FACILITATING AN ENHANCED INFORMATION SHARING NETWORK THAT LINKS LAW ENFORCEMENT AND HOMELAND SECURITY FOR FEDERAL, STATE, AND LOCAL GOVERNMENTS

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JULY 13, 2004

Serial No. 108–254

Printed for the use of the Committee on Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE
98–119 PDF WASHINGTON : 2005

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

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. McHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LaTOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, Jr., Tennessee
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
MARSHA BLACKBURN, Tennessee
PATRICK J. TIBERI, Ohio
KATHERINE HARRIS, Florida

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
BETTY McCOLLUM, Minnesota

———

BERNARD SANDERS, Vermont (Independent)

Melissa Wojciak, *Staff Director*
David Marin, *Deputy Staff Director/Communications Director*
Rob Borden, *Parliamentarian*
Teresa Austin, *Chief Clerk*
Phil Barnett, *Minority Chief of Staff/Chief Counsel*

Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan
DOUG OSE, California
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio

WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
——— ———

Ex Officio

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

Bob Dix, *Staff Director*
Chip Walker, *Professional Staff Member*
Juliana French, *Clerk*
Adam Bordes, *Minority Professional Staff Member*

CONTENTS

FACILITATING AN ENHANCED INFORMATION SHARING NETWORK THAT LINKS LAW ENFORCEMENT AND HOMELAND SECURITY FOR FEDERAL, STATE, AND LOCAL GOVERNMENTS

TUESDAY, JULY 13, 2004

House of Representatives,
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census,
Committee on Government Reform,
Washington, DC.

The subcommittee met, pursuant to notice, at 3 p.m., in room 2154, Rayburn House Office Building, Hon. Adam Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam, Turner, and Clay.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Ursula Wojciechowski, professional staff member; Juliana French, clerk; Felipe Colon, fellow; Kaitlyn Jahrling, intern; Adam Bordes, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. Putnam. A quorum being present, this hearing on the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order. Our deepest apologies for us running an hour late because of votes, but that is the nature of this business.

Good afternoon and welcome to the subcommittee's hearing entitled "Facilitating an Enhanced Information Sharing Network that Links Law Enforcement and Homeland Security for Federal, State, and Local governments." This hearing will address the initiatives and strategies being implemented to enhance information sharing capabilities between Federal, State and local law enforcement agencies and homeland security activities. There are many examples of direct and indirect links between criminal activity and terrorist-related activity. Accordingly, law enforcement agencies at all levels of government should have effective collaborative capabilities for information sharing.

The need to coordinate the efforts of Federal, State, and local governments for homeland security is now well understood. September 11th highlighted the increasing risk of terrorist attacks on U.S. soil. Consequently, Federal, State and local governments recognized the need to effectively unify efforts to enhance homeland security by employing the unique contribution at each level a government can make on the basis of its capabilities and knowledge of its own environment. U.S. intelligence and law enforcement communities continuously assess both foreign and domestic terrorist threats to the United States. In October 2001, Congress passed the USA Patriot Act, to improve the sharing of information between the intelligence and law enforcement communities.

Information sharing and coordination among government organizations are essential to producing comprehensive and practical approaches to combating threats. Having information on threats and actual incidents experienced by others can help an organization identify trends, better understand the risk, and determine what preventive measures should be implemented. In addition, comprehensive, timely information on incidents can help Federal and nonFederal analysis centers determine the nature of an attack, provide warnings and advise on how to mitigate an imminent attack. Also, sharing information on known terrorists and criminals can help secure our Nation's borders.

There is clear, compelling, and documented evidence to support the notion that there are instances of a direct link between criminal activity such as drug trafficking, illegal gambling, and money laundering whose primary beneficiaries are terrorist organizations. Cutting off funding sources and interrupting the linkage that supports the threat activity will contribute to a more secure America.

