistance, information sharing and investigative assistance between federal, tribal, state and local governments and agencies and the private sector. NNALEA has conducted twelve (12) National Training Conferences across the United States, and is currently preparing for its thirteenth (13) National Training Conference to be held on November 15-17, 2005 in Las Vegas, Nevada. Homeland

Security and information sharing will be hot topics at this upcoming National Training Conference. In my capacity as the CEO of NNALEA I have served on a number of advisory committees, task forces and working groups of the Department of Homeland Security and the Department of Justice.

***Information Sharing for Homeland Security—Past***

The progress of information sharing for Homeland Security can best be understood by comparing today's information sharing for Homeland Security with that of the past. Prior to the formation and efforts of the Department of Homeland Security, information sharing on issues relating to the security of our Homeland were handled in "patches," wherein the federal departments, states, tribes, localities, and the private sector would largely engage in information sharing for homeland security independently or through limited coordination. There was not a "Master Weaver," so to speak, to achieve a seamless fusion of all of the "patches." The result was that in the past, although there was some information sharing, there were no comprehensive plans, no centralized coordination, and no seamless functionality of information sharing for Homeland Security as a whole. With the formation of the Department of Homeland Security, information sharing to secure our Homeland was finally given its much needed "Master Weaver."

***Information Sharing for Homeland Security—Present***

Presently, the Department of Homeland Security has placed a great focus on information sharing for Homeland Security. As Secretary Chertoff recently stated: "The ability to share information with our international, state, [tribal] and local partners, the private sector, law enforcement and first responders is absolutely critical to our success." The Department of Homeland Security has employed a national approach, engaging national organizations such as the National Congress of American Indians (NCAI) and NNALEA, among numerous others, to work towards achieving information sharing goals such as: integration among public and private stakeholders of the roles and responsibilities for the security of our homeland; seamless functionality of information sharing; establishment of effective partnerships for information sharing; information sharing pertaining to prevention, protection, and all-hazards response and recovery; establishment of comprehensive information sharing plans; centralized coordination of information sharing; promotion of greater situational awareness; and the fusion and sharing of a richer intelligence base.

For example, NNALEA, NCAI, and a number of other partners with the support of the United States Department of Homeland Security Office for Domestic Preparedness are currently performing the Tribal Border Security Pilot Program ("TBS Pilot Program"). The TBS Pilot Program is cutting-edge and provides Indian Tribes located on or near our International Borders with the opportunity to advance their respective Tribe's ability to deal with threats or acts of terrorism, natural disasters and other national emergencies, while also advancing Indian Country and National Homeland Security. In one phase of the TBS Pilot Program a number of information gathering tools are utilized to collect information on areas vital to Homeland Security, such as: Emergency Management and Public Works; Law Enforcement, Border Security and Detention Facilities; Emergency Fire Responders; Emergency Medical Responders and Facilities; Critical Infrastructure and Environment; and Public Safety Communications and Interoperability. It is anticipated that the Department of Homeland Security may use the information from the TBS Pilot Program as an aid in assessing the "as is" environment of Homeland Security on our borders, as well as a Homeland Security capabilities, preparedness and needs assessment of the participating Tribes, among other uses.

Much recognition and many thanks should be given to the nearly forty (40) tribes who have graciously shared their information on the above areas for the TBS Pilot Program. Their participation is a testament to their vigilance for the security of our Homeland. In addition, much recognition and many thanks should be given to the United States Department of Homeland Security for its insightfulness in recognizing the important role that these border Indian Tribes play in our Homeland Security.

***Information Sharing for Homeland Security—Future***

As information sharing for Homeland Security progresses into the future, the focus should continue to be upon the integration of information sharing systems between federal, state, tribal, and local governments and agencies, as well as the private sector. This integration can be achieved through the following:

- the federal government clearly defining what type of intelligence and information is needed;
- the removal of barriers, like long waits for Security Clearances;
- the empowerment of local and tribal law enforcement to collect intelligence;

- the creation of a legal structure for intelligence gathering and information sharing that law enforcement officers feel comfortable in;
- the removal of any legal impediments that prevent law enforcements' ability to gather legitimate intelligence at the state, tribal and local levels, without spying on people and all the while protecting the Constitutional Rights and Human Rights of American Citizens;
- the continued establishment of coordinated intelligence and information fusion centers;
- the development of clear "Open Interoperable Communications Information Sharing Policies" that require "two-way" information sharing between the federal departments, states, tribes, local entities and the private sector, because 'top-down' information sharing is an ineffective, inefficient method that creates untimely critical information sharing;
- the development of innovative means to build and maintain personal relationships across our great Homeland—for personal relationships are the one time-tested catalyst for information sharing; and
- the provision for funding for much needed equipment, technology, training, accreditations/certifications, personnel, pay parity and so forth, to allow governments and agencies of differing means to be able to achieve seamless information sharing for Homeland Security.

As Winston Churchill once said: "Give us the tools and we will finish the job."

**Conclusion**

Thank you again for the opportunity to address you today. I am happy to answer any questions that any of you may have.

Mr. SIMMONS. Thank you, Mr. Edwards.

Now, I would like to recognize Dr. Colwell. Again, if you could summarize your key points in 5 minutes, that would be most helpful. I have already read your very good statement.

**STATEMENT OF LEE COLWELL, EXECUTIVE DIRECTOR,  
PEGASUS RESEARCH FOUNDATION**

Mr. COLWELL. Thank you, Mr. Chairman. I will be brief.

I request the written statement that I submitted be entered in the record.

Mr. SIMMONS. Without objection.

Mr. COLWELL. I will summarize, with your permission, comments made in the written statement.

I want to talk about the functions of a 501(c)(3) foundation, the Pegasus program, and how it facilitates information sharing among our local-to-local law enforcement agencies, that is not without, although the mission is horizontal, it is not without vertical accessibility, given certain parameters.

I think that we live in interesting and unprecedented challenging, changing paradigms involving how law enforcement does its job. I think that the recognition of a national imperative that existed long before it was identified has been good for our country and the noble efforts of this body and the executive branch are commendable.

I would suggest that when we talk about federal, state and local, that we raise and, A-N-D, to all caps because local law enforcement agencies are where all of the day-to-day routine crimes occur, and that reservoir or body of information collected through traditional and historical law enforcement efforts is rich in data that can aid and support law enforcement at the local level, as well as at the national level with those agencies of the federal government that have the first-line responsibility for the strategies involving what we can do to protect our nation.

I would like to spend a moment describing to you what the Pegasus program, Local-to-Local, is about. Briefly, Pegasus facilitates information sharing at the local-to-local level, the horizontal. This was started by the National Sheriffs' Association in the year 2000, prior to the tragic events of 9/11. At that time, and in our view remains to this day, the only national initiative initiated through this body and funded through this body that directly involves facilitating and accessing by local law enforcement information agencies the information that is generated and created there. There is nowhere else that this data resides in the form that it is.

There are summaries. There are statistical reports that are submitted. And there are certain warrants and crimes that rise on up through the system to the state and the federal level. Simply stated, the Pegasus program facilitates information sharing from disparate legacy databases, whatever is there, without changing it or modifying it in any way, and makes it accessible to other law enforcement agencies through a biometric fingerprint authentication process as part of the protocols for accessing the data system. We use a fingerprint.

It is an Internet-based, secure, biometric fingerprint performing the following functions: access to legacy databases that do not meet, for the most part, the global justice XML standards. It would be a huge cost factor to try to change all those quickly. It provides a directory of law enforcement agencies and the personnel, a secure directory. It provides alert functions. It provides a consular notification function. When a foreign national is arrested by a local law enforcement agency, it provides notification to the consulate and the State Department.

It links databases. It shares information. We have a governance board of sitting members, former and current members, sheriffs and chiefs. It does not compete or duplicate with existing databases or vendors. It works with the existing software and hardware. It does not extract data. It provides access. It is not an intelligence system. It is a voluntary participating process. There is no cost, thanks to the Congress, to the agencies who are linked up. It employs multiple vendors who actually perform and make up databases.

We conform to the privacy laws and traditions of each state and those law enforcement bodies in which they operate. It is a system for law enforcement.

Thank you, Mr. Chairman.

[The statement of Mr. Colwell follows:]

PREPARED STATEMENT OF LEE COLWELL, DPA

Chairman Simmons, Ranking Member Lofgren, and Subcommittee Members:

Thank you for the opportunity to appear before this Committee and provide you with information and my views about law enforcement and homeland security information sharing, especially regarding the needs of local agencies for Local-To-Local (L2L) law enforcement data communications, not voice (i.e., public safety radio). I speak especially to the needs of agencies in rural and small-town America. Thank you also for the work you do to make all our communities and Nation safer places for all Americans.

My name is Lee Colwell. I am Executive Director of the Pegasus Research Foundation, located in Little Rock, AR. I am a Former Associate Director of the FBI, the number two position in the FBI at the time, a retired university professor, a life member of the NSA and IACP. My entire professional career has been deeply involved in law enforcement and public safety at all levels of government.

I am speaking on the need for L2L data communications, especially in rural areas, on behalf of the Pegasus Program, which includes Pegasus Technology Consortium members from Colorado, Iowa, Kentucky, Minnesota, Mississippi, Pennsylvania, and Virginia. I will discuss what the Pegasus program is, what Pegasus is not, what the program does, the background on local law enforcement, how Pegasus could assist the Department of Homeland Security, and a final comment on information sharing.

I also reflect the views, I believe, of the approximately 700 local law enforcement agencies from more than 30 states, from Maine to California and Washington to Florida, and numerous points in between, which Pegasus currently serves, either by providing an outlet for their local agency legacy data, or by providing access to that data which is not available elsewhere, or both. A map showing the location of those local agencies involved in the Pegasus Program is attached to my written statement.

#### WHAT THE PEGASUS PROGRAM IS

The Pegasus program is Congressionally-led. Pegasus is locally managed as a nationwide initiative for highly-secure nationwide L2L legacy data exchange of local law enforcement and homeland security data. As far as we know, the Congressionally initiated Pegasus program is the only nationwide program with a strategy and plan for nationwide implementation.

Pegasus is a good example of how Congress provided for previously unmet local agency needs to solve an essentially Federal problem by engaging thousands of local front line law enforcement personnel in the solution. Pegasus was initiated by the National Sheriffs' Association in 2000 and supported by Congress in 2001 prior to 9/11.

With continued support, Pegasus provides a basic tool that serves local agency needs for L2L law enforcement data communications. This is especially critical to those small and rural agencies where the need is the greatest because they have limited or few financial and information technology resources and little or no access to local agency data from other areas.

The Pegasus Program has been working with local agencies to build local agency consensus on local agency data sharing, namely:

- (a) what information do local agencies want to share;
- (b) how do they want to share it; and,
- (c) who do they want to share it with.

Based on needs assessment work over several years and on-going policy guidance of local law enforcement, the Pegasus Program has implemented a technology solution that reflects the "bottom-up" needs of local agency. This program is designed to provide access to specific and actionable local law enforcement information on a real-time or near-real-time basis, and the ability to communicate that data without human intervention.

During the first half of 2005, more than 750 county Sheriff's Offices and municipal police departments in more than 30 states participated in the Pegasus Program, either by contributing data, accessing data, or both. Pegasus is providing authorized secure access to local law enforcement booking and warrant data that is nowhere else available, and has taken first steps to provide access to local incident data nowhere else available. This has been achieved in a little over a year, with fairly nominal levels of Federal funding, and is poised to rapidly expand with additional funding.

Built around secure encrypted Internet transport and the Department of Justice Global Justice XML Data Model and other Federal standards wherever possible, Pegasus uses commercial off-the-shelf (COTS) technology. The data is highly-secure, in particular through biometric fingerprint access authentication. This process is implemented through formal enrollment procedures and fingerprint-based authentication technology that is more resistant to "hacking" than commonly used UserID/Password systems. This authentication technology allows system administrators to "track the insider", which is perhaps the greatest security risk. To do this Pegasus uses COTS fingerprint readers that are marketed by a dozen different manufacturers and COTS software.

Pegasus is a highly cost-effective vehicle for regional information sharing projects, especially for local agencies in small towns and rural areas that do not have the financial and information technology resources to build technology-intensive data sharing capabilities. A good example here is the rural law enforcement agencies in Virginia, West Virginia and Maryland located near Clarke County, Virginia which work with the Mount Weather Police Department to provide security to FEMA facilities in the area. These local agencies want and need a secure information exchange capability of the type that can be provided both by and to the Mount Weather PD. Pegasus has been working with them with the view toward providing that capability.

The Pegasus program builds on existing technology deployment which significantly reduces time to deploy, training, capital and implementation costs, and maintenance costs. This has the added benefit of making it fast and cheap to deploy relative to other “common software” and “common data center” initiatives.

Your colleagues in the Senate have recently made it clear that improved information sharing among emergency responders is essential to a comprehensive homeland security response. Improved information sharing among emergency responders is also essential to homeland security preparedness, as well as homeland response.

A classic “dual-benefit” system, Pegasus is primarily focused on local agency needs, starting with local law enforcement, but also can serve Federal law enforcement and Homeland Security by making local agency data available for Federal personnel access, not extraction, in accordance with local agency policies. Pegasus is working with several federal law enforcement agencies to help them achieve their law enforcement information exchange mission on terms acceptable to local law enforcement.

#### **WHAT PEGASUS IS NOT**

Pegasus is not a theoretical or “ivory tower” standards-setting body. Pegasus does advance and implement Federal standards like the Global Justice XML Data Model, which have been adopted by DHS. Most importantly, Pegasus is actually working in the field to implement Federal standards, not just discuss them.

Pegasus does not replicate what is in place—where a regional information sharing system is in place which meets Pegasus security and other policy requirements, Pegasus works with those system’s to provide a conduit for data to be exchanged in and out of the region.

Pegasus does provide a nationwide, Internet based conduit by which local agency information in these regional systems can be accessed nationally, and by which local agency information outside these regions may be accessed by these regional systems, subject to meeting Pegasus security standards, in particular biometric access authentication.

Many regional systems do not use biometrics or other strong access authentication technologies and processes—and we are unable to share with them because the Pegasus governing policy is to share only with systems that have biometric fingerprint access authentication technologies and processes in place.

In this connection, Pegasus is working with local law enforcement agencies in several locations that have adopted the biometric fingerprint access authentication technologies and processes. These include agencies in Hinds, Madison and Rankin Counties, Mississippi; Jefferson County, Alabama and surrounding counties along Interstate 20; Marshall County, Iowa and surrounding counties; Linn County, Iowa and its police departments; Calhoun County, Michigan and surrounding counties; the Vermont Sheriffs’ Association; and, the County Sheriffs of Colorado. Pegasus provides cost-effective services to these regional information exchange efforts. A point of discussion is that most local information sharing systems are being built without strong access authentication technologies. As a result, Pegasus security policies do not allow their linkage.

Pegasus is not a data aggregator that owns local agency data, but a data utility that transports local agency data. Unlike some other initiatives, Pegasus does not push privacy boundaries or mix law enforcement and private sector data in powerful data mining technologies. Pegasus focuses on enabling traditional exchange of law enforcement data. The Pegasus program emphasis is on information exchange of traditionally collected law enforcement data and automating those processes.

#### **WHAT THE PEGASUS PROGRAM DOES**

Pegasus’ mission is to serve as a nationwide vehicle for local law enforcement and public safety data in existing legacy systems to be securely accessed (but not extracted) by authorized law enforcement, public safety and Homeland Security users at all levels of government, within policy and security framework approved at the local agency level.

Pegasus builds local agency consensus and speaks for local-level agencies nationwide on data integration and data interoperability issues. It provides a nationwide L2L biometric fingerprint-secured law enforcement data communications service for agencies located in both rural and urban areas, ranging from Dawes County, Nebraska, with a population of 9,060, to Los Angeles County, California, with a population of over 9,800,000.

Pegasus provides legacy database integration for local law enforcement agencies nationwide. This system can facilitate law enforcement agencies at local as well as State and Federal levels to access but not extract legacy data that local agencies wish to share. The program also provides a nationwide directory of critical contact information useful to local agencies; secure messaging and alerting capabilities that

represent a secure alternative to inherently insecure email; services that automate exchange of information by local law enforcement, such as consular notifications of foreign nationals who have been arrested or detained; shared mapping for local agency location and local critical infrastructure location; and, training on data interoperability issues.

The Pegasus program governance is through the Pegasus Advisory Board. Our policy board consists of sitting or recently-retired local law enforcement officials. The Pegasus Advisory Board addresses nationwide local-level agency policy on data interoperability issues as they are developed.

#### **BACKGROUND ON LOCAL AGENCIES AND LOCAL LAW ENFORCEMENT**

As you know, under our Federal system of Government, the overwhelming majority of law enforcement activity is carried out by local law enforcement—some 14,000 local law enforcement agencies composed of approximately 3,100 Sheriff's Offices, led by Sheriffs who are typically the highest constitutionally-elected officials in most counties, and about 11,000 municipal police departments.

There are some 160 large U.S. cities and counties, served by a few hundred large local law enforcement agencies—Sheriff's Offices and Police Departments—that provide law enforcement and public safety services to the majority of the Nation's population living and working in a small fraction of the Nation's landmass.

These urban areas and their law enforcement agencies serving them face many challenges. When compared to non-urban law enforcement these large urban areas have significant resource advantages; e.g., access to personnel with cutting edge technology expertise, large tax bases with significant tax revenues, and the specially-focused Federal programs such as the Homeland Security Urban Area Security Initiative (UASI), which focuses on the needs of the largest urban areas.

At the same time, a very significant portion of the Nation's population and the critical infrastructure serving the entire nation, including bridges and dams, interstate transportation network, railroads, shipping, chemical plants, pipelines, nuclear and conventional power plants and electric transmission facilities, are located in predominantly rural counties. These rural areas are served by more than 13,000 local law enforcement agencies—the vast majority of law enforcement agencies. These small police departments and Sheriff's Offices typically have 5 or less employees, and are located in small non-urban communities with a static at best or declining tax bases: 89.7% of local law enforcement agencies serve populations of less than 25,000. These municipal police departments and Sheriff's offices serving rural and small town America are a special focus area for the Pegasus Program.

The Pegasus Program was conceived of by the Nation's Sheriffs in the Spring of 2000, to address their need to make their data available to their local law enforcement partners, in "local-to-local communication". As you know, 90% of the deputy sheriffs work for an office with a jail and as such, these offices are the primary source of information about persons arrested and detained for illegal actions, including criminal aliens. Sheriffs and municipal police departments work together daily on criminal investigations and other routine law enforcement matters which require secure L2L data communications capabilities. This kind of L2L communications is behind the explosive deployment of regional information sharing projects around the Nation, many of them "regional stovepipes" which do not have L2L communications capabilities outside their small region.

Rural and small local agencies do not operate in isolation nor are they immune from the crime in the rest of the Nation. Historically, every major US terrorist incident has involved major direct contact with rural law enforcement—ranging from the 9/11 hijackers to the Unabomber, to the Midwest Pipe Bomber to Timothy McVeigh to Eric Robert Rudolph, the 1996 Atlanta Olympic Games Bomber. Currently, two of our Nation's more significant law enforcement challenges—methamphetamine and gang activity—heavily involve urban/rural interaction. Most methamphetamine production in the Nation takes place in rural America, where it can be produced without detection before being transported to both urban and rural areas. Similarly, gang activity, a traditionally-urban phenomenon, is spreading from urban areas to rural areas throughout the Nation. Because criminal gangs from Central America, in particular, are "franchising" rural areas, the Nation's local law enforcement leadership in large urban areas, such as Los Angeles Sheriff's Department, are seeking ways to work more effectively with rural law enforcement to control the gang problem, and are looking to Pegasus and other vehicles to help solve our gang problem.

There is a great deal of misunderstanding about where local law enforcement data may be found. It is well understood that most law enforcement activity takes place at the local agency level, and that most law enforcement data is generated and may be found at the local agency where it is generated. The twelve million plus reported

crimes by the Uniform Crime Report data are crimes in local jurisdictions. Many Federal policymakers and agencies also perceive that the National Crime Information Center (NCIC) or the State agencies generally known as the “State Crime Information Centers” have access to all of this local law enforcement data: in fact, nothing could be further from the truth. All narrative criminal offense/incident reports and most misdemeanor warrants are created and reside exclusively at the municipal and county level—not at the State level. These records contain specific and actionable information of great value to law enforcement at all levels of government, but, in my opinion, the vast majority of them will never be accessible by local, State or Federal law enforcement except through L2L data exchange of the kind that Pegasus is providing.

Enormous quantities of specific and actionable law enforcement data—highly useful to persons with law enforcement and homeland defense responsibilities at local, State and Federal levels of government. These records remain within local agencies and local agency computer systems, and are never accessed by other agencies. It is estimated 80-90% of local agency warrants are not reflected in the NCIC or State Crime Information Centers. These records not in NCIC are primarily misdemeanor and some felony warrants (most frequently due to costs to extradite). This data represents a tremendous potential resource for the Nation’s homeland security and other Federal law enforcement agencies.

There is also a major policy issue regarding Federal access to local law enforcement data, as opposed to unfettered Federal extraction of local agency data to reside in Federal databases for manipulation by Federal agencies. Federal access to local agency data is generally supported by local law enforcement, but local law enforcement data is solidly opposed to Federal extraction of their data, which raises numerous privacy and legal issues. In this connection, 42 USC § 3789d, “Prohibition of Federal control over State and local criminal justice agencies”, provides in relevant part as follows: “(a) Nothing in this chapter or any other Act shall be construed to authorize any department, agency, officer, or employee of the United States to exercise any direction, supervision, or control over any police force or any other criminal justice agency of any State or any political subdivision thereof.”

The overwhelming view of local agency officials nationwide is that Federal extraction of local law enforcement data is a significant start down the slippery slope to prohibited Federal control over local police. The overwhelming majority of local law enforcement leaders are prepared to allow Federal agencies to access their data on local agency terms, but are not about to start down the slippery slope toward Federal control over local policing, which is inherent in Federal extraction of local agency data.

I will now address the ambiguous usages of the term “information sharing”, which means different things to different users. Most Federal information sharing initiatives are driven by Federal needs and perspectives. For most Federal information sharing initiatives, “information sharing” means providing Federal information from one Federal agency to another Federal agency or pushing Federal data down to a local or State agency. Sometimes it also means providing the capability for local agency to push information up to a State or Federal user.

As important and valid as this Federal view of “information sharing” is, local law enforcement agencies are mostly concerned about a very different type of L2L “information sharing”: sharing law enforcement and public safety information with other agencies—mostly municipal police departments and Sheriff’s Offices—with which they work on routine criminal investigative matters, some percentage of which carry Federal law enforcement and Homeland Security implications. This is the area of “information sharing” with which local law enforcement and Pegasus are most concerned. Except for Pegasus, we are not aware of any Federal or, for that matter, any non-Federal initiative which has a strategy and plan for nationwide L2L “information sharing.”

#### **HOW COULD PEGASUS ASSIST THE DEPARTMENT OF HOMELAND SECURITY IN ACHIEVING ITS MISSIONS?**

We believe there are several opportunities.

(1) One is The Homeland Security Information Network (HSIN), which serves as a nationwide vehicle for Federal Sensitive But Unclassified (SBU) data to be securely accessed by emergency responders and critical infrastructure sector users. This process occurs within policy and security framework approved by the Federal Government. We believe Pegasus can help with this mission.

(2) The ICE Detention and Removal Office (DRO) and other DHS units have information which would be useful for a broad range of law enforcement personnel to have access to, including persons that DHS or local officials may not want to have access to HSIN—e.g., DRO data on alien criminals.

Pegasus and HSIN staffers have discussed working together so that HSIN recognizes Pegasus-authenticated users. That means that Pegasus authenticated users will have credentials and permissions recognized by HSIN. Under this arrangement, Pegasus will bring to HSIN several thousand users in more than 30 states, many of them from rural counties and small agencies are added on to the HSIN first-priority areas. We anticipate that, should HSIN implement strong access authentication with biometrics for law enforcement personnel, Pegasus will recognize the HSIN credentials and permissions of HSIN users, as part of the HSIN Law Enforcement Community.

#### **OTHER INFORMATION SHARING**

(3) Pegasus is actively facilitating the sharing of relevant and timely information between local law enforcement agencies in its L2L program. Pegasus has also briefed DHS investigative personnel who have indicated a strong interest in having access to a pilot project which would provide sophisticated and link analysis to data maintained in local databases along our southern borders. Pegasus has briefed a number of Department of Justice federal law enforcement agencies including the FBI and DEA and proposed providing access to local data especially jail records. We see relevance to this data with a pilot project and partnership of federal agencies with Pegasus in providing link analysis of these records. We have proposed partnerships with a pilot project utilizing federal prison records with several federal agencies including the FBI, DEA, ICE and DRO.

(4) Law enforcement officials at the local level are also concerned about criminal enterprises, including terrorist activity being run from not only the federal prison population but the 3000+ local jails. To investigate such criminal enterprises, authorized investigators (both federal and local) face a daunting and time-consuming process of assembling jail booking records and detail call records. The Pegasus Program with its Pegasus Technology Consortium, believe this existing tool (link analysis) needs to be demonstrated through the pilot projects we have proposed to the above cited agencies.

Mr. Chairman, thank you and all the committee members for allowing me to provide my views on L2L information sharing. We look forward to facilitating a growing dialogue between the Congress and local agencies, as Congress works to address national law enforcement and Homeland Security needs and the role and needs of local agencies for L2L data communications in that larger context.

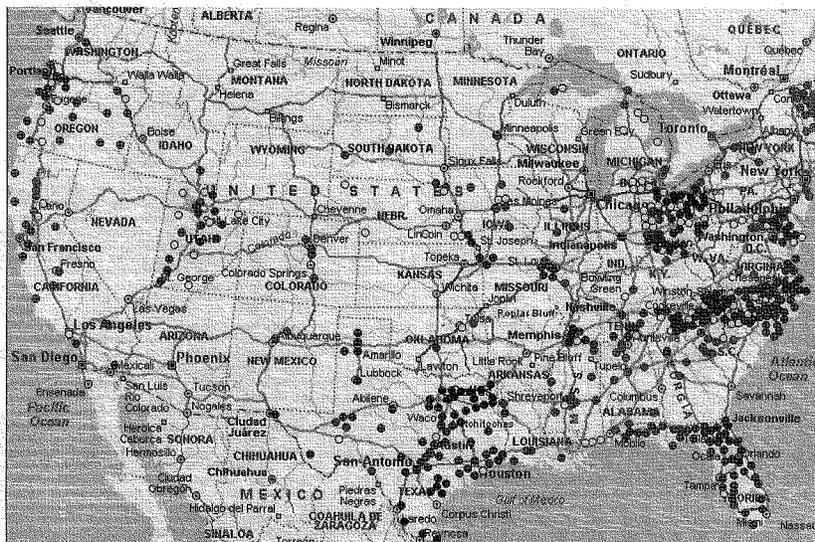
I will address any questions you may have.

**Pegasus Agency Map**

June 2005

**KEY**

- Accessing Agencies
- Contributing and Accessing Agencies
- Contributing Agencies



Attachment 1

National Law Enforcement Data Communications Networks: Functionality and Constituency Analysis (Rev.060402)

	Constituency	Governance	Functionality	Legal Regime	Mission
RISS	Federal, State and Local Law Enforcement	Authorized by Congress; line item appropriation; oversight at OJP/BIA; National Policy Group; Six center policy boards	<ul style="list-style-type: none"> <li>-Provision of a secure law enforcement intranet; secure e-mail; access to intelligence databases at local, state, regional, federal levels; national gang database</li> <li>-RISSLeads investigative bulletin board/news group server for collaborative law enforcement efforts</li> <li>-On-line access to RISSTraining server for training materials restricted to law enforcement; deconfliction databases; EPIC clan lab database</li> <li>-Access to law enforcement publications; connection to HIDJAs; utilizations of XML to facilitate data exchange</li> <li>-RISSSearch—a system wide search engine</li> </ul>	Intelligence databases operate under provisions of Criminal Intelligence Systems Regulations (28 CFR, Part 23)	Communication and information sharing among local, state, and federal law enforcement agencies

<p>LEO (Law Enforcement On-line)</p>	<p>Federal, State and Local Law Enforcement, Criminal Justice and First Responders</p>	<p>Joint cooperative agreement between FBI and LSU; authorized by Congress, funded through OJP/BIA and managed by FBI</p>	<p>-LEO is the only Certified and Accredited (C&amp;A) Internet based system for Sensitive But Unclassified (SBU) Information by the FBI with 37,000 registered users nationwide                  -Secure email: LEO is a secure Virtual Private Network (VPN) for information sharing between all levels of law enforcement, criminal justice officials and first responders                  -Online training; Online publications; Multiple levels of security within Special Interest Groups (SIGs); Webpage services; News Group Services; Real-time Chat                  -Listserv/Broadcast messaging to members; Used to disseminate weekly FBI Intelligence Bulletin as well as hosting local and state intelligence reports within the Law Enforcement Sensitive Communications SIG; Utilized to support all criminal investigative programs as well as counter-terrorism and homeland security matters</p>	<p>Secure communications and information sharing. Presently, it is not a system of record and contains no databases under provisions of Criminal Intelligence Systems Regulations (28 CFR, Part 23)</p>	<p>National Secure Data Communications Network for information sharing, distance learning, and communications for local, state, and federal law enforcement agencies and first responders.</p>
<p>NCIC/State CICs</p>	<p>Federal, State and Local Law Enforcement</p>	<p>DOJ/State CICs</p>	<p>Federally-managed, National Crime Information Center (NCIC) linked with State-managed CICs for accessing Felony Criminal History Record Databases</p>	<p>Criminal Justice System operating under 28 CFR Part 20 and State Laws</p>	<p>National Felony Criminal History Records Network work</p>

National Law Enforcement Data Communications Networks: Functionality and Constituency Analysis (Rev.060402)—Continued

<p>Pegasus Program For Local Law Enforcement Data-bases and Connectivity</p>	<p>Local Law Enforcement (sponsored for Sheriffs and Municipal Law Enforcement)</p>	<p>Policy Boards composed of Local Law Enforcement (NSA/Sheriffs and Municipal Law Enforcement), Fire, and EMS Officials, subject to OJP/BIA Oversight</p>	<p>-Creates new databases and makes existing databases accessible by others, nationwide (including help desk services for local agency database users) for records which RISS, LEO and NCIC/State CICs do not provide                  -Creates optimal Database Architecture for Local Records, using XML and wireless aware protocols and Federally-encouraged standards                  -Enables local agency database sharing by providing broadband Internet access and computer equipment linking local agency databases for local level information sharing by Law Enforcement, Fire, and EMS with local public health offices, hospitals, and public utility, transportation, and other private sector entities with responsibilities in Critical Infrastructure Protection and Homeland Security                  -Provides live training and education, and substantive technical assistance for local agencies                  -Provides a platform for bringing emergency priority data communications to local agencies and Public Key Infrastructure ("PKI") for secure and authenticated information sharing among local agencies</p>	<p>Criminal Justice Databases operating under 28 CFR Part 20 and State Public Records Laws; No Criminal Intelligence Databases under 28 CFR Part 23</p>	<p>Mission                  Local Agency Database Network (Non-Felony Criminal History and other Public Records)</p>
--	---	--	--	---	--

Mr. SIMMONS. Thank you very much for that summary.

Now, we will move to questions.

I have a couple of questions for the panel. Let me start by making a comment, though, and thank Mr. Edwards for his testimony. Sometimes people ask me why is tribal involved in these issues. Of course, we have very substantial Indian tribes that occupy territories on our borders, and that is a pretty obvious example of where we need to work closely with the tribes.

I will also say in my district in Eastern Connecticut, we have the Mashantucket Pequot and the Mohegan Tribes who operate the two largest casinos in the world, the two largest casinos in the world. We know from reading the translation of the Manchester, England, al-Qa'ida manual that places of amusement are potential targets. So it is very important when you have anywhere from 60,000 to 100,000 people aggregating in one place over 1 weekend, it is very important that the people who operate facilities like that be included in the system. I thank you for your participation.

I would like to focus a little bit on Mr. Cohen's testimony. He made reference to the fact that information sharing is complicated by virtue of the need of people having clearances and the need to move classified information very, very carefully. That sometimes inhibits information sharing. I have been an advocate for many years of open source intelligence, that is intelligence that is produced from the acquisition and analysis of information that is openly available. Of course, the Pegasus system, I think, describes a mechanism for transferring those openly available data systems from one organization to another.

One of the advantages of open source acquisition is that you are not placed in the position of being a spy. You are simply accessing databases that somebody else has accumulated. The information that you acquire and the analysis that takes place, takes place in an open environment where you can share with others. If people question your analysis, you can show the factual basis for the analysis.

Are we doing enough in the area of open source intelligence and does this discipline lend itself to the homeland security mission? I would be interested in any comments you might have to make.

Mr. COHEN. Thank you, Mr. Chairman.

I think you make a very valid point. As I stated earlier, for me to be able to use intelligence that is produced from information from a variety of sources, I need to be able to share that information or that intelligence oftentimes with people who do not have clearances. Sometimes they are law enforcement officials. Oftentimes they are emergency management fire officials. They are all important parts of not only our response planning activities, but they are an important part of our ability to protect or mitigate the risks to specific targets.

So we need to have an intelligence sharing environment that allows us to take that intelligence and share it with as many people as possible who are involved in our homeland security-related activities.

Right now, there is sort of a conflict, however. There is a conflict between some in the federal system, and quite frankly there is a disconnect by some at the state and local level. At the state and

local level, there are still a great number of people who believe, if I only had my security clearance, I would see the magic. I would see the unicorn. The sun would come through the trees and I would have a full understanding of those threats which we face.

I think there is an education process that is necessary to train these state and local folks and tribal folks that the magic panacea does not lie with a security clearance; that there is important information, critical information that is not classified, that can be accumulated through open source-related activities, and that it is much more important to put in place an effective process of gathering analysis, dissemination and use and re-evaluation than necessarily having a security clearance.

Within the federal side of the house, I think there is still a debate over whether we should continue the practices of the Cold War era and try to classify as much as possible, and then provide clearances to people at the state and local level and let those people in on the secrets. In contrast, there are those at the federal level, and DHS has been a real champion of this in many respects, of saying no, we need to take this information. We have to put it into an unclassified format. We have to blend it with other information that is taken from open source and taken from state and local sources, and we need to get that finished product to state and locals so it can become part of their planning efforts.