Another critical issue in developing effective analysis and warning capabilities is to ensure that appropriate intelligence and other threat information, both cyber and physical, are received from the intelligence and law enforcement communities. For example, there has been great public debate regarding the quality and timeliness of intelligence data shared between and among relevant intelligence law enforcement and other agencies. Today we will not focus on the rear-view mirror or dwell on past breakdowns in the process of gathering or sharing information. Today's hearing seeks to address this matter in the unclassified space, with knowledge that there's an enormously valuable and important component of information sharing managed and conducted in the classified space. Regardless of source, it is important that relevant information be available to appropriate decisionmakers to enhance our prevention efforts in the law enforcement and homeland security communities on behalf of protecting our citizens from foreign and domestic threats. We need only to be reminded of the sniper tragedy in the Washington area during the fall of 2002 to reflect on the intrinsic value of such collaboration.

During this hearing, we will examine the efforts and progress achieved in developing secure, reliable, and interoperable information sharing networks that facilitate a comprehensive real-time information sharing capability that is dependable and respects privacy. The subcommittee will seek a better understanding of how improved collaboration and communication will enhance two-way flow of information between Federal, State and local law enforcement entities. With the threat environment that exists in the world today, it is increasingly important that cross-agency and intergovernmental collaboration is effective and efficient. Accordingly, the subcommittee will explore progress and obstacles to achieving the most successful implementation of a strategy for information sharing related to law enforcement and homeland security.

We have a very distinguished panel of witnesses today and I look forward to their testimony and the opportunity to explore these matters in greater detail. Today's hearing can be viewed live via Webcast by going to reform.house.gov and clicking on the link under live committee broadcast.

[The prepared statement of Hon. Adam H. Putnam follows:]

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY	(202) 225–5074
FACSIMILE	(202) 225–3974
MINORITY	(202) 225–5051
TTY	(202) 225–6852

www.house.gov/reform

Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Congressman Adam Putnam, Chairman

OVERSIGHT HEARING
STATEMENT BY ADAM PUTNAM, CHAIRMAN

Hearing topic: ***"Facilitating an Enhanced Information-Sharing Network That Links Law Enforcement and Homeland Security for Federal, State and Local Governments."***

Tuesday, July 13, 2004
2:00 p.m.
Room 2154, Rayburn House Office Building

OPENING STATEMENT

Good afternoon and welcome to the Subcommittee's hearing on " Facilitating an Enhanced Information-Sharing Network That Links Law Enforcement and Homeland Security for Federal, State and Local Governments." This hearing will address the initiatives and strategies being implemented to enhance information sharing capabilities between Federal, state and local law enforcement agencies and homeland security activities. There are many examples of direct and indirect linkage between criminal activity and terrorist-related activity. Accordingly, law enforcement agencies at all levels of government should have effective collaborative capabilities for information sharing.

The need to effectively coordinate the efforts of Federal, state and local governments for homeland security is now well understood. September 11th highlighted the increasing risk of terrorist attacks on U.S. soil. Consequently, Federal, state and local governments recognized an urgent need to effectively unify their efforts to enhance homeland security by employing the unique contribution that each level of government can make on the basis of its capabilities and knowledge of its own environment. U.S. intelligence and law enforcement communities continuously assess both foreign and domestic terrorist threats to the United States. In October 2001, Congress passed the USA PATRIOT Act, to improve the sharing of information between the intelligence and law enforcement communities.

Information sharing and coordination among government organizations are central to producing comprehensive and practical approaches and solutions to combating threats. Having information on threats and actual incidents experienced by others can help an organization identify trends, better understand the risk it faces, and determine what preventive measures should be implemented. In addition, comprehensive, timely information on incidents can help Federal and nonfederal analysis centers determine the nature of an attack, provide warnings, and advise on how to mitigate an imminent attack. Also, sharing information on known terrorists and criminals can help to secure our Nation's borders.

There is clear, compelling and documented evidence to support the notion that there are instances of a direct link between criminal activity such as drug trafficking, illegal gambling, and money laundering whose primary beneficiaries are terrorists organizations. Cutting off funding sources and interrupting the linkage that supports the threat activity will contribute to a more secure America.