So I would agree with you. I think the vast majority of state and local officials would also agree with you, the more open the better.

Mr. SIMMONS. Thank you very much.

Any other comments from the panel? You do not have to if you do not want to.

Mr. COLWELL. Mr. Chairman?

Mr. SIMMONS. Yes, Mr. Colwell.

Mr. COLWELL. I would add to the comments and support the comments made. I would make a couple of observations. I do not believe that local law enforcement, meaning the county sheriff and the municipal police department, want every piece of information. They want those items that are specific and actionable so that they can tell their officers what they need to know and what needs to be done. They are not talking about classified information.

I am aware that there is a major initiative by my former organization, the FBI, to present information in an unclassified version at the outset, if it is significant information and contains specific and actionable information, then they are trying to do that. They are not there yet, but the point is the attitude and the willingness and the will to do it is there. But on the other hand, there is not a demand for that information because there is a lot of information that all of us do not need to know. The question is whether I can do something about it.

Thank you.

Mr. SIMMONS. Thank you for those comments.

The chair now recognizes the distinguished ranking member of the full committee, Mr. Thompson, for questions.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

I appreciate the testimony of all the witnesses.

Dr. Colwell, I live in a community of 500 people, just west of your operation. How would a rural community relate to this intel-

ligence gathering network? And how would that information be delivered? And what would be the backbone for a system like that so that we would make sure that the right information is getting to a community of that size?

Mr. COLWELL. There are a number of communication links where that can occur and is occurring in varying degrees of accuracy and success. So permit me, if you will, to just speak about the Pegasus program. It links databases that are resident in those small communities and permits them to share information. Built in with that is a secure system of notification to communities. The non-law enforcement portion of those communications that does not involve investigations of individuals or involve privacy issues could be linked to a mayor's office even in a small community of 500, where there is a need to know that.

I think that overall there is an effort being made to address that. A lot of progress has been made, but there is a huge amount of work yet to be done. The Pegasus program, with the information alerts to the law enforcement agency, whether it is a chief of police or a sheriff, can get information to those areas, unlike any other. It is economically feasible with a project like the Pegasus because of the use of the Internet. Anyone who has a computer can, with pre-authentication and validation, can subscribe to that or participate in that.

Mr. THOMPSON. Thank you very much.

Mr. Cohen, you have heard a description of a system like that. What do we have available to state and local law enforcement people at this present time?

Mr. COHEN. Congressman, there are a variety of mechanisms that are out there.

I think one that we are looking at in Massachusetts very strongly at is the Homeland Security Information Network that is being provided to us by the Department of Homeland Security. We are going to put it in every local community, even those in the rural areas. We are going to accompany its deployment with a training program for all of our communities so we can tell people, whether they are rural police officers or firefighters or someone inspecting the tracks on our transit and rail infrastructure, what they should be looking for, how they should report it, how to use the system.

The system will link into our statewide fusion center. It will provide feedback back to those rural communities that provide us the information and intelligence. Then it also gives us a way to communicate with our Joint Terrorism Task Force and the HSOC.

Mr. THOMPSON. But at this moment, we do not have a system.

Mr. COHEN. Right. At this moment we depend on a variety of processes, whether it is telephone calls, faxes, using email systems. We have a system we call Saturn in Massachusetts, but it is one-directional. We can send information out. We have to have people call us back with additional information.

Mr. THOMPSON. Dr. Colwell, do you want to make a comment?

Mr. COLWELL. Yes. In meeting with Homeland Security officials yesterday, I believe their plans calls for the creation of 2000 sites in the next 2 years. My understanding is that it will not go to the specific, you know, the 500-member community unless there is a compelling reason to put it there due to critical infrastructure pres-

ence or some extenuating circumstance. The point is, as Mr. Cohen mentioned, they are in the process of doing that and it just takes a little time.

Mr. THOMPSON. I think it is important, and that we encourage the department to move forward because obviously this is a vulnerability from the standpoint of intelligence.

If I might, I would like to ask Mr. Edwards, to your information, are Indian tribes plugged into the intelligence network so that you can receive information on any homeland security-related activities?

Mr. EDWARDS. For the most part, no. There are some departments that are some of the top in the country that are connected, but they are connected through cross-deputization and other user agreements. Most of Indian Country, the majority of the 562 federally recognized tribes, do not have access to the information, and many times they do not have a way to give information that they see or hear in their communities.

Mr. THOMPSON. Thank you.

Mr. KING. [Presiding.] Thank you, Mr. Thompson.

Chairman Simmons has left the chair for approximately 10 or 15 minutes, and I will be sitting in his place for that time.

I would like to ask Mr. Cohen the question, then, and either of the other two gentleman certainly are encouraged to add anything they want to it. Really, it is a two-part question.

One is, if you could just give me the chain of command or exactly what happens when you arrive in the office in the morning. Who in Washington would be giving you intelligence? You mentioned Homeland Security, but also you said other agencies and departments also feed you information. Some of it is useful and some of it is not. You also, I believe, said that some of it is conflicting. Some information you get says it is deemed not to be credible, but it is given to you anyway.

If you could just lay out the process as to who gives you information, where you look for it, who gives it to you outside of Homeland Security from the federal government? Does FBI information come separate or does that go through Homeland Security?

Then as an add-on to that, I think it flows, you mentioned a number of problems that still exist as far as the flow of information. Can you just give a general thematic answer to that? Are those problems decreasing? Is the system getting better? Or do you think the problems are locked in place?

Thank you.

Mr. COHEN. Thank you, Congressman. May I answer your second question first?

Mr. KING. Surely, yes.

Mr. COHEN. Because I was getting a red light, and I would have gone into this in my general testimony.

Things are getting better. The Department of Homeland Security, the FBI, the Justice Department are working very closely with us at the state and local level and the tribal level to begin working through some of these issues.

We had a meeting yesterday, in fact, a combined meeting of the Homeland Security Advisory Council Working Group on Intelligence and Information Sharing, with the Global Justice Informa-

tion Sharing Working Group. It was attended by folks from the FBI, from the Justice Department, from DHS, and people outside of the law enforcement community.

We are thinking through not just how do we share information and intelligence more effectively between law enforcement, but also how do we bring in the other disciplines that are critical, both as consumers and gatherers of information.

So there is a lot of progress. DHS has been working very aggressively with us to fix these problems. They recognize that there are some challenges. Secretary Chertoff really seems to get it from the perspective the state and locals are a key partner. So we are at the table. We are working together. Things are getting better.

From the standpoint of your first question, that is a great question because my day usually begins with me calling the Department of Homeland Security, at least most days, just to see what is going on on a general basis. They are very good about sending out a morning operation report, which I look at. There are other reports that come to me from a variety of other sources such as TSA, FAA, the information sharing advisory committees for the different industry sectors.

At the same time, I check with our state police to see if our folks assigned to the JTTF, the Joint Terrorism Task Force, have anything on the horizon. I then make a call to the U.S. Attorney's office in Massachusetts to see if they have anything that they are looking at. If I see anything that causes me the least bit of concern, I then begin calling around to some of my colleagues in the FBI, in the Department of Homeland Security, and other parts of the intelligence community to see if they have any additional information.

In fact, when we had our situation in January where there was some concern about potential folks coming cross the Southwest border, coming to Boston with a potential dirty bomb, a good part of my morning was calling a variety of folks that I have developed strong relationships with here in Washington and in other states around the country at the federal, state and local level to see what I could find out they knew about the situation. I usually go through that process, sometimes in an expedited manner, before I do my briefing for the governor or for the secretary of public safety.

So the answer to your question is, every morning I am pinging my sources to see what they are hearing and what is going on. If I hear something that causes me concern, I then begin an aggressive effort to talk to pretty much everyone I can think of to see what they know about the situation that is concerning me.

Mr. KING. Who is responsible for the reverse part of the process as far as local intelligence going to Washington? Does that go through you or the local police chiefs on their own? How is that coordinated?

Mr. COHEN. In Massachusetts, we have now established a state-wide fusion center. They will do part of the process of what I just described earlier as far as checking each morning what is going on and put out a report that I would look at, instead of me making the phone calls. In our state, and this is being replicated in a number of states, local jurisdictions who want to report up can report directly to the HSOC through a variety of channels, the Homeland

Security Operations Center. At the same time, what we are asking them to do is to send it to us and the JTTF directly.

That is when there is a clear nexus with terrorism. For the most part, much of the information we are getting from localities, maybe reports of suspicious circumstances where they do not know if it is terrorism-related or not, or maybe just general crime information, because it is through the analysis of that general crime information, when we blend that with the intelligence we get from DHS, we are able to identify patterns and trends that may reflect a threat.

Mr. KING. Mr. Edwards or Dr. Colwell, do you have any comments?

Mr. COLWELL. I do. Thank you, Mr. Chairman.

I think, number one, I support the answers that Mr. Cohen gave and their accuracy. But I think when good questions, important questions like that are asked, it is important to put them in context.

There are 87 joint terrorism task forces in the United States. That is expected to grow to about 167. There are, depending on your definition, 53 to 57 major cities in the United States. So, much of the initiative and effort and challenge of the federal law enforcement community in a state is directed at where the population densities are.

When a question like that is asked and answered accurately and appropriately, it is in that context of what we are talking about, not out in these many, many 22,000-some odd municipalities around the country and 3,109 counties that serve, for the most part, small populations.

Thank you.

Mr. KING. The gentleman from North Carolina, Mr. Etheridge?

Mr. ETHERIDGE. Thank you, Mr. Chairman.

As you know, we have been talking a lot about the role of first responders and law enforcement and others, and of course you just touched on it a little bit, simply because we are a big country and terrorists do not determine where they are going to come in except where the soft spots are. It seems to me that is a soft spot that we have to find a way at a minimum to help plug.

Let me go back to one of the questions that was asked earlier, because a 2003 GAO report reports that local officials said that they did not receive timely and pertinent information. You have alluded to some of that, that we are making progress, from the Homeland Security or from the federal government, for that matter, in general terms overall. I must say to you, the first responders from my district tell me the same thing today that they did in this report.

I would like to know from a generic standpoint, Mr. Cohen and each one of you, if you would touch on it, yes, we are making progress, but it has been a long time. We have spent a lot of money. And to get there, it seems to me, number one, you have to have a plan. And number two, you have to work the plan. And number three, whether it is terrorism or just out and out pure crime, we may be looking for terrorists, but we ought to be looking for the criminals first, because it seems to me that is where it starts. These are criminals. They are international criminals. If we

get our focus in the wrong place and look for the big stuff, we are going to miss all of the opportunities to get the job done.

So I hope you will touch on that, because it seems to me it does not matter whether it happens in isolated Iowa or North Carolina, it has the same problem in the long run.

Mr. COHEN. Congressman, you have made some very important points.

The first point that I would like to talk a little bit about is the connection between terrorism and crime. In the state and local community, you are starting to hear about the all-hazards, all-crime approach to the intelligence process. That is critically important because terrorists do not come into this country and hide in a hotel room waiting for the day of their attack, and then suddenly come out.

They are involved in a whole host of activities, planning activities and pre-operational activities, many of which are illegal. They are involved in cigarette smuggling. They are involved in document fraud. They are involved in money laundering. They are involved in drug trafficking. They are involved in weapons trafficking. They are conducting surveillance activities. They are doing things that rise to the attention of local officials, either through crime investigations or reports being made to those state and local officials.

We should not be putting our state and local officials in the position of having to figure out when is something terrorism-related and who should they report it to. We should be putting in place a system that regardless of who they report it to, it gets to the right place so it can be analyzed and put into the national analytical mix.

You are right, there has been no plan for prevention and intelligence sharing up to this point, but we have been working aggressively, particularly over the last 6 to 9 months with the Department of Homeland Security, with the White House, with the Department of Justice, to think through these issues. With the passage of the Intel Reform Act, the creation of the Project Managers Office to begin the design of the information sharing environment, that provides an excellent opportunity to create the environment that you just talked about as badly needed.

Part of the other reason why we have not made more progress, I truly believe, is because I do not think consistently across the board at the federal level there has really been a true understanding of the value that state and locals bring. I think for the most part, state and locals were viewed simply, in the early days after September 11, as folks who responded after the attack occurred, which required a certain type of intelligence and information sharing. I think there is a growing level of sophistication that no, wait a minute, state and locals and tribal governments are important from a prevention perspective.

But it goes beyond that. Prevention is more than just conducting investigations. Prevention includes identifying at-risk locations, mitigating the risks to those locations. It means disrupting the environment so they cannot plan and carry out their operations. That requires a whole host of activities at the state and local level. While a growing number of officials are beginning to understand

that at the federal level, not everybody does yet, and that is a problem.

Mr. ETHERIDGE. Before we run out of time, I hope somebody will touch on this one too. Has a lack of leadership at the federal level up to this point created an informal network that has always been out there in law enforcement, that is growing and allowing for information to be shared?

Mr. EDWARDS. From the tribal perspective, that is certainly true, and DHS is leading the way. When you look at the NIMS and the NRP, anywhere you see federal, state and local, you see tribal. So we have actually been given a seat at the table, so therefore when we begin to talk and we begin to exchange information and see each other at exercises, we are beginning to establish that personal relationship. So yes, it is.

And when we look at the national preparedness goal and the critical task list and the universal task list, then we are beginning to come together with a lot of things that we were just doing in the regular routine parts of our job that now have true meaning based on that strategy.

Mr. COLWELL. Congressman, the things that have changed in my view—and I am talking about in the context of primarily non-urban, small town, rural America, where Interstate highways go through and trains and hazardous materials and waterways and water reservoirs, electrical grids and so forth exist—what has changed there is an understanding that they are part of a holistic approach to homeland security.

What is needed, and to a certain degree many efforts have been made to accomplish this, it is just hard to define what should you be on the lookout for at the local level?

When I say “local,” it is different than what Mr. Cohen says. When I say “local,” I mean outside the urban areas where the majority of our population lives.

It is an integral part of any holistic approach to homeland security. They are using computers more. Many of them still do not have computers, and they need the database links which are being provided. A lot of progress has been made and there is a lot of work left to be done.

Mr. COHEN. Congressman, can I just make one quick point?

I am not really sure why Mr. Colwell indicated that I am not referring when I say “local” rural communities. I think once you do the type of intelligence analysis that we are talking about, blending state, local, federal intelligence community information, you learn how these organizations operate. You then see how through those operations local communities are involved. You then can train those rural police officers, those rural firefighters what they need to be prepared for and what they should be looking for.

So when I say “local,” I mean urban, I mean rural, I mean suburban, I mean local.

Mr. KING. The gentleman from Pennsylvania, Mr. Dent?

Mr. DENT. Thank you, Mr. Chairman.

My question will be directed to Mr. Cohen.

The Homeland Security Information Network and the Joint Regional Information Exchange System, the is an issue that has been

created in my state's Homeland Security Office. I was just curious if you were part of that pilot effort in your State of Massachusetts?

Mr. COHEN. Yes, Congressman. The commonwealth is working closely with the Department of Homeland Security to do a statewide rollout of HSI and how we will be rolling it out as we will be putting a capacity or providing access to each locality, rural, suburban, urban, throughout the commonwealth, and routing that information both on a regional basis and on a statewide basis.

So as information rolls out and as information comes in or is put in, it will be routed to other regional entities of relevance as defined by our planning regions into our state fusion center and then to DHS and the FBI.

Mr. DENT. Has your experience in that program been useful and helpful? In my state, there has been some concern. I know some of the stakeholders, I believe, has disengaged from that process. Can you just give me your perspective?

Mr. COHEN. HSIN and the JRIES system have gone through some growing pains. I think the initial deployment of what was called at that point JRIES, there were some issues. I think it grew faster than they were prepared for and the technology could support. I think there was some frustration that came from that.

As they migrated JRIES over to the Homeland Security Information Network, to more of a portal-based system or an Internet-based system, I think that the capacity of the system has increased. So far, DHS, we have no complaints with how DHS has worked with us in the deployment of the pilot project. They have been attentive. They have been responsive to what we have talked about, and we are looking forward to deploying it.

Mr. DENT. Is your state currently exploring their own information sharing network, outside of the JRIES and HSIN system?

Mr. COHEN. Yes. We are looking at integrating our HSIN in deployment with the deployment of a statewide information management system that is going to be run out of our fusion center. And then we are also looking to leverage our Health Alert Network.

Mr. DENT. Would that be outside the JRIES system?

Mr. COHEN. It is a separate system, but they are all going to be integrated and fused together.

Mr. DENT. Okay. Thank you.

Does anybody else want to comment on that? Okay.

Thank you. No further questions.

Mr. KING. Thank you, Mr. Dent.

The gentleman from Rhode Island, Mr. Langevin?

Mr. LANGEVIN. Thank you, Mr. Chairman.

Gentlemen, I want to thank you for your testimony today.

Similar to the question that Mr. Dent was just asking, I guess I wanted to start and just go to Mr. Colwell for a second. I know there are several information sharing systems out there. There is RISS, which I am very familiar with. I know there is HSIN.

Mr. Colwell, can you compare and contrast a little bit the Pegasus system with some of these others? To what degree are we re-inventing the wheel and to what degree do you think it is possible that we can have just one information sharing system that everybody can get behind? It seems like there is a lot of duplication of effort out there.

Mr. COLWELL. Congressman, I believe that you referred to RISS. That is a criminal intelligence network system.

Mr. LANGEVIN. I bring that up because—

Mr. COLWELL. And the Pegasus program is—

Mr. LANGEVIN. —it is something we can build onto, which is what HSIN is.

Mr. COLWELL. The links, the communication links could be, and in many instances are coordinated, consolidated. The FBI has a LEO system and it is highly specialized and compartmented. All of them have great attributes, including the Pegasus program. The Pegasus program just links existing data and makes no attempt to interpret it or analyze it, so we are not in the intelligence business.

With the chairman's permission, I could submit for the record a written comparison of the systems. It would be quite instructive.

Mr. KING. Without objection, so ordered.

Mr. COLWELL. I might add that those descriptions on that comparison that I will submit is about 2 years old and the narratives in that description were submitted by each of the entities that are mentioned. They describe themselves. Pegasus did not describe them. I will submit it for the record.

Mr. LANGEVIN. Would either of you gentlemen like to comment?

Mr. COHEN. You know, Congressman, this is actually an issue that the working group that the governor chairs looked at.

There are a variety of systems. You have RISS, RISS-Net, LEO, Law Enforcement Online. You have the CDC's Health Alert Network. All of them are used to communicate certain subcomponents or information that could have a homeland security relationship.

I think we looked at the issue sort of two ways. One, the working group came out and said we want a single conduit coming from the federal government for threat-related information and intelligence. So if you are going to send to us terrorism-related or homeland security-related threat intelligence, pick a conduit, whether it is HSIN, LEO, RISS. Pick one.

On the other hand, we recognized that all of those systems that you have described or that we have been talking about play an important role in activities outside of those which are clearly identified as being terrorism related. So they are important. They need to be maintained because they support other activities that we need to be involved in each and every day.

So therefore, pick one to communicate threat intelligence; keep the other ones in place because they are valuable tools, don't make those the mechanism in which you are sharing defined threat-related intelligence.

Mr. EDWARDS. I think from the tribal and very rural law enforcement entities, and most law enforcement departments across the country, you know, 92 percent are less than 50 people in the department, and I think maybe 80-some percent of that 92 percent have less than 25. Many times, the problem is we do not have the equipment, the technology, the training, the personnel to be able to even access these information systems that are out there. So that is our first step, is just to get connectivity.

Mr. LANGEVIN. And on the issue of information sharing, I know you touched on this in some of your testimony already, but more specifically if you can expand upon it. In an August 2003 report,

the GAO reported that local officials routinely complained that the homeland security information they received was not timely.

For example, police chiefs reported that they often received critical homeland security information at the same time that the public received it. The chiefs blame the federal government's historical reluctance to share this type of information with local officials.

Can you discuss more fully what changes you have seen or witnessed in this culture, if you will, and what can be done to undo this historical reluctance to reach out to local officials? This reluctance clearly would place our first responders and our citizens at risk.

Mr. Cohen, you can start.

Mr. COHEN. I think there are a couple of issues there, Congressman. I think one issue, as an outside observer, but someone looking in, I think there is a pretty unwieldy process that takes place at the federal level as far as clearing and vetting intelligence that comes down to the state and local level. I think at times that process in itself may be part of the issue.

But I think there is a bigger issue, and the bigger issue is depending on where that intelligence resides, depending on what department, there may be separate systems or disclosure protocols that are in place. Here is an example. If the information or intelligence that is threat-related comes as a result of an ongoing JTTF investigation, and the communication of it to Boston, say, comes from a JTTF office in California to the JTTF office in Boston, the culture has changed dramatically as far as the FBI sharing that information with state and locals, but they share it with state and locals that are involved in the JTTF and involved in that criminal investigation or that terrorism investigation.

There is nothing wrong with that. That is really important. But at the same time they are sharing it with the other law enforcement entities, there is oftentimes a cultural reluctance to share it with those who are outside of the investigation. Now, I have been a law enforcement person for 21 years in different functions. Even though my current job is not strictly a law enforcement job, but I may need portions of that information or intelligence that is maintained by the JTTF to do some very important threat mitigation and planning activities.

So part of the issue is is that we have to develop a process that without compromising intelligence operations or law enforcement operations, information is shared outside of the investigative circle so that planning and protection activities can take place by those who are involved with it.

Mr. LANGEVIN. Does the other gentleman want to comment?

Mr. COLWELL. One of the things that is occurring now that did not exist previously, and I would add that there is a lot of progress that is not seen and noted that has been made since the GAO report in 2003. But one of the things that is occurring, there are some databases that are now accessible that were not accessible before to make inquiries of information at the non-urban area.

Mr. LANGEVIN. Thank you very much for your testimony. It is obviously clear we are making progress, but I still get the sense that we are in this mode of need to know versus need to share. We need

to be ever-vigilant in changing that culture. So thank you very much.

Mr. KING. Go ahead.

Mr. COLWELL. One footnote, Mr. Chairman. A lot of the technology that existed in the past was there, is being utilized to a more appropriate level. For example, the Pegasus program uses a priority software that overrides any other communication if it is from one law enforcement agency to another, which is an advance that was not commonly used in the past.

Mr. LANGEVIN. Thank you.

Mr. KING. The gentleman from the state of Washington, Sheriff Reichert?

Mr. REICHERT. Thank you, Mr. Chairman.

You said "Sheriff Reichert." I was the sheriff in Seattle, King County, Washington, for the last 8 years. I started out in a police car 33 years ago at 21 years old. So thank you for that honor, Mr. Chairman.

I have a question. It always boils down to me, at least for the last few years after September 11, and I have had a lot of experience in dealing with federal agencies, as you might imagine, over my 33 years. In this post-9/11 world that we live in, the gathering of information, the analysis of information, and the sharing of information really are the three key pieces to this puzzle.

There are a lot of initiatives out there. The integration initiative that was just recently announced by the Department of Homeland Security, which \$10 million and four cities have been identified across the nation. Seattle, King County is one of those chosen to participate.

Promises about local help are—I should say federal dollars in helping the locals construct a system where we can actually have first-hand, real-time information on the street for the people in the police cars, it is not happening. Difficulties with the U.S. Attorney's office in being a partner. Actually, the U.S. Attorney's office in Seattle has really stepped forward. The FBI at first would not participate because they did not want to share certain information.

So I guess my concern is that there are two—to help us get to the gathering, analysis and the sharing, local cops need help in funding personnel. We are supplying people to the federal task forces, to the joint analytical centers, and to the Joint Terrorism Task Force out of our own budget.

I think the Department of Homeland Security, I would hope, would take a close look at funding, and I know it has been their policy not to, funding bodies to help us in that area.

Can you comment on that, Mr. Cohen, first, and then others?

Mr. COHEN. Congressman, when you mentioned patrol cars, there is not a day that goes by that I do not wish that I am back to driving a patrol car. Life was a lot simpler back then.

I think you raise a very intriguing issue because on the one hand I think there are a lot of folks who will acknowledge that the frontlines on our homeland security efforts and our global terrorism efforts are the police officers that work at the local level, whether it is in a rural community or an urban community.

At the same time that we are asking them to take on more, raise their level of sophistication, increase their awareness about ter-

rorism, they are still required to handle their day-to-day jobs, handling bank robberies, drug traffickers, arresting prostitutes, handling burglary reports.

At the same time, most local communities are dealing with pretty severe budget issues. So we are losing police officers and firefighters, at the same time relying on them more to protect our communities from future terrorist attacks.

So yes, I think you raise a very valid issue and it is something we need to figure out because on the one hand, by asking them to do more, but on the other hand, as we saw with London, it is going to be those activities that probably provide our greatest chance at stopping the next attack. The next attack may not come from someone coming from abroad. It may come from someone who was born and raised in this country, who lived in the local community, and conducted all their planning activities in that local community or in that region prior to the attack.

At the same time, I do not know how you balance the fact that confronting terrorism is now part of what we do on a day-to-day basis from a state and local perspective. It means that we need to change the way we do business to take that into account.

So I think you raise a very valid point. There is definitely a resource issue from the standpoint of how can we be losing police officers and firefighters at a time when we need them more than ever, and at the same time there is how do we integrate this into their day-to-day business.

Mr. EDWARDS. I totally agree with what John is saying. I think one thing that we are really missing is the law enforcement officers that are on the street, particularly in the rural areas, being able to gather that information and know what information to gather, and feel comfortable in the environment that they are gathering it in, and feel like once they have put it forward, that they are getting some information back.

I think that is why you see the popularity of the state fusion centers, and the coming together there. I do think that we are making progress. We need not just personnel, but technical assistance, high-speed hookups. A lot of the local police departments say, well, it takes me maybe 10 minutes to download one information report or bulletin because I have a slow-speed dialup. These are things that we have to address at the local level and I think we could do that with a reasonable amount of funding to get people connected first, and then teach them what we need together, second.

Mr. REICHERT. Thank you, Mr. Chairman.

Mr. KING. Thank you, Congressman Reichert.

The gentlelady from Texas, Ms. Jackson-Lee?

Ms. JACKSON-LEE. Thank you, Mr. Chairman, for your kindness and indulgence.

I thank the ranking member and the committee, and I thank the panelists for their service. Many of us come from local government and understand the importance of your work.

Let me just, if I might, read a paragraph into the record, "From Hometown Security to Homeland Security." This was prepared by some good friends of mine, the International Association of Chiefs of Police. I think it is important because, Mr. Cohen, I think you have made it eloquently, as I have been here, and I know that Mr.

Edwards and certainly Dr. Colwell has made it very clear, law enforcement efforts to combat terrorism did not begin on September 11, 2001.

For decades prior to that fateful day, law enforcement agencies throughout Europe, Asia, Central and South America, and the Middle East and the United States were engaged in daily battles to apprehend terrorists and keep their communities safe from harm.

Of course, this does not have the United States, but I know that the work that many in law enforcement were doing certainly was in tune with potential danger or threats to the United States within their local communities.

I think it is important to put this on the record. This is a document prepared by the chiefs of police and seemingly was provided to us by the Democratic staff.

Mr. KING. Without objection, it will be made part of the record.

Ms. JACKSON-LEE. I thank the distinguished chairman.

That is the line of questioning that I would like to proceed with. Let me give you a little background for that.

Many of us on this committee, and some of us were on the Select Committee on Homeland Community, kept talking about the question of sharing of intelligence. I think we can be reminded, aside from some of the tendencies and the fear after 9/11 to stereotype, to racially profile, to suggest it was a particular religion or ethnic group. I kept saying, one, we should keep level heads, even in the midst of the enormous tragedy, and look at what happened. We can track it down to the issue of intelligence, sharing of intelligence.

We are reminded of the young FBI agent way out west, who had a document on her desk about an individual who was learning to fly without learning to land. That information did not translate, and Mr. Cohen I think I heard you mention the FBI, or the sheriff mentioned the FBI. They have made great strides now, but it did not get translated. It was not where it needed to be, the sharing of intelligence. I cannot imagine a more important point for this hearing today.

I will just lead into a question with this comment. On Monday, I was with, and Dr. Colwell, you mentioned rural communities. There are rural communities inside urban areas, and I happen to represent that kind of area in Houston where you can have a big city, but you go to areas that are not connected, if you will; 24,000 people in the Fifth Ward. But a very innovative nonprofit has established, with a homeland security grant or an appropriations that we secured, to put in a Web site in that community at a major place. One of the Web sites would include access to first responders information in time of, unfortunately, a crisis.

Interestingly enough, when it was reported, we know the bloggers are out there. BlogHouston.com reported and said, I do not understand what they are talking about. Everybody is always talking about safety. Here is another project that has the word "safety" in it. What does it mean?

So here is, you know, the smart bloggers could not understand that hooking up or putting technology or information sharing in a community to be able to understand what is going on a few miles down the road in downtown Houston, maybe there is some threat; maybe a chemical plant has exploded, did not understand it, could

not make sense out of it, which shows that we are not educating and securing the hometown.

So I would like to ask Mr. Cohen on this progress that we may or may not have made in respect to this area, and I will ask Mr. Edwards as well. You come from an area where you know well the goodness of the Minutemen, but obviously they have taken on another name. I think primarily because of the frustration on some issues, but also they have gone to suggest that they will be at both the northern and southern border.

What kind of informational access is important for you to have in order to make the point that you have it under control, and that the volunteers that we had in the revolution may not be needed at this time because you have the local support and state support that you need.

Mr. KING. If I could just ask the witnesses to try to expedite their answers because we do have two more questioners and we have another panel following it, and we have to be out of the room by 1 o'clock.

Mr. COHEN. Okay. Thank you, Mr. Chairman.

Congresswoman, what I need to know to do my job is I need to know as best as possible what individuals and organizations want to carry out attacks in the United States and of those organizations, which ones have the capacity to do it. I need to know how they operate, how they plan, how they structure their communications and transportation networks. I need to know what type of targets they want to attack, and I need to know how they want to do it. I need to know whether to invest my money in protecting against a thermonuclear bomb going off or someone trying to blow up an LNG tanker.

I think to your point, and you make an excellent point, is that if we do not have this type of intelligence, we have to rely on conjecture. If we rely on conjecture, then that is how racial prejudices creep into what we are doing. I think the vast majority of people involved in counterterrorism activities truly want to stop the terrorists from attacking our country. But if we do not give them the information to do it effectively, then that is when you are going to see people's civil liberties, privacy, and you are going to see racial discrimination enter into what we are doing.

Ms. JACKSON-LEE. Mr. Edwards, and, Mr. Colwell, if you would as well.

Mr. EDWARDS. Native American people have been practicing homeland security since 1492.

[Laughter.]

And you all will be relieved that we are still on the job today.

Ms. JACKSON-LEE. You are.

Mr. EDWARDS. We are still watching. Just like in World War II, we had a tribe from the Seattle area go out into the ocean in their canoes to spot German submarines off the coast. Now, what would we have done with the information that we got? We did not have any connectivity, but we would have fought to the death defending the country.

We are almost in the same shape today on our borders. We are there. We are watching. We are vigilant. We are American citizens.

We want to protect our country. We want to protect our freedom, but we need the tools to finish the job.

Ms. JACKSON-LEE. Mr. Colwell, and I know that yours is on information sharing, you might emphasize that, but the importance of what you are focusing on in terms of that local-to-local information sharing.

Mr. COLWELL. Thank you.

I think I agree with my colleague here. I want to state that there is a massive effort going on at the federal level in the midst of huge reorganization initiatives, homeland security; change of mission for the FBI; and also attempts to clarify what the threat is. I think more than anything else, the small towns and the rural, as well as the major cities, need clarity of the threats so they can take the risks that exist in that community and they will have a better idea of what they need to do to prepare themselves.

My view is that the preparedness for this also has to occur at the local level in addition to the initiatives that are being carried on by the federal government. But there is a lot of progress that has been made in sharing information, but there is a lot of work left to be done. It is a long, unidentified and unmet need, but it is now an imperative that this occur.

My view is that the more informed our local law enforcement, and when I say "local," outside the major metropolitan areas. The more informed they are, the more they will be responsible, and they will contribute in meaningful ways to our national security.

One last thing, crime has always been local. Even with terrorist events, it is still local crime in that, although there are federal laws and state laws. The local crime that occurs still goes on, still the same volume. The jails are still full, unfortunately, and the added burden of homeland security calls for extra resources and demands, but the local crime continues. It is just a question of clarity and helping give information so that people can act on their own and their own initiative in the context of homeland security.

Thank you.

Ms. JACKSON-LEE. Mr. Chairman, may I just put this in for the record to indicate that in dealing with the Minutemen coming to Houston, I convened local law enforcement called constables, and nobody has ever heard of them, but they had not received any terrorism training, which I gleaned from just having that meeting. So your points are very well taken.

I would conclude by saying I hope that we will have the opportunity of hearing from you distinguished gentlemen, but Sheriff Tommy Farrell, which I had hoped that we would have been able to hear from from Mississippi, who has that rural base of understanding of the lack of resources that he has no been able to receive during his tenure. I hope we will have that opportunity.

I thank you for your answers and your service.

Mr. SIMMONS. [Presiding.] The chair now recognizes the gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman.

Mr. Edwards, I would like to know more about the program that you have with various tribes and the Tribal Border Security Pilot Program. Is it stood up completely now? What are the objectives there? What do you do with respect to, if anything, those that are

on the border? What do you do with respect to immigration? How do you share intelligence with immigration? Has it changed since we now have the terrorist threat aspect involved in all of this?

Mr. EDWARDS. There are currently 40 tribes that are on or near the United States borders. They are usually not included in a lot of the homeland security planning, at least prior to the Department of Homeland Security including tribes in the NIMS and the NRP.

I think at that point, DHS realized that in order to have a good border strategy and protect our country from our borders which should be our first line of hard defense for our country, that we had to find out exactly what existed in capabilities with regard to tribes and what were their needs to achieve parity the tribal communities' emergency services and law enforcement and that of the nontribal areas.

We, to do this particular thing, developed a capabilities baseline based upon the national preparedness goals critical task list and universal task list to develop some kind of level that we could look and gauge and see and monitor where the needs may be and what capabilities we had to work with our neighbors.