Another critical issue in developing effective analysis and warning capabilities is to ensure that appropriate intelligence and other threat information, both cyber and physical, are received from the intelligence and law enforcement communities. For example, there has been considerable public debate regarding the quality and timeliness of intelligence data shared between and among relevant intelligence, law enforcement, and other agencies. Today, we will not focus on the rear view mirror or dwell unnecessarily on past breakdowns in the process of gathering and sharing information. Further, today's hearing will only address this matter in the unclassified space, acknowledging that there is an enormously valuable and important component of information sharing managed and conducted in the classified space. No matter the source, it is important that relevant information be available to appropriate decision makers to enhance our prevention efforts in the law enforcement and homeland security communities on behalf of protecting our citizens from foreign or domestic terrorism. We need only to be reminded of the "sniper" tragedy in the Washington area during the fall of 2002, to reflect on the intrinsic value of such collaboration.

During this hearing, we will examine the efforts and progress achieved in developing secure, reliable, and interoperable information-sharing networks that facilitate a comprehensive and real-time information-sharing capability that is dependable and that respects privacy provisions. The Subcommittee will seek a better understanding of how improved collaboration, cooperation, and communications will enhance improved two-way flow of information between appropriate Federal, state and local law enforcement entities.

Information barriers can be, depending on the case, cultural, organizational, human, or technological. Such barriers often prevent the formation of integrated information systems across all levels of government.

Federal, state, and city governments have undertaken initiatives to improve the sharing of information that could be used to fight terrorism and protect the homeland. Many of the initiatives are implemented by states and cities and are not necessarily coordinated with other sharing initiatives, including those implemented by the Federal government.

While beneficial to participants, the initiatives do not necessarily integrate others into a truly national system and may inadvertently hamper information sharing for this reason. A lack of effective integration could increase the risk that officials will overlook, or never even receive, information needed to prevent a terrorist attack.

New technologies for data integration and interoperability could enable agencies to share information without the need for radical structural changes. Developing and implementing appropriate technological solutions can improve the effectiveness and efficiency of information sharing. Additionally, tools, processes, and technologies available today address privacy issues and provide protection against privacy intrusion.

With the threat environment that exists in the world today, it is increasingly important that cross-agency and intergovernmental collaboration is effective and efficient. Accordingly, the Subcommittee will explore progress and obstacles to achieving the most successful implementation of a national strategy for information sharing related to law enforcement and homeland security.

All law enforcement agencies must act in partnership to maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks. Protocols for reciprocal exchanges of information have to be firmly established because the free flow of information among Federal, state and local law enforcement agencies is vital to fighting the war on terrorism and protecting citizens.

#######

Mr. PUTNAM. At this time, I would yield to the gentleman from Ohio for any opening statements he may have. You are recognized for 5 minutes.

Mr. TURNER. Thank you, Mr. Chairman. I want to congratulate you on your efforts to continue the review of the issues of technology and how it plays an important role in homeland security. So much of the work we have had in front of us has been an ascertainment of areas in which we need to bolster the ability for agencies to work together both in information sharing and just in basic communications, so I appreciate your focus on this issue.

Mr. PUTNAM. Thank you very much. And we will insert Mr. Clay's statement for the record at the appropriate time.

At this time, we will move directly into testimony. If the first panel would please rise for the administration of the oath and anyone accompanying who will be providing answers.

[Witnesses sworn.]

Mr. PUTNAM. All the witnesses have responded in the affirmative, and we will move to testimony. As you know, you have a light panel on your desk indicating the 5-minute time restraints, and the bulk of your statement will be inserted into the record.