We are almost completed with that. We have 38 of the 40 tribes participating, and the information that we got will be put into searchable databases that will be able to give us trends in different areas, and would also be a tool that we can use to show where improvements exist and accountability. And then if we have a problem, we can also pull from that 100-mile radius to the area of the critical incident, because every critical incident is local and you need to first pull in those resources. But the report is due to be completed by December of this year and we are well on our way.

Mr. LUNGREN. What is the geographic reach of those 40 tribes? That is, how much territory are we talking about? I am talking about border territory.

Mr. EDWARDS. There are over 225 land miles of border that are on tribal reservations, and there are also numerous waterways between the United States and Canada.

Mr. LUNGREN. Okay. This is a question for the entire panel. My perspective is based on the fact that I was here in Congress for 10 years, 1979 to 1989, left and went back to California. I was Attorney General there for 8 years.

While I was here in the Congress, I served on the oversight committees for the FBI and had very good relations with them. I thought everything worked well. Then when I was elected Attorney General, I found out that I was local or state and they were feds. And frankly, I ran into that problem.

I hear all this stuff about how we have improved the intelligence gathering, but it seems to me in many cases I discovered as the Attorney General, that the intelligence gathering was one way. We gathered it. They took it. We did not get much in return.

Mr. Cohen, you said things have improved. How much have they improved? Has the culture changed?

Mr. COHEN. You know, I used to think when I was a police officer that it was a bureaucratic or a turf issue, why information was not shared. I have now come by the FBI with state and local authorities. And the FBI is a great organization. They do a very important job.

Mr. LUNGREN. That is on the record. I do not want anybody to say we are attacking the FBI. I am trying to get to the problem, which is a continuing problem that I hear about from people in my state. I would like to know from your experience how much has it improved.

Mr. COHEN. It has improved, but it has only improved from the perspective that they share information and intelligence more effectively with those state and local law enforcement entities that are involved in the investigations that they are conducting. That makes sense, because from their perspective their mission is to conduct investigations into individuals and groups. From the JTTF perspective, they are conducting investigations into individuals and groups that may be involved in terrorism.

They do not focus on, from an operational perspective, emergency response planning, critical infrastructure protection, or risk mitigation, the activities that I have to focus on. So from their perspective and in their world, they are doing a better job sharing information.

Mr. LUNGREN. How about your world, your perspective?

Mr. COHEN. In my world, I get more of a response, and we have a great relationship with our local FBI, but the intelligence that I need most often comes through DHS because DHS has a multi-disciplined mission. They have a law enforcement response, risk mitigation, consequence management mission. They tend to provide me the intelligence in the format that allows me to carry out my multidisciplinary mission.

Mr. LUNGREN. Well, if they are gathering information and they get it from the FBI and they are sorting it and then they are getting it to you, that might be enough. Is it enough for you?

Mr. COHEN. Eighty percent of the time. There are times that it is not enough and I have to go through my own sort of interpersonal processes that I put in place.

Mr. LUNGREN. You see, that is what I am talking about. I found it was very serendipitous. That is, if we had a good personal relationship with a particular staff, it worked out. If we did not, it didn't. There was not a cultural imperative that the FBI was going to work closely with local and state law enforcement. I understand if they are investigating, local and state law enforcement, because of a question of public corruption. That is one thing, but I am talking about overall attitude.

I am just trying to figure out from your standpoint, where are we?

Mr. COHEN. I think we are getting better. We are not where we need to be. I think the culture is beginning to change. It has not changed yet. I think that even if the culture changes within the FBI in totality, they still do not operationally see themselves as part of the risk mitigation, consequence management process and they are going to be reluctant to share with entities outside of the investigative cycle.

Mr. LUNGREN. Mr. Edwards, with respect to the entities that you represent?

Mr. EDWARDS. Well, I think that the FBI has made great inroads in developing relationships and sharing information with local and tribal entities. They have developed at the associate-director level an Office of State and Local and Tribal Operations. They reach out

regularly to us. I was just at a briefing with them on intelligence and information sharing last Friday, and they are really focusing on what they can do. They have a ways to go. They know it, but they are taking those steps.

Mr. LUNGREN. Mr. Colwell, I know you are here for Pegasus and for particular systems, but you have tremendous prior experience with the FBI. Your comments?

Mr. COLWELL. I think it is a complex issue. I think it is important to note that the FBI has been mandated to change its mission and it is doing so, has done so. Any student of organizational change and development will tell you it takes at least 27 months for an organization that size to effectively start moving into its new mission and role. I think they are well on their way in that area.

They have been and are prohibited still with a lot of laws that prohibit disclosure to non-law enforcement personnel. I think they rely, in my observation they rely then on disseminating that information to a law enforcement official, and it is up to them to translate that to those that need to know in the community. Now, whether that is the best way to do it, I do not know, but that is one of the ways they exercise it.

Mr. SIMMONS. The chair thanks the gentleman.

Unfortunately, we are in a time constraint. We lose the room at 1 o'clock promptly, with votes perhaps at 12:30.

I think the line of questioning from the gentleman from California was excellent. When you talk about state and local in California, California is a state that is the size of a country, and so these are huge issues.

I would like at this point to recognize the distinguished ranking member of the Intelligence Subcommittee, and then move quickly to the next panel. The chair recognizes the ranking member.

Ms. LOFGREN. Thank you, Mr. Chairman. I am just going to ask one question, and hopefully then hear from the second panel.

The question I have really relates not how we can do better by sharing information, because I think that has been explored quite thoroughly and importantly, but really what protections we are putting in place, the other side of the coin.

Mr. Cohen, recently there was an editorial in the Boston Globe about the commonwealth fusion center. I am not saying they are correct, but they criticized the center by saying there was not accountability.

It reminded me of an issue that is currently being discussed in California, and I do not know the truth of it. The allegation is that the National Guard engaged in surveillance of a group called the Raging Grannies, where I think the average age is 75 years old, and a demonstration that was held on Mother's Day of the mothers of soldiers who have died in Iraq.

We need to look at that and find out whether or not that is true. I cannot say it is true, but that is not something we want to have happen, for two reasons. One, it violates constitutional rights of people to express their viewpoints; and two, it is a waste of time and money because the Raging Grannies and the mothers of the dead soldiers are not a threat to us.

What efforts, what steps should we put in place to make sure that we prevent that kind of, if that were the case, I do not want

you to say that it is because we do not know that, but that sort of thing, to protect against that kind of misstep, if you will?

Mr. COHEN. Thank you. That is a great question, Congresswoman.

First of all, one of the things that we have made a key part of our statewide homeland security strategy is that we sort of dispel the notion that security only comes at the violation of privacy rights and civil liberties. That is a false choice and it is wrong. You can be aggressive in fighting crime. You can be aggressive in fighting terrorism and still respect privacy and key civil liberties that are the foundation of this country.

We are putting in place an advisory committee that is going to include the civil liberties community and privacy experts to help us think through issues regarding not only our fusion center, but also issues regarding homeland security in general. But I think at the end of the day, the most important protection we have is allowing open and broad oversight.

My one concern from a personal perspective is as we have gone down the road of expanding accessibility to information, as we have gone down the road of trying to think through how state and locals fit into this mix, we have, one, tried to bring them under the umbrella of the intelligence community, which according to our working group everyone believed would be a huge mistake; and secondly, we sort of push back oversight, whether it be legislative oversight, media oversight, or independent oversight bodies within the executive branch.

So I think it is important that we are aggressive. I think it is important that we work to protect our communities, again whether it is from crime or terrorism, but we also have to put in place aggressive oversight mechanisms to protect and make sure privacy and civil liberties are protected.

Ms. LOFGREN. Do the other two witnesses have comments on this?

Mr. EDWARDS. Well, my beautiful mother is 75 years old, and she is still threatens to go up the side of my head whenever I get out of line.

[Laughter.]

Ms. LOFGREN. But she is not a threat to the nation.

Mr. EDWARDS. Yes. Let's hope not. As a federal officer, I may be alone. At least I was. And she is always right, no doubt.

But, you know, I think that we have to have the federal government in the form of Congress and the courts, Supreme Court on down, to define for the local law enforcement and gatherers of the information, what information is to be gathered. Once we do that, then they will know exactly what their limits are and they will go after that.

Mr. COLWELL. There is a lot of precedent for that. All one has to do is look at history in the 1960s and 1970s and it can prove to be quite instructive on the concerns that you expressed. Title 28, Part 23, I think, attempts to address this and what the law enforcement agencies can do and should do, especially when federal funds are involved.

So I think it is always an area that must be of concern, and law enforcement needs to be sensitive to.

Ms. LOFGREN. Thank you very much.

I yield back.

Mr. SIMMONS. Thank you.

I think a quick review of the green books of the Church Committee or the brown books of the Pike Committee will show that when the United States goes down that path, nobody benefits and nobody wins. The purpose of intelligence collection and analysis is to defend Americans and their freedom and their liberties, not to in any encroach on those. So I think it is a good question, and I think the answers from the witnesses have been excellent.

I want to thank this panel for appearing before us today.

I would like now to invite the next panel to come to the table.

It is my pleasure to welcome General Matthew Broderick, director of the Homeland Security Operations Center. He will be representing the Department of Homeland Security. He served for over 30 years as an infantry officer in the U.S. Marine Corps; commanded platoon, company, battalion and brigade level; attended the Marine Corps Amphibious Warfare School, the Armed Forces Staff College, the Naval War College and has a distinguished military career.

He is joined by Mr. Josh Filler, director of the Office of State and Local Government Coordination for the Department of Homeland Security.

I would express to both gentlemen that you have had an opportunity to hear from panel one. You have heard the questions of the members of the subcommittee, as well as the distinguished ranking member of the full committee. We would encourage you, given the fact that we may be called for votes at 12:30 or 12:45, and we lose the room at 1 o'clock, we would encourage you to summarize your testimony and then give the members maximum opportunity to ask questions.

That being said, we will start with General Broderick.

Ms. LOFGREN. Excuse me.

Mr. SIMMONS. Yes

Ms. LOFGREN. I just would like to make a comment. Mr. Filler's testimony was not received until 7:30 this morning, and the rules of the committee and the House require that the testimony be submitted at least 24 hours in advance or 48 hours, I don't recall which, but certainly before 7:30 of the day. I recall hearing in the last Congress where the chairman of the Judiciary Committee actually adjourned the hearing because Mr. Ziegler had late testimony. I am not suggesting that we do that today, but I do think that it is worth noting and we expect better than this. I hate to be critical, but I must be. The committee deserves an opportunity to review the testimony.

I thank the chairman.

Mr. SIMMONS. I thank the gentlelady for her comments.

We could pursue that further, but perhaps we will wait for General Broderick and Mr. Filler to make their comments, and then if they wish to respond on that issue, we would be happy to hear what they have to say.

General Broderick, welcome, and we look forward to your testimony.

**STATEMENT OF BRIGADIER GENERAL MATTHEW BRODERICK,  
DIRECTOR, HOMELAND SECURITY OPERATIONS CENTER,  
DEPARTMENT OF HOMELAND SECURITY**

Mr. BRODERICK. Good morning, Chairman Simmons, Ranking Member Lofgren and distinguished members of the committee.

It is my privilege to come before you today to discuss the primary ways the Department of Homeland Security shares information through its operations center and through its Homeland Security Information Network. Because I was asked to expedite this, I will summarize it in a few minutes.

The Homeland Security Operations Center is a 24–7 operation. It is probably one of the largest ones in the country. A large operations center, even by military standards, would be 35 or 40 people on a shift. We have up to 84 people on one shift representing federal, state, local and even county-level representation.

It facilitates security information sharing and operational coordination with federal, state, local, tribal, territorial and private sector organizations. The private sector is a new entry that we are proud to say that we have been able to pull in with us. It comprises over 35 federal, state and local government agencies.

It has three primary missions, two of which are core. One is to try and detect and report suspicious activity throughout the United States. The other core mission is to coordinate incident management during catastrophic events within the United States. The submission within that is to provide domestic situational awareness throughout the United States and a common operational picture that everyone can participate in at any level.

Currently, as you know, DHS leads in controlling the U.S. borders and ports of entry. Because of that, we have new insight into who is coming into the borders, who is coming at the borders, and who is inside the borders, with ICE, CVP, Coast Guard and TSA all combined now under one organization. That provides us with great insight into who may be within the borders that is a threat to the United States, or who or what is coming at the borders. It allows us to collect that data each day from situational reports from these components and then share that information with the entire intelligence community and as appropriate with other federal, state and local organizations and private organizations.

What people do not realize is that that is a 24–7 job for us, looking for suspicious activity, collecting it, and then passing it on and making sure it is shared appropriately with all agencies and all entities.

The second core mission, as stated in the National Response Plan, is to share information and coordinate actions during catastrophic events. It is the primary conduit for the White House and the Secretary of Homeland Security to provide domestic situational awareness when we do have a catastrophic event.

It also provides a common operational picture in situational awareness for the Interagency Incident Management Group that meets during a catastrophic event. The IIMG are senior-level executives from all the government agencies that form in the Homeland Security Operations Center and provide courses of action and recommendations on how to mitigate a major national disaster.

The Homeland Security Operations Center also monitors all the major events in the United States. There are five different types. The national special security events, or the NSSEs, are the major events usually sponsored by the federal government, inaugurations, conventions. We provide people to those cities as part of a staff with a principal federal official and the connectivity back to the Homeland Security Operations Center so that we will have good connectivity and good situational awareness throughout an event.

The other four categories of events go from size from New York City at the New Year's Eve event, which is a category one, down to a category two which may be the Super Bowl; category three may be the Kentucky Derby; and a category four may be less. What we do, though, under three and four is that we go into this local or state and offer our assistance. We go to local sheriffs, if they are the ones responsible for the security around that event, offer them assistance and assessments of critical infrastructure. They may not be aware that they have great security around that forum, but that there is a chemical factory up-wind a half-mile away. We also agree to provide them any pertinent information on intelligence that may have an effect on that event.

The third part of homeland security is the Homeland Security Information Network. We have broken that down into communities of interest. One of the communities of interest is law enforcement, and that law enforcement subdivides into two communities of interest. There are the major law enforcement intelligence agencies, the big ones. There are about 124 of them, and we put that in a community of interest called law enforcement analysis.

We also have another portal for law enforcement, and that is just law enforcement sharing. All law enforcement agencies go in there and they share information within that portal. We have a portal for emergency responders. Those are basically hooked to all the emergency operations centers throughout the country. We have HSIN Intelligence. That is now linking intra-DHS, our own internal intelligence agencies. We have HSIN International, which links us with Great Britain, Canada and Australia. We have HSIN Secret, and that is a new program being rolled out on existing networks to all the states, territories and 18 major police departments in the United States. It will be online this fall. We have HSIN Critical Infrastructure.

We have 40,000 members from private industry on that network. These are vice presidents of security, Texas Gas and Oil; vice president for security, Texas Instruments; Northrop Grumman; Boeing, a very large audience. We asked for 16,000 in our pilot and 40,000 signed up. We are in 17 major states right now.

Mr. SIMMONS. If you could summarize, General.

Mr. BRODERICK. Yes, sir.

Homeland Security Information Network is the network the country needed to link all agencies together, fire, emergency responders, leadership and police.

Sir, it has been a privilege to pass this information to you. I conclude with my prepared remarks and I will be happy to answer any questions you may have.

[The statement of Brigadier General Broderick follows:]

PREPARED STATEMENT OF MATTHEW E. BRODERICK

### **Introduction**

Good morning, Chairman Simmons, Representative Lofgren, and distinguished members of the Committee. It is my privilege to come before you today to discuss the primary ways the Department of Homeland Security (DHS) shares information through its Operations Center and the Homeland Security Information Network.

### **Homeland Security Operations Center (HSOC)**

The Homeland Security Operations Center (HSOC) is a standing 24/7, interagency organization that is the national-level hub for domestic situational awareness and operational coordination pertaining to the prevention of terrorist attacks and domestic incident management. The HSOC facilitates homeland security information sharing and operational coordination with other Federal, State, local, tribal, and private sector organizations. It comprises over 35 Federal, State, and local government agencies.

The HSOC has three primary missions:

- Daily receipt and reporting of information from all available sources on suspicious activity, throughout the United States
- Incident management during catastrophic events within the United States
- Domestic situational awareness and development of common operating picture

Currently, DHS has the lead for controlling U.S. borders and ports of entry. The HSOC's day-to-day responsibilities include identification of possible terrorist threats to the Nation by collecting and reporting suspicious activities on who or what is approaching, attempting to cross, or residing within our borders. Collection and reporting of that information is shared with the entire Intelligence Community (IC), with a primary focus of providing information to the FBI, the National Counter Terrorism Center (NCTC), and the Office of Information Analysis (IA) within the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate. Those entities, rather than the HSOC, perform the intelligence analysis function. The information also is shared with other appropriate Federal, State, and local agencies, as well as with the private sector, primarily via the Homeland Security Information Network, which I will address momentarily.

The most critical element of the daily information gathering and refinement cycle is sharing the information gathered with IA, which then passes on possible threats to the Office of Infrastructure Protection. The HSOC follows a structured timeline throughout the course of the day. Beginning at midnight, DHS organizational components submit daily situational reports that are collected and vetted by the HSOC prior to being passed on for analysis. This provides a cursory first screening of information to avoid an inefficient use of IC analytical resources. This information also serves as material for the Secretary's morning brief and for the interagency Secure Video Teleconferencing (SVTC) that takes place twice daily. A product called the Homeland Security Operations Morning Brief, comprised of mostly suspicious activity reports minus any information on U.S. persons contained within criminal intelligence protected by privacy laws, is shared on a Sensitive but Unclassified (SBU) level with about 1500 Federal, State, and local intelligence and law enforcement agencies and subscribers. In the morning and afternoon, a SVTC occurs with NCTC as chair and other members of the intelligence community. Information obtained the day before is discussed and shared as are requests for specific actions. DHS has been able to provide new insight and visibility into this process with its reports on who is entering, or trying to enter our borders; information, which in past years, would have been stove piped within individual agency data bases. Midmorning, all agencies within the HSOC meet and an intelligence brief is shared with all representatives and they are encouraged to share this information with their respective agencies. At the end of each day, HSOC-generated items are closed out or passed forward, if appropriate, and the cycle begins again.

As stated in the National Response Plan (NRP), another core mission of the HSOC is to serve as the national-level hub for information sharing during catastrophic events within the United States. It is also the primary conduit to the White House and the Secretary of Homeland Security for domestic situational awareness. Sharing of information and operational coordination is conducted through Emergency Operations Centers (EOC) at Federal, State, local, tribal, and regional levels, with the State Governors and their Homeland Security Advisors, as well as in relevant format with the private sector. During these incidents, situational awareness is also passed to the Inter-agency Incident Management Group (IIMG).

The IIMG, comprised of subject matter experts at the Assistant Secretary and Senior Government Executive level from most Federal agencies, is established within the HSOC. The IIMG provides strategic level recommendations and courses of ac-

tion, prior to and/or during a catastrophic event, for consideration by the Secretary and other senior officials. In order to allow these representatives the time to focus on courses of action and recommendations, the IIMG members have reciprocal desk officers within the HSOC to provide them with continuous situational awareness and for requests for information.

The HSOC is also responsible for monitoring special events. These events come in five levels dependent upon the situation participants and estimated crowd number. The five levels and examples are:

National Special Security Events (NSSEs): Inaugurations, etc

Level 1: New Years Eve in New York City

Level 2: World Series

Level 3: Kentucky Derby

Level 4: Local Events

In each case, the HSOC offers senior watch officers to support major events in other cities or helps local officials “plug in” to national level intelligence and information sharing as it pertains to their particular event.

#### **The Homeland Security Information Network (HSIN)**

The Homeland Security Information Network (HSIN) is the primary conduit through which DHS shares information on domestic terrorist threats, suspicious activity reports, and incident management between and among all DHS stakeholders. It is set of tools and data sources that support DHS customers defined as users within multiple communities of interest (COI). It also provides collaboration and information sharing while enabling the stakeholder organization to determine the information and communications streams of value to its needs. The HSIN is a capability that provides secure and protected, real-time interactive connectivity among users at all levels of government, critical sectors and private industry with the HSOC.

The HSIN directly supports the Department’s strategic goals to identify and understand threats, assess vulnerabilities; determine potential impacts and disseminate timely information to our homeland security partners and the American public; and detect, deter, and mitigate threats to our homeland. Specifically, it is designed to allow users to gather and fuse all terrorism-related intelligence; analyze and coordinate access to information related to potential terrorists and other threats; develop timely, actionable, and valuable information based on intelligence analysis and vulnerability assessments; ensure quick and accurate dissemination of relevant intelligence information to homeland security partners, including the public; and provide operational end users with the technology and capabilities to detect and prevent terrorist attacks, means of terrorism, and other illegal activities.

HSIN is a user-friendly system. It enables Federal, State, territorial, local, international, tribal and private sector users to communicate and share information both with each other and with DHS in a real-time, secure and protected Web-based environment. This system provides participants direct access to an extensive suite of functions: mapping, a robust search engine/library, instant messaging and chat (collaboration) and an information-posting capability which interfaces with both DOJ’s Law Enforcement Online (LEO) and the Regional Information Sharing System (RISS) networks. We currently have tens of thousands of users and we project to have hundreds of thousands of users by FY07.

Currently, the HSIN Communities of Interests include:

- HSIN Counter Terrorism (HSIN-CT)*: the common portal for all Federal, State, territorial, tribal, and local government agencies to share information relating to counter-terrorism and incident management
- Law Enforcement (JRIES LE-A)*: for law enforcement agencies that have major intelligence analysis departments (~150 or more members)
- Law Enforcement (LE)*: for all agencies dealing with LE Sensitive data (F/S/L) that meet the DOJ definition of Law Enforcement Sensitive
- Emergency Management (EM)*: for Federal, State, tribal, and local levels (local refers to county/major city) emergency operations centers to deal with major incidents
- HSIN Intelligence*: being set up for use by the internal DHS intelligence community
- HSIN International*: allows for rapid dialog between the HSOC and Canada, the United Kingdom, and Australia during a crisis
- HSIN SECRET*: an immediate, inexpensive, and temporary approach to reach State and local homeland security and law enforcement sites that can receive Secret level information, pending full deployment in fiscal year 2007 of a new DHS Secret backbone called HSDN

*Critical Infrastructure Warning Information Network (CWIN)*

The Critical infrastructure Warning Information Network (CWIN) is a Federal government-operated network within HSIN that provides mission-critical, yet survivable, connectivity. CWIN Communities of Interest, include:

- Entities in the private sector vital to restoring the nation's critical infrastructures(e.g., electrical, information technology, and telecommunications)
- Entities in the Federal and State government, vital to maintain government-wide connectivity with DHS; sector-specific agencies and resources; State Homeland Security Advisors; and Emergency Management Centers.

Most importantly, CWIN provides survivable DHS capability for information sharing and collaboration for critical infrastructure restoration when primary forms of communication such as the Internet and Public Switched Telephone Network (PSTN) are inoperable because it is not dependent on the public internet or PSTN. CWIN is used routinely for testing and exercises as well as information sharing to ensure operational readiness when the need arises.

#### *HSIN Critical Infrastructure (HSIN-CI)*

The HSIN-CI program was designed, implemented, and deployed as a DHS-directed and regionally coordinated private and public self-governing program, with a vetted audience (approximately 40,000 members, 90% private sector) for national, regional, and local information sharing and all hazards, 24/7 alerts and warnings. The technology to support the program field operations was installed in the secured facilities of the FEMA Regional District Offices in FEMA regions IV, V, VI, and X. Participation includes private and public members from the 19 states within these regions and, because the program uses the Internet, HSIN-CI has membership from all 50 states.

The HSIN-CI program is administered through Regional Managers from the FBI's Field Intelligence Groups, at the direction of the HSOC. CI members nationwide promote the HSIN-CI program within their areas of expertise, creating a self-administered and vetted private and public membership built upon existing relationships and communication lines that is locally administered and governed in coordination with DHS (HSOC). Public notification options in HSIN-CI include two-way voice and short message service (SMS) messaging based on current location and/or proximity to an event, and a publicly available collection of suspicious activity reports. HSIN-CI members can submit reports, as well as receive sector/location-specific information from submitted reports.

#### *HSIN Critical Sector (HSIN-CS)*

HSIN-CI is designed to enhance the protection, preparedness, and crisis communication and coordination capabilities of the nation's 17 critical infrastructure and key resource sector owners and operators, HSIN-CS is primarily a mechanism for information sharing and collaboration within each specific critical infrastructure sector and the Federal government.

The following is the list of Critical Infrastructures and Key Resources, as defined by HSPD-7: Agriculture and Food, Public Health/Health Care, Drinking Water and Waste Water Treatment Systems, Energy, Banking and Finance, National Monuments and Icons, Defense Industrial Base, Information Technology, Telecommunications, Chemical, Transportation Systems, Emergency Services, Postal and Shipping, Government Facilities, Dams, Commercial Facilities, Nuclear Reactors, Materials, and Waste

#### *HSIN/US Computer Emergency Response Team (HSIN/US-CERT)*

This is the focal point for addressing cyber security incidents within the federal government. The portal is an information dissemination mechanism to communicate relevant cyber information. Using a suite of tools such as secure messaging, forms, secure chat rooms, alerts, and shared libraries, US-CERT pushes necessary information to a broad or targeted audience, as required.

#### *HSIN Current Status*

The HSIN is operational in 50 States, the District of Columbia, five U.S. Territories, 53 major urban areas, Emergency Management Agencies, Homeland Security Advisors' Offices, Governors' Offices, State Law Enforcement Agencies, National Guard Centers, mayors of major cities, Emergency Operations Centers, and city law enforcement agencies. It is operational in three foreign countries: the United Kingdom, Canada, and Australia. HSIN SBU is currently being expanded at the state and local level through a pilot program involving 7-8 States in order to determine how the system can best be utilized within different governance structures. HSIN SECRET is being deployed and tested at 50 state EOCs and 18 additional State and local LE activities. There are pilot programs in 11 Information Sharing and Analysis Centers (Electric, Water, Food and Agriculture, Public Transit, Oil and Gas, Nuclear, Dams, Chemical, Postal, Nonprofit, and Health/Public Health). Plans are in

place to begin deployment of a SECRET level component of HSIN to State and Local sites, and HSIN is being rolled out to all DHS component agencies.

HSIN has become a cornerstone of the Department's ability to communicate with homeland security partners and stakeholders across the nation. We will continue to build on our success as we extend connectivity to a wider user population and improve the tools availability for communication, collaboration and analysis of information.

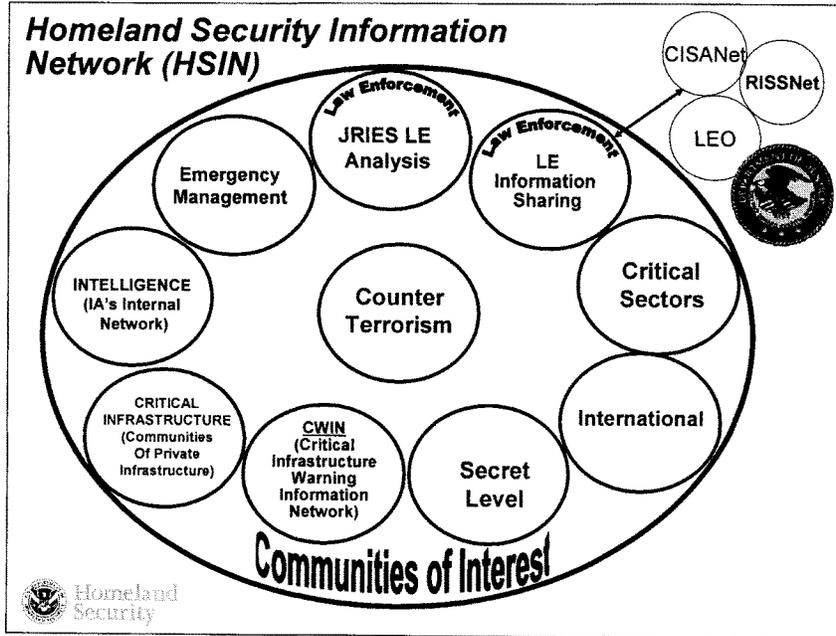
This concludes my prepared remarks. I would be happy to answer any questions you may have at this time.

## Annex A

## HSOC Composition

- INTEL & INFRASTRUCTURE PROTECTION
- Central Intelligence Agency
- Defense Intelligence Agency
- National Security Agency
- National Geospatial Intelligence Agency
- Federal Bureau of Investigation
- Department of Interior (US Park Police)
- Drug Enforcement Administration
- Alcohol, Tobacco, and Firearms
- United States Secret Service
- Immigration Customs Enforcement
- Federal Protective Service
- Federal Air Marshal Service
- Transportation Security Administration
- Customs and Border Protection
- United States Coast Guard
- Department of Energy
- Department of State
- Department of Defense
- Department of Transportation
- Postal Inspection Service
- Environmental Protection Agency
- US Capitol Police
- DC Metro PD
- VA State Police
- Fairfax County PD
- LAPD
- NYPD
- INCIDENT MANAGEMENT
- Department of Veterans Affairs
- Department of Health and Human Services
- Federal Emergency Management Agency
- National Oceanic Atmospheric Administration
- OVERARCHING
- Border and Transportation Security
- State and Local Coordination Liaison
- Science and Technology Directorate
- Public Affairs
- Information Analysis Office
- Infrastructure Protection Office
- Geo-Spatial Mapping Office
- ON AN AS REQUIRED BASIS
- Nuclear Regulatory Commission
- US Department of the Treasury

Annex B



Mr. SIMMONS. Thank you very much. We will put the full statement in the record. For the record, I enjoyed my visit out to the HSOC. You run a tight ship, and thank you for your service.

Mr. Filler?

**STATEMENT OF JOSHUA D. FILLER, DIRECTOR, OFFICE OF STATE AND LOCAL GOVERNMENT COORDINATION, DEPARTMENT OF HOMELAND SECURITY**

Mr. FILLER. Thank you, Mr. Chairman and Ranking Member Lofgren, and members of the subcommittee.

First, I do want to apologize for the late presentation of the testimony. All I can say is that it will not happen again in the future.

I am Joshua Filler. I serve as the director of the Office of State and Local Government Coordination at DHS. I want to thank you for the opportunity to appear before you today to discuss the department's intelligence and information sharing programs with state, local, territorial and tribal governments around the country.

As the committee is well aware, the exchange of information between the department and our partners is crucial to the mission of Homeland Security. Our efforts consist of keeping our partners informed of and facilitating their participation in DHS policy and program development.

We have a number of methods that we employ in order to share information with all of our partners around the country. As General Broderick indicated, we have our Homeland Security Operations Center. Within the HSOC, we also have a state and local watch desk. This is a 24-7 watch that maintains constant connectivity to state and local officials, law enforcement, EOCs around the country 24-7.

We also host bi-weekly calls with all of the state homeland security advisers. John Cohen is actually one of them. We do that every 2 weeks. We have a formal agenda. We discuss issues. We exchange information, best practices and basically maintain open lines of communication.

We also host monthly national organization calls, which includes all of the law enforcement, first responder, National Governors Association, U.S. Conference of Mayors, every month similar to the bi-weekly call. We have an agenda. We have subject-matter experts that come on and brief issues, and again maintain that ability to keep in touch and make sure we are communicating on a regular basis.

We also obviously share information in the context of intelligence and incident management. We do this at both the classified and the unclassified level. As General Broderick noted, much of this information is shared by the HSOC and our Office of Information Analysis through the Homeland Security Information Network. It is also shared by the state and local watch desk and through teleconferences, faxes, and secure email.

To date, DHS has provided over 250 unclassified and classified homeland security threat advisories and bulletins, including joint DHS-FBI bulletins to our state, territorial, tribal and local partners. Of that 250 number, approximately 225 are at the unclassified level. These bulletins have included summaries of terrorist tactics used overseas, such as in Madrid, Baghdad, Riyadh and more;

potential threats to jurisdictions or economic sectors in the homeland; potential terrorist indicators; and assessments of the strategic intent and capability of al-Qa'ida and other terrorist groups to attack the United States.

Of course, all of the DHS operational components, CBP, ICE, Coast Guard, regularly share information at the tactical level with all of their partners at the local level.

DHS has also facilitated a clearance program for state, local and tribal officials around the country. While we are committed to sharing information at the unclassified level, we know there are times that information should be shared at the classified level. So currently we have more than 250 state and local government officials with either secret or top secret level DES clearances. There are an additional 150 state and local officials who have non-DHS clearances that have been permanently certified with the department so that we can regularly share classified information with them as well.

We have also deployed numerous communication modes, systems including video teleconferencing capability to every state in the country, two in fact to every state. One is in their EOC; the second is at the state's choosing. We are also in the process of deploying secret telephones to every state and many major urban areas around the country.

DHS is also deploying a secret-level data network, the Homeland Security Information Network that General Broderick oversees. We are in the process of putting that out at the secret level as well.

Just to sum up, I think it is important to note that while we talk about all the different modes and methods of sharing, if I could just very briefly walk you through what happened on July 7 when London was attacked. On that morning, when DHS learned of the attacks, the Department of Homeland Security immediately began reaching out to our federal, state, tribal and local partners. This included the secretary personally calling key governors and mayors in major states and cities that had large mass transit systems, urging them to immediately deploy additional security to those systems.

The department later, through my office, hosted two national unclassified conference calls with all 56 states and territories, major cities and counties from around the nation. Shortly thereafter, the deputy secretary hosted a similar national call and announced that the alert level would be raised to Code Orange for the mass transit systems only. I then personally hosted a call and we told all the first responder associations, tribal organizations and other government organizations that we were raising the alert level.

Later that day, the department, jointly with the FBI, released a bulletin outlining what had happened in London and giving the best intelligence picture we could at that time.

Mr. Chairman, I know my time has run out. Let me just sum up by saying I again appreciate the opportunity to be here and am happy to answer any questions you may have.