Our first is Lieutenant General Patrick Hughes, U.S. Army, retired, the Assistant Secretary for Information Analysis with the Department of Homeland Security. General Hughes assumed his current duties on November 17, 2003. He was formerly president of PMH Enterprises, LLC, a private consulting firm specializing in intelligence, national security and international relations. He retired from the U.S. Army on October 1, 1999 after more than 37 years of military service beginning as an enlisted soldier and combat medic in January 1962. His last Active-Duty assignment was Director of the Defense Intelligence Agency, a position which he held for 3½ years. Other positions included Director of Intelligence, J2, Joint Staff and DIA, Director of Intelligence J2 U.S. Central Command, and Commanding General of the U.S. Army Intelligence Agency. We appreciate the work that you have done for this Nation and you are recognized for your opening statement.

STATEMENTS OF LIEUTENANT GENERAL PATRICK HUGHES, ASSISTANT SECRETARY FOR INFORMATION ANALYSIS, U.S. DEPARTMENT OF HOMELAND SECURITY; RUSSELL TRAVERS, DEPUTY DIRECTOR AND ASSOCIATE DIRECTOR FOR DEFENSE ISSUES, TERRORIST THREAT INTEGRATION CENTER; AND WILLIE HULON, DEPUTY ASSISTANT DIRECTOR, COUNTERTERRORISM DIVISION, FEDERAL BUREAU OF INVESTIGATION

General HUGHES. Thank you very much, Mr. Chairman and Congressman Turner and other distinguished staff of the subcommittee.

I am privileged to appear before you today to discuss the current status of the progress being made by the Department of Homeland Security to coordinate efforts to achieve common goals. In this case, we are focused on information sharing and collaboration. Information sharing is becoming more common throughout the Federal, State, territorial, tribal, major city, local and private sector environment in which DHS interacts. However, we have not yet completed the mechanisms to engage in information sharing nor have we fully developed the systemic methodology necessary to fully achieve our collaborative goals. We are working toward that end as rapidly as we can.

Our goal is to effectively, efficiently, and synergistically pass and receive information in all of its forms for the benefit of the U.S. Government, our nonFederal constituents and DHS entities. In order to achieve this goal, we must build an architecture with technical and procedural transparency and interoperability wherever possible.

However, the most significant impediments to information sharing are not technological. They are legal and cultural and evolve both policy and procedure. In response to these and other challenges, DHS has established an Information Sharing and Collaboration Center which will achieve improvements in these areas. The primary means of interdepartmental, interagency, and intersector communication, intersector communication being two way, that DHS will use is the Homeland Security Information Network, otherwise known as HSIN. The service system and capabilities that form the larger network are on the way to being fielded throughout the State and territorial constituency with plans to expand that fielded element to all other partners and associates as soon as possible.

Given our imperative to provide support and assistance to State and local officials, it is no longer sufficient to have vertical and horizontal linkage just with some of the participants. The Nation must achieve a fully collaborative environment through which homeland security officials, law enforcement, first responders, and decisionmakers can fully interact, across traditional boundaries, seamlessly and effectively to deal with issues of terrorism and response to terrorism and other emergency conditions.

I would like to inform you at the present time, including our participation in the newly constructed Homeland Security Interactive Operations Center, we in DHS at the Office of Information Analysis, which I am privileged to head, have the following connectivity: standard telephone; secure telephones; facsimile of all kinds; wideband encrypted NSTS, or gray phone; courier service; standard Internet connectivity; open-source information system and NIPRNet connectivity; SIPRNet connectivity; joint worldwide intelligence communication system linkage; secure VTC capability; and many software and hardware tools which collectively affords us access to virtually every communication and information sharing level and capability that we need to fully engage in the intelligence function.

We have liaison officers with online access to the CIA, to the Terrorism Threat Integration Center, TTIC, to the National Security Agency, to the National Geospatial Agency, DOD, and especially to the Federal Bureau of Investigation. All of those liaison officers have access to their automated systems of their organizations. We are fully integrated into the national government meeting mechanism. We are making steady progress to connect to the Homeland Security Information Network.

We can do the job now and do it well. We seek to continue to make progress to more fully realize the goals we have set for broad and unfettered access to as much information as possible in the shared context to secure our homeland.