[The statement of Mr. Filler follows:]

## PREPARED STATEMENT JOSHUA D. FILLER

Mr. Chairman, Ranking Member Lofgren, and Members of the Sub-Committee: I am Joshua D. Filler and I serve as the Director of the Office of State & Local Government Coordination (SLGC) at DHS. I want to thank you for the opportunity to appear before you today to discuss the Department's intelligence and information sharing programs with state, local, territorial, and tribal governments, and for your ongoing support of the Department of Homeland Security's efforts to keep America secure.

As the Committee is well aware, the exchange of information between the Department and our state, tribal and local partners is crucial to the mission of homeland security. SLGC, in addition to its other authorities and responsibilities, currently serves as a national coordinator and clearing house in DHS for information sharing between the Department and state, local, territorial, and tribal governments as well as the first responder community. We operate under the basic premise of providing as much information as possible to those who need it. We accomplish this using several different methods of coordination and information dissemination.

Our efforts consist of keeping our partners informed of and facilitating their participation in DHS policy and program development actions, such as implementation of the Real ID Act, the Security and Prosperity Partnership, the National Response Plan, and the National Preparedness Goal. We also issue press releases and other announcements covering the full range of homeland security events, including grant announcements such as FIRE ACT grants and Law Enforcement Terrorism Prevention Grants; the Secretary's public speeches and testimony, including his recent testimony before the House and Senate on the future of DHS; and fact sheets on major homeland security issues such as mass transit and maritime security, critical infrastructure protection, identification of fraudulent passport documents, and much more. All of this information is provided to ensure that our partners are kept constantly up to date on what DHS is doing and that they are made a part of the process.

#### **Information Sharing Methods**

DHS employs a number of methods to share this kind of information and to keep the information sharing channels open at all times. First and primarily, DHS maintains the Homeland Security Operations Center to be the "eyes and ears of the Nation" for homeland security. The HSOC is a 24 hour a day, 7 days a week operational watch. Within the HSOC is the State and Local Watch Desk which is the primary communication arm for sharing all of the information I just described with our state, local, territorial and tribal partners, and for certain intelligence and incident management information that I will describe in more detail later in my testimony. The State & Local Watch has access to multiple points of contact within each state and from around the nation including police chiefs, tribal leaders, fire chiefs, homeland security advisors, emergency managers, governors, mayors, and county officials.

Second, the Department, through SLGC, hosts bi-weekly conference calls with the state and territorial Homeland Security Advisors and other officials to ensure they have a consistent and formal means of communicating with the Department on general issues. The calls are split into three parts: the Northeast; the South and parts of the Mid-West; and the Mid-West and Western states. The calls are an open forum for the free exchange of information and an opportunity for collaboration between DHS and our partners and include a formal agenda, read-ahead materials and subject matter experts from across the Department and the government as a whole.

Third, DHS also hosts a monthly conference call with all of the state, tribal, local and first responder associations to provide them routine updates on what is happening at DHS and the federal government as a whole and for the opportunity to exchange ideas and best practices. Like the bi-weekly calls these association calls include a formal agenda, read ahead materials, etc. Recent calls have included information on the Port Security Exercise Training Program (PortStep) and updates on the Department's Second Stage Review process.

Finally, SLGC and other DHS officials from all of our components stay in constant contact with our partners through other less formal means. We regularly attend conferences and meetings around the country to brief our partners on what is happening at the federal level and to hear from and learn from our partners directly on what is happening in their jurisdictions. We also work with the Office of the Private Sector to make sure that there is a constant, mutual exchange of information with our private sector partners.

All of these methods and interactions that I have described help to ensure that DHS stays in touch with its key partners in securing the homeland.

**Intelligence and Incident Management Information**

DHS shares intelligence and incident information at both the classified and unclassified level. Working with our partners in the federal government, DHS works to ensure that our partners at the state, tribal and local level have useful information they can either act upon immediately, use for situational awareness, or for strategic planning and more. Much of this information is shared by the HSOC and our Office of Information Analysis through the Homeland Security Information Network (HSIN), the State & Local Watch Desk, or through teleconferences or video teleconferences, secure faxes and secure email.

The Information Analysis and Infrastructure Protection element of DHS participates in the Intelligence Community Information Sharing initiatives through the Community Interoperability and Information Sharing Office under the DNI. DNI policy is that all terrorist related intelligence is disseminated at the unclassified level through the use of "tearlines." The majority of this kind of information can and should be shared at the unclassified level. This ensures maximum distribution among the first responder and homeland security community around the nation. DHS has worked hard with the Intelligence Community to "write to release" classified information into unclassified products as rapidly as possible, while ensuring the protection of intelligence and law enforcement sources and methods. This will continue to be a priority.

Since its inception, DHS has provided over 250 unclassified and classified homeland security threat advisories and bulletins, including joint DHS and FBI bulletins, to our state, tribal and local partners. These have included summaries of terrorist tactics used in overseas attacks, such as in Madrid, Baghdad, Riyadh and more; potential threats to jurisdictions or economic sectors in the homeland; potential terrorist indicators and assessments of the strategic intent and capability of al-Qa'ida and other terrorist groups to attack the United States.

The operational components of DHS also routinely share information with state, local and tribal officials. For example, in close coordination with DHS/IAIP, the Coast Guard disseminates intelligence information throughout all levels of government and, where appropriate, the private sector. They are able to provide actionable tactical intelligence to Coast Guard operational commanders and state and local partners through Maritime Intelligence Fusion Centers (MIFC). At the state and local level, the Coast Guard facilitates information sharing between government partners through Area Maritime Security Committees (AMSC). The Coast Guard has also created Field Intelligence Support Teams (FIST) to collect and report intelligence information and liaison with federal, state, local partners. Furthermore, Coast Guard Investigative Service (CGIS) conducts investigations that produce actionable, human intelligence.

In addition, CBP Border Patrol Agents routinely work with and share information and intelligence with local, state, tribal and federal law enforcement agencies. One example is the Integrated Border Enforcement Teams (IBETS) along the Northern border. In many IBET locations there are local, state, federal and Canadian government representatives with whom we share information to increase operational effectiveness.

The United States Secret Service is also involved in task forces with state and local law enforcement partners. One such task force, the Electronic Crimes Task Force, is comprised of computer and electronic experts that perform forensic analysis and investigations into computer and electronic crimes.

Finally, Immigration and Customs Enforcement (ICE) maintains two tactical intelligence facilities that collect and disseminate real-time and operational information and intelligence, in both the maritime and land border environments. This information is shared with Intelligence Community and law enforcement agencies at the state, local and tribal level, in a variety of formats, and at multiple classification levels.

While DHS is committed to sharing information at the unclassified level, we know there are times that information should be shared at the classified level to ensure maximum specificity. DHS also provides such classified information to our partners on a routine basis.

In order to better share classified information, DHS grants federally-sponsored security clearances to appropriate state, local and tribal officials with an ongoing need for access. There are currently more than 250 state and local government officials with SECRET and TOP SECRET-level DHS clearances, and there are an additional 150 state and local officials with non-DHS sponsored clearances who have been permanently certified (perm-certed) to DHS to allow them to participate in the Department's classified briefings and receive classified products. Furthermore, the Department has funding for several thousand more SECRET-level clearances for state,

local, territorial, tribal, and private sector homeland security officials who can demonstrate an ongoing need for access to classified information.

The Department has also deployed several classified SECRET communications systems. In 2003 and 2004, DHS deployed two secure Video Teleconference (VTC) units to each state. One unit has been placed in each state Emergency Operations Center (EOC) and a second has been placed in each Governor's Office, or an alternate location of the State's choosing. DHS now has the capability to host all 50 states at once at the classified SECRET level.

In addition to the VTCs, DHS has deployed secure telephones to each state and several local governments. A secure phone has been deployed to each state EOC as well as to each state Governor's Office or alternate location. DHS also now has a secure conference call capability that is capable of hosting 18 secure calls simultaneously at the SECRET-level. SLGC is also working with the Office of Security and the Office of the Chief Information Officer to deploy several hundred excess secure phones at little to no cost to cleared state and local government officials with a need for additional phones.

DHS is also deploying a classified, SECRET-level data network called HSIN-SECRET that Director Broderick will discuss in more detail. This system is being deployed to every state and to 18 additional state and local homeland security and law enforcement sites. HSIN-SECRET will be available through a dedicated laptop computer and by those officials with a clearance on file with DHS and a HSIN-SECRET user account. Upon its completion, HSIN-SECRET will allow the Department to rapidly disseminate classified threat data and other information to state and local officials.

While a summary of modes of communication is important, let me provide the Sub-Committee with a few important examples of how some of these modes work and the type of classified and unclassified information that is shared. Recently, DHS hosted a national threat update via SECRET VTC with all 50 states, the FBI and the National Counter Terrorism Center (NCTC). The briefing consisted of an update on a variety of threat streams and lessons learned from tactics used in Iraq and other overseas locations. The briefing was followed-up with a written classified summary distributed to all 50 states.

An even more recent example involves the London bombings. On the morning of July 7, 2005, upon learning of the attacks, the Department immediately began reaching out to our federal, state, tribal and local partners. This included the Secretary contacting key Governors and Mayors to discuss the London attacks and the need to provide immediate additional security in major mass transit systems.

After further consulting with the Intelligence Community later that morning, the Department, through SLGC, hosted two national unclassified conference calls with all 56 states and territories and major cities and counties from around the country, along with the FBI. On the first call, the Secretary outlined what had happened in London and discussed the possibility of raising the alert level in the United States. Shortly thereafter, the Deputy Secretary hosted a similar national call and announced the alert level would be raised to Code Orange nationally for the mass transit sector only. I then personally hosted a call with all the first responder and state, tribal and local associations to announce the raising of the alert level. Later that afternoon, DHS and the FBI released a joint unclassified bulletin to our partners outlining the intelligence picture we had and the basis for raising the alert level for mass transit in the United States along with specific protective measures for the mass transit sector. Towards the end of the day, another national call hosted by DHS with the Coast Guard and the U.S. Department of Transportation was held to announce the raising of the maritime security level to MARSEC 2 for passenger ferries carrying 150 passengers or more.

### **Tribes**

As mentioned before, the sharing of information does not extend only to the states and local governments; tribal governments are also an important information sharing partner. To build relationships and share information about the Department with tribal officials, DHS personnel regularly participate in tribal association meetings, conferences, and other events including the National Native American Law Enforcement Association annual conference, the National Congress of American Indians annual conference and the United South and East American Indian annual conference. The Department also worked directly with the leadership of the Mohegan and Mashantucket-Pequot Tribes from Connecticut in 2005 during the Top Officials (TOPOFF) 3 exercise.

At this time, the majority of the unclassified threat information communicated by DHS to the tribes is distributed via email to appropriate officials as well as posted on HSIN. The Department's ability to communicate information to the tribes is lim-

ited by a lack of email connections among tribal leaders; however, we have been working to bring tribal nations into HSIN. Several tribal nations in California and Arizona are currently using HSIN.

#### **Fusion Centers**

As the Sub-Committee is aware, many states and large urban areas have established intelligence fusion centers to better collect, analyze, and disseminate homeland security information. Several federal agencies, including DHS components and the FBI have representatives working in these fusion centers. The Department's Homeland Security Advisory Council Intelligence and Information Sharing Working Group and the Department of Justice's Global Justice Information Sharing Initiative have worked closely to establish baseline standards for fusion center to operate under. The Department will continue to work with all of our partners, including the DNI, DOJ, and state, local, and tribal officials, to further enhance these standards and integrate these fusion centers around the nation.

#### **Conclusion**

Information sharing with our state, territorial, tribal, and local partners is one of the key priorities of the Department of Homeland Security. Since September 11, 2001 we have made tremendous progress in this area. However, we still have much more work to do. We at DHS will continue to make adjustments, we will continue to enhance our methods, and we will continue to work closely with all of our partners to better secure the homeland.

Once again, I thank the Sub-Committee for providing me this opportunity today as well as for their continued support and valuable input. I look forward to answering any questions you may have.

Mr. SIMMONS. I thank you, General Broderick and Mr. Filler.

A very brief question from me, and then I will defer to the distinguished ranking member.

I talked earlier about cultural changes in the intelligence community in our government with regard to intelligence information sharing. I also understand that the Department of Homeland Security is in the process of a reorganization. If the Homeland Security Operations Center, which is currently part of the IAIP, is taken out of that entity, how might that affect positively or negatively your mission for information sharing? That is question one.

And then to you, Mr. Filler, for all of the host of calls and bulletins and other activities that you are engaged in, what kind of feedback loops do you have in the system where your customers, the people that you are contacting and communicating with, have the opportunity to tell you how useful that is so you can tailor that program to their needs?

Mr. BRODERICK. Sir, in response to your question on the HSOC, we do not intend to change the way the HSOC is currently set up. We realize that that is really the fusion point between ops and intel and that it must remain and actually get more robust. But we do not intend to break that synergism. As you know, there is a high side with a lot of intelligence, and a low side with the consequence management and a lot of law enforcement. We intend to keep that fused together.

The positive part of the reorganization is that it gives the HSOC now a direct voice to the secretary and it also allows the HSOC to go down faster on the operational side and try to work operational coordination at a level that we did not have before. Before, there was a buffer. Border and Transportation Security oversaw many of our components. So it was another layer.

The layer worked fine except that it was slower in the process. Now we can go directly down to these operations centers, access that information, get it back up and hopefully coordinate with state and locals faster. So the process should be fast.

Mr. FILLER. Sir, we actually exercise as number of ways to get feedback. Most of the time when we actually put out a product to our partners; we actually have a customer satisfaction survey attached to the document so they can informally tell us whether they found the information useful, timely, so on and so forth.

For those who would prefer a less formal means, one of the purposes of my office is to be a conduit to our state, tribal and local partners so that they have a place to go to tell us what is working, what is not working, and do so in a confidential way if they want to, but to make sure that their concerns are getting into the senior leadership of the department. Sometimes they do that through a confidential conference call; other times through the biweekly calls that I described they will take the opportunity to pass that information there. But there are very, very, very robust methods to get that information in.

Mr. SIMMONS. Thank you very much

The chair now recognizes the distinguished ranking member of the full committee, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Last week, this committee heard testimony with respect to transit security. One of the things we found out is the department did not have a transit plan for security. A lot of this came about because of the unfortunate situation in London. We have since found out that there are some 100-odd deadlines that the department just ordinarily has missed, most of which have been requested by Congress.

General Broderick, I see that Chairman Rogers in House Appropriations deducted \$5 million from the administration's request because the Homeland Security Operations Center did not provide the mandated 5-year implementation plan. Where are we on that plan at this point?

Mr. BRODERICK. Sir, we submitted the 5-year implementation plan from my office on time. It has had problems working its way up through the system, but at my level, we were able to provide that out we thought in a proper time. The implementation plan is in effect. We do know where we want to go as far as the Homeland Security Information Center, and where we want to go with our system, and where we want to go with our center and how we want to develop those systems.

Mr. THOMPSON. If this plan that you refer to is in effect, can you provide members of this committee with a copy of it?

Mr. BRODERICK. Yes, sir. I would be glad to.

Mr. THOMPSON. And so do I assume that whoever is reviewing whatever you submitted, that it is still somewhere in the pipeline for review?

Mr. BRODERICK. Yes, sir. My concern is trying to gain back that \$5 million and I have been requesting that it be pushed almost on a daily basis.

Mr. THOMPSON. Mr. Chairman, I would just like to note for the record that in my sitting on various hearings before a committee hearing testimony, what the general is saying is not unusual. It appears that the people who have the responsibility for preparing many of the documents requested by Congress, they are actually

doing their job. But for some reason along the way, the process is more or less stymied, if not stopped.

I think at some point we will have to perhaps ask the secretary if he can unblock the logjam by which we have heard testimony that occurs from getting the congressionally mandated reports to a committee, because I think it is important for all of us to have the information, since some of the information obviously is for various plans for different departments. I think we, along with the public, should have a right to know.

I yield back.

Mr. SIMMONS. I think the ranking member's point is well taken. Certainly, the loss of \$5 million is an adverse impact for the Department of Homeland Security. Our interest here is to strengthen and oversee that department and make it as effective as possible. That is, I think, our goal. So I welcome the ranking member's comments on that subject.

The chair now recognizes Mr. King, the gentleman from New York.

Mr. KING. Thank you, Mr. Chairman.

I want to thank General Broderick and Mr. Filler for their testimony.

I would like to focus, Mr. Filler, on your situation, since you really are in a unique position of being at both ends of this process, having served in New York City and now being at the federal level.

Which deputy mayor did you report to, Rudy Washington or Joe Lhota?

Mr. FILLER. Joe Lhota.

Mr. KING. Joe Lhota. Okay.

Again, thank you for your service to New York. Obviously, New York was in the forefront of providing local protection for antiterrorism, and I want to thank you for that.

You sat here during Mr. Cohen's testimony. He made a number of points basically saying that the system is not where it should be; that occasionally conflicting information is given out; sometimes too much classified information is given out. If you were back in New York right now and you were dealing with some federal bureaucrat called Josh Filler, how would you feel you were being treated? How would you feel the information was? Would you feel that the system was working properly?

Mr. FILLER. I would say he is working hard, trying to do the right thing.

[Laughter.]

Mr. KING. Spoken like a St. John's man.

[Laughter.]