Mr. Chairman and members of the subcommittee, this concludes my prepared statement. Thank you very much.

Mr. PUTNAM. Thank you very much, General Hughes.

[The prepared statement of General Hughes follows:]

Statement of
Patrick M. Hughes
Lieutenant General, USA, Ret
Assistant Secretary for Information Analysis

Information Analysis and Infrastructure Protection Directorate

U.S. Department of Homeland Security

Before the House Committee on Government Reform's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

July 13, 2004

Good morning Mr. Chairman and distinguished members of the Subcommittee. I am privileged to appear before you today to discuss the current status of the progress being made by the Department of Homeland Security (DHS) to coordinate efforts to more effectively achieve common goals in national security and domestic law enforcement

Information Sharing is ubiquitous throughout the Federal, State, tribal, territorial, local and private sector environment in which DHS seeks to interact. The goal is to effectively, efficiently, and synergistically pass and receive information in all of its forms for the benefit of the United States Government (USG), our State, tribal, territorial, local, and private sector partners, and other DHS entities. In order to achieve this goal we must design a "system of systems" with systemic transparency and interoperability in mind wherever possible. However, the most significant impediments to information sharing are not technological, they are legal, cultural, psychological, and sociological. Hence, the need exists to start with the "business case" and work toward a common, integrated, and rational vision for the Department.

In response to these challenges, DHS has established an Information Sharing and Collaboration Program which will achieve improvements in Information Sharing and Collaboration. The program has four specific imperatives:

- Improve information sharing and collaboration within each of the Directorates of the Department,
- Improve information sharing and collaboration between DHS elements,
- Improve information sharing and collaboration across the cabinet level departments and agencies, and
- Improve information sharing and collaboration with our State, tribal, territorial, local, and private sector partners responsible for securing the people and infrastructure of this country.

These improvements will aid in developing a unified vision and defining where we are, where we want to go, and the roadmap to get there. To achieve success, we must simultaneously conceive, design, resource, build, and field a DHS Information Sharing Enterprise System (ES) that will ensure the achievement of our goal and that will be expandable to meet future technical and operational requirements.

This program will assess current systems in use within DHS to determine how we can best leverage existing technologies to meet mission requirements, review existing efforts to build more compatible and collaborative connectivity with all of our partners and stakeholders, and assure that we achieve the maximum feasible synergism with other cabinet departments and agencies in the effort to assure that information is shared openly, effectively, and rapidly with all concerned. It will be critical in this effort to gain the willing participation of all players, but it is particularly noteworthy that DHS is charged by law and executive order to lead this effort for the Federal Government.

Additionally, this program involves working with the Department of Justice (DOJ), Federal Bureau of Investigation (FBI), and Department of Defense (DOD) to assure that current systems achieve higher levels of compatibility and that future systems are fully compatible and interoperable. For instance, as part of this effort, the DOJ and DHS information sharing staffs are working hard to bring HSIN (which is based on groove technology), LEO, and RISS together with the goal of making the systems more compatible as quickly as possible, making the systems fully compatible in the short term, and developing a common system for the future.

Given the imperative to provide guidance and assistance to State, tribal, territorial, and local officials, it is no longer sufficient to have vertical and horizontal linkage with law enforcement. The nation must achieve a fully collaborative environment through which law enforcement, first responders, and decision makers can fully interact, across traditional boundaries, seamlessly and effectively to deal with issues of terrorism and response. This is the major advantage of Homeland Security Interactive Network (HSIN) over the technologies formerly used by the USG. While one technology allowed information sharing vertically and sometimes horizontally within a certain discipline, the systems did not provide for robust collaboration between and among various entities which must interact to achieve success in fighting terrorism and crime, and respond to major incidents and disasters.