Mr. FILLER. I would say, Congressman, that yes, things really have gotten better. I notice even in the time from 9/11 to my departure in New York City that things were getting better; that the shock of that event really did drive a lot of good things happening. But as John Cohen said, they are not where they should be. There are still times where information is not shared or if it is shared, it is so compartmentalized that people who do need access to it do not have it or their underlings have it and senior leadership at the local level or state level might not actually have it.

So I think great progress has been made on two fronts. On the cultural side, I do think that we have changed the culture in part in law enforcement and intelligence, but it has not been changed to the point where it needs to be. I think development of systems like HSIN, the creation of DHS, all of these things have helped push the ball down the field. But if I were at the local level, I would still probably be frustrated at times that I am not getting all the information I think I need, or there may be times where I am getting conflicting information from different federal agencies.

So again, I think we have made a lot of progress, but we still have more work to do.

Mr. KING. Do you feel within your own department that some of the agencies you have assumed control over are not cooperating fully with each other, have not accepted the concept that they are now working for the Department of Homeland Security and they still have their own turf they are trying to protect?

Mr. FILLER. I would say this, that the integration of DHS is an ongoing process, and the second-stage review and the secretary's reorganization of DHS is designed precisely to that point, to make sure that we are organized in the best possible way to achieve our mission. That includes integrating our operational capabilities, integrating our intelligence capabilities.

So while, again, I think a lot of integration has gone on over the last 2 years, we are obviously not where we should be and I think second-stage review bore some of that out and the secretary has now made a decision on where he wants to go.

I think everyone in DHS comes to work in all of the former 22 legacy agencies with the idea of how can they better secure the homeland; how can they better work within their department; and how can they better work with their partners at the state, tribal and local level. What we need to do is create an environment for them where they can do that in the best possible way.

Mr. KING. General Broderick, do you have anything to add to that?

Mr. BRODERICK. I agree, sir. I think that the second-stage review showed that there were warts out there, and rightfully so. I mean, people build organizations that have a lot of pride and when we came in, we asserted ourselves over them as the "higher headquarters." It is like the federal government over state and local. There is always going to be that little bit of friction of we are those guys.

But I think that with the second-stage review and trying to build this one team and this faster conduit for coordination with the ops and the intel, the recipient on the other end, the state and local are going to find that it is a lot smoother organization, and we can get information to them quicker.

Mr. KING. I want to thank both of you for your service.

I think that it is easy for us to find fault. I am not trying to do that. I think what the committee wants reassurance on, though, is that the process is going forward; that the department realizes things are not perfect; they realize that local police are not getting the full cooperation, probably more so from the FBI than Homeland Security, to be honest with you, but at least they still feel that there is a certain breakdown in communication.

I think what we again really want is the assurance that you realize that and you are moving forward, and I really commend you for what you are doing.

Mr. Filler, again, thank you for what you did in New York City.

Mr. SIMMONS. I thank the gentleman from New York.

I am now going to recognize the gentlewoman from Texas, Ms. Jackson-Lee, with the caveat that I will stick to the 5-minute rule because we are going to lose this room at about 12:50 p.m.

The gentlewoman from Texas?

Ms. JACKSON-LEE. I thank the chairman very much. It must be attributable to lawyers, and I am not sure if the gentleman is, but when we are probing we are probing, but I thank him for his kindness.

Let me also thank you, Brigadier General, for your work and certainly let me thank seemingly a good friend of my friend from New York, Congressman King, and we thank you for your service as well.

I just want to focus on this question of local translation of intelligence, if I might, and really say what I have said in earlier remarks that I think this is the key to our security. People laugh, but I do think hometown security is homeland security. I sit next to a very distinguished member of Congress from New York, and I have not heard of one homeland security meeting where the Congresswoman has not spoken about the need for assistance and resources in the local area.

But let me share with you what I said earlier about the structure in Texas. It is a law enforcement group called Constables. I think part of the issue is in working with Washington and working with the corporate headquarters, if you will, is knowing what is happening outside the beltway. And so, I would be interested in finding out first of all what efforts have been made, if you will, to understand the structure in our local communities.

I bring up the Constables because there have been some efforts to do threat and terrorist training with conspicuous entities, police, sheriffs. But when you get down to many areas in this country, they have their own names. For example, I am sure there are different names on Indian reservations or pueblos that do not fall into "police." So I am concerned that we are not connecting by getting the information from local communities, to find out what their structures are.

I will be asking the Homeland Security Department to give training to Constables and their staff because they were left out of the loop when that training came into our region. But I would first like to pose that question.

What better ways are you working to ensure that you know the structures and you are reaching those local entities that may not be as well known and conspicuous, but work in the areas that first responders work?

I would also ask the question, does the reorganization that Secretary Chertoff announced last week have any direct impact on better improvement of local-state communication, meaning Homeland Security's local-state communications?

Mr. FILLER. Congresswoman, that is a very good question. I think it raises a very important point. We need to understand our partners. I think we do it in two ways at DHS.

First, my office in particular, when we hire people, we try to hire people who have a background at the state, local or tribal level. In fact, we have someone from Texas in my office in a very senior position who works with local governments, so I am familiar with Constables, and I learned it from him.

And so I think that is a very important part of what we do, not only within my office, but throughout the department, that we bring people in who understand how things operate, how they are structured at the local level, county level, tribal level, state and territorial level. So I think if we do those things, that will obviously help the department's internal mechanisms better understand its customers.

Secondly, I think aggressive outreach, and that is another part of what my office does, maintaining that constant contact, getting to know people, getting to know their structure, their leadership, their laws and rules that govern them. Not every state is the same. Not every county is the same. Not every city is the same.

I come from New York, which is a strong home rule state. So the mayors of those cities have tremendous responsibility and independent authority from the state. New Jersey, just across the river, is different. The governor there is a very powerful executive and the state wields great authority.

So understanding these distinctions is absolutely critical, and I could not agree with you more.

Ms. JACKSON-LEE. Brigadier General, and as you answer that question would you just also add the ways in which your intelligence analysis is different from the NCTCs, and particularly as it may relate to being effective in getting intelligence to our local communities. Are you just analyzing the same data or are you bringing in a new perspective to the analysis?

Mr. BRODERICK. To answer that last question first, ma'am, NCTC looks at information globally, so we are actually providers and then we are takers. The great thing about that is they are getting their information from multiple sources, both internationally and nationally, and then they are able to push it back down. What we try to do is we try to look at it from a state and local perspective when we get it.

What is it that domestic U.S. intelligence requires? What do we need out of that?

So as they push that information back down to us, we are able to go back with requests for information that we think are more structured for state and local people, and try to get it down to actionable intelligence, unclassified, or the lowest level of tear-lines that we can get when we push that back down.

So we are hoping that we are being the advocate for the state and locals, and we are trying to push that information down as quickly as we can in actionable-type informational form.

Mr. SIMMONS. The chair now recognizes the gentleman from Washington.

If the gentlewoman from Texas wants a third round, we will accommodate her.

Ms. JACKSON-LEE. I thank the chairman.

Mr. SIMMONS. The gentleman from Washington?

Mr. REICHERT. Thank you, Mr. Chairman.

I do agree there has been progress in the last couple of years, so congratulations on that work. I also appreciate the fact that you recognize there is a lot more work to do, as all of us recognize that absolutely true fact.

How important do you think first responders are in collecting intelligence information on a day-to-day basis during their job on the street, when it comes to homeland security?

Mr. BRODERICK. I think that is the domestic intelligence collection effort. I think that is where the rubber meets the road. We clearly recognize that that is where we are going to really get the information and quickly and on-hand. We are going to get information that might not have gone through normal intelligence channels. It may have just been something that a very savvy police officer saw in the street and questioned, and that may be the key to the puzzle.

We have noticed in the U.K. on other instances that it is just an observant law enforcement or private citizen who noticed something a little different, and they reported it, and it was able to go up, and they were able to prevent several incidents. I really believe that that is where it all starts. That is why HSIN now is going out at the local level. We have hit the state level. We have hit the major city level now. We have gone to the first seven states and offered free to link all of their local communities in both fire, emergency response, and their emergency operations centers and try to link that so that they can share that information with the state, with themselves and up to us.

Mr. REICHERT. Are you familiar, either one of you, with the LINKS system?

Mr. BRODERICK. Is that the one in Washington State?

Mr. REICHERT. Yes, sir.

Mr. BRODERICK. Yes, sir. I am sort of, sir.

Mr. REICHERT. Sort of. Well, I guess that is my point. We do not have a seamless, really a system in place to share that kind of information, so if a first responder is very important in collecting that data.

For example, not too long ago we had a state trooper stop someone on the highway, and they were written a citation and they were allowed to leave. Two months later, as the ticket goes through the process, we recognize that this is a person who has committing crime and sending money to Al Qaida. So we had to track that person down again.

If we had real-time information in those police cars, and that has been something that I have been working on since September 11, as the sheriff in King County, with the Seattle Police Department, in connection with LINKS, but it has not happened yet.

I commend you for the cooperative effort and the energy that you are putting forth there, and the relationships that need to be built, which are absolutely necessary.

But back to where the rubber meets the road, it is action that has to happen. There has been a promise that has been proposed to us through the FBI and the U.S. Attorney's office in King Coun-

ty and Seattle. Do you see that coming together in the near future sometime?

Mr. BRODERICK. Yes, sir, I do. As I said, we have not started the third phase. We went to the state level. We went to the major city level. Now we are starting at the local level. But simultaneous with that, we are working with the FBI on all their major products that they have out there—LEO, RISS—and we are trying to get that all to be interoperable so that all that information is shared through one database and we can turn it around and get it back out there, or we can recognize that is actionable intelligence and get the proper authorities.

Mr. REICHERT. Is the DHS integrated initiative certainly a key factor or key component of this effort?

Mr. BRODERICK. Yes, sir.

Mr. REICHERT. Anaheim, Seattle?

Mr. FILLER. I am familiar with the Anaheim, Seattle, and there are two others.

Mr. REICHERT. Cincinnati.

Mr. FILLER. Cincinnati. And yes, I think we are constantly looking at ways to try to make these things interoperable. I think the integration effort is really a technology effort. We are trying to find some best practices in the technology field that we can then use in other parts of the country. I think one of those things obviously is our ability to integrate different systems. I know Matt's office has worked very hard to try to integrate RISS, LEO and HSIN, but there are obviously other systems that should be integrated as well.

Mr. REICHERT. Great.

Thank you, Mr. Chairman. I yield the balance of my time.

Mr. SIMMONS. I thank the gentleman from Washington.

The comment was made that the gentlewoman from New York, Ms. Lowey, is a great expert on homeland security. That has certainly been my observation. I thank her for her patience, and she is now recognized for her questions.

Mrs. LOWEY. Thank you, Mr. Chairman.

I would like to follow up on your comments, General.

First of all, let me thank the General and Mr. Filler for your presentations.

If there are seven states chosen for some coordinative mechanism between firefighters, police, EMS workers, I certainly have not been aware of it. Frankly, since the beginning of our contact with Homeland Security, we have been asking for a federal initiative on interoperability because we continue to get no direction.

I am a New Yorker. My district is just north of New York City, but I consider myself part of a region. I must say, Mr. Filler, I have been tremendously impressed with the work of Ray Kelly and the New York City department. But if there is an interoperability plan with some direction from the Department of Homeland Security that is operating in seven states, I would love to give you the opportunity to brief me further on it and perhaps I will use my time for that.

Mr. BRODERICK. Yes, ma'am.

Mrs. LOWEY. Is that what you referred to? Did I hear incorrectly?

Mr. BRODERICK. No, ma'am. What we have done now is the third stage of going out with HSIN is to go to individual states, and New York was the first state we went to, and offer to link all the emergency operation centers, the police departments and the leadership into whatever system they wanted. What we did not want to do is be prescriptive. We wanted the states to come back and tell us how they would like to organize themselves and how they would like that information to flow and to link each other.

We work with Bart Johnson at the New York State Police. He has hooked us into their fusion center. New York State already has a very intricate system on its own, and they asked us to link in at the fusion center and at several larger points, but that they felt that the system underneath them was adequate at this time, and they are re-evaluating whether they need to take HSIN and use that system.

Mrs. LOWEY. I am not sure what that really means. I appreciate the opportunity, Mr. Chairman, to pursue this.

We have been looking for direction from the Department of Homeland Security. In fact, I recall probably a year ago there was an RFP that went out so that the Department of Homeland Security could get some direction down to the localities about the interoperability of their systems. I am really shocked to know that New York State thinks everything is just fine.

Now, when you go down to the state, do you hear problems of frequency? This is an issue in New York City. It is an issue in Westchester County. I have been hearing this for 3 years. Right now, no one is talking to each other.

And so I am still a little confused as to what you are offering the state and what they say they have. If you are implying that the state thinks that they have an effective interoperability system so that they can communicate with information sharing, I am puzzled, and maybe I should go to my next question. Could you explain?

Mr. FILLER. I think I can try, Congresswoman. I think there are two different issues here. I think we are talking about interoperability of a data network, HSIN, RISS, LEO, versus interoperability of communications, primarily radio communications, during an incident which obviously was something that the 9/11 Commission and others looked into.

The issue of interoperability of communications primarily through radio communications is really something that the SAFECOM Office and our Office of Interoperability and Compatibility has been looking into for some time.

Mrs. LOWEY. Have they accomplished anything?

Mr. FILLER. Well, there a number of?

Mrs. LOWEY. We will not deal with that since it is not your office. So you are focused on the information sharing. I misunderstood.

Mr. FILLER. Correct.

Mrs. LOWEY. Okay.

Mr. BRODERICK. Yes, ma'am. I think you were talking about radio communications, ma'am. I was talking about something else.

Mrs. LOWEY. I see. So I will not burden you with that question because we are still waiting to get response on the other. It will be 4 years I guess in September, but maybe we will get it right eventually. I am optimistic.

Let me get to the question about the information sharing. Perhaps you can clarify it. Are there tools inherent to homeland security operations center dispatches that allow the local enforcement officials to hone in on information that might be relevant to them, without having to comb through information that is not? How is this done when you are either the General or Mr. Filler?

Mr. BRODERICK. Ma'am, we are now establishing what we are calling a current operational picture. It is based on iMAP data. iMAP is geospatial data that lays down all infrastructure and what all the cities and even many of the rural areas possess for infrastructure. Within that layer, though, we are building intelligent suspicious activity layers where law enforcement people can come in and just access those layers and pull out the information they need. They have the ability to come in and look at key infrastructure and query that infrastructure and see how that infrastructure is progressing in their area, whether it needs protective measures, how it is going to influence certain events that are going on in that community.

This is a progress in being right now, but we are working with L.A., Washington, D.C., on what local police departments would need to go in and pull that out without having to query through all of our other data. They can go in and use it at their own time.

Mrs. LOWEY. I see my red light is on. Thank you, Mr. Chairman.

Mr. SIMMONS. I thank you very much. I would be happy to extend to the gentlewoman an additional couple of minutes if she would like to take them.

Mrs. LOWEY. Thank you for the generosity. Then perhaps I will pursue that.

If you are increasing the availability of actionable information to local law enforcement, what I hear is really a dearth of funds locally, and they need the funds to be able to move forward and to implement. How can you ensure, or how will you ensure that locals have the funds sufficient to ensure that this information can actually be used?

Mr. BRODERICK. Well, I will let Josh answer the rest of that. On my side, ma'am, both with HSIN and with COP, the current operational picture, it is free to them. So we provide all the means necessary for them to do that.

Mr. FILLER. The fact that it is free I think obviously helps, but there is a wealth of funding, as you are well aware, that has been distributed to first responders, state and local governments since 9/11. We have specifically outlined to them that much of that funding is eligible for information sharing to buy the systems, the equipment, the software so that they are able to actually analyze data, share information among themselves and with the department.

Mrs. LOWEY. I will not pursue this, but you must know that maybe New York City is different, but most of my communities do not have a fraction of the money they need for training, for equipment purchases. And there really has not been sufficient money that is coming down to the local. Even New York City, which has been able to benefit from some direct grants does not have what they need, as you well know. So I think after developing the plan, we need to make sure that the locals have what they need to implement it.

Thank you, Mr. Chairman.

Mr. SIMMONS. Thank you very much.

I want to take this opportunity to thank our witnesses for providing their very valuable testimony.

I remind members that we have additional time to submit questions for the record. The record will be held open for 10 days to submit questions. I believe that the distinguished ranking member of the committee requested a report of the General, and we would look forward to seeing that report, understanding that it has not been cleared through the department, but perhaps we can see it in some form in response to questions from members of the subcommittee.

Let me just conclude by saying that information sharing is a critical component of our homeland security, now and into the future. And yet information sharing, intelligence information sharing is something new and different, so there are challenges involved. This subcommittee, the members of this subcommittee, I believe all want to be participants in making this process work.

I lost constituents on 9/11. I do not live in New York. I live in Connecticut, but my daughter lives in New York. On 9/11, the apartment that she occupied was not reoccupied because of that terrible tragic attack. Members of my family continue to live in New York City and in other areas that are potential target areas.

So we feel a certain sense of urgency, as I am sure you do as well, that we want to be successful; that we do not want another attack. And we certainly do not want to think that at some future date those who oppose us would be successful because we held a piece of information that was not shared.

So again, thank you for your testimony. Thank you for your service to the country.

Hearing no objections, this hearing is now adjourned.

[Whereupon, at 12:38 p.m., the subcommittee was adjourned.]