If we have learned nothing else from the events of the past, we have learned that law enforcement does not just catch criminals. Law enforcement, in many communities, carries the significant responsibility of a first response force, as collectors of vital information, and as the manpower to manage crisis events which are visited upon cites and towns across the nation. As such, we must stop sharing information in a hierarchical fashion and begin sharing in a fully collaborative manner where the police in any community can communicate directly with whom they need to communicate, at any time, and receive an effective response. This effort will require automated addressing of copies of information exchanged to go to those who have traditional roles in the hierarchy, but not require that the hierarchical structure see all information "before" it can move forward to the intended receiver. In so doing, we will achieve a significant increase in the speed and effectiveness of information sharing across the entire enterprise.

At the same time, we must increase the ability of law enforcement and emergency management to communicate with private sector security personnel to assure that information related to the protection of critical infrastructure is fully coordinated and rapidly provided to those who have the responsibility to respond. The HSIN does just that. While each community of interest operates each day within HSIN with sequestration or sensitive information available to only those invited into the community of interest, because HSIN operates on a common technology base, it allows those with a need to do so to establish a cross-connected and fully collaborative space. This permits all to see the information necessary to achieve the desired outcome during periods when a natural or man made threat appears with potential to adversely affect the community.

Within DHS, information sharing has greatly improved over the first year of operation. As the various separate elements have merged and found more common operating methodologies, so their personal and technological cohesiveness has improved. But we are not home yet. We must continue aggressive efforts to improve information sharing and collaboration across the Department. This is one of the four imperatives of our Information Sharing and Collaboration Program described previously. It is clear that we have much work ahead in this enterprise. And we are moving ahead. This fiscal year we have achieved an interim Homeland Security Operations Center which provides a significantly enhanced capability to fuse information from intelligence and operations into a coherent common operating picture, a clear set of information to provide to customers, and a focal point for collaboration between all Federal law enforcement, intelligence, and emergency response organizations.

In addition, our liaison and outreach activities are providing a greater level of cooperation and collaboration with and between the many partners who play a vital role in securing the homeland. The current development of a secret level infrastructure, formerly known as HSDN, will become HSIN-Secret as it stands up and the HSIN suite of communities of interest are able to share classified information on a routine basis...using the same software tools available on HSIN at the SBU level. This is another significant achievement for the DHS in leading information sharing and collaboration efforts into the future.

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

Mr. PUTNAM. Our next witness is Mr. Russell Travers. Mr. Travers is serving as TTIC Deputy Director and the Associate Director for Defense Issues. Mr. Travers manages the government-wide information sharing initiative, TTIC's red team, and knowledge-development efforts in the maintenance of the USG's terrorists' identities' data base. He is responsible for TTIC's interaction with DOD's analytic efforts focused on terrorism. Formerly he was the Deputy Director for Policy Support at the Defense Intelligence Agency and responsible for intelligence support to the Office of Secretary of Defense, managing activities of the Defense intelligence officers and overseas liaison officers, administering special access programs and organizing agency support to homeland defense. He received his B.A. in government from the College of William & Mary and his J.D. from George Washington. Welcome to the subcommittee.

Mr. TRAVERS. Mr. Chairman, members of the subcommittee, I am pleased to be here today to discuss TTIC's role in information sharing. I will summarize three areas from my written statement: first, TTIC's access to information; second, TTIC information sharing initiatives; and third, an important qualifier about what information sharing can and can't do.

First, our access. TTIC is an integration center, and by DCI directive we are to have unfettered access to terrorist threat-related information. For the last 14 months we have been working with the community to achieve that all-encompassing access. With our recent move to a new facility, TTIC analysts can now access up to 21 networks from across the relevant communities. That number will soon grow to at least 26. To give you some perspective on what that means, I am a Defense Department assignee to TTIC. At my desk, I can access the CIA operational traffic related to terrorism. At my desk, I can access FBI case files related to international terrorism. We have come a very long way. To be sure, we are still working some access issues, and our CIO is intently focusing on how we handle assimilation of data and the ability to efficiently search across the holdings from so many diverse networks. But the progress over the past 14 months has been exceptional.

The second issue I want to address relates to a number of TTIC initiatives associated with information sharing. Importantly, by DCI directive our mandate is to work information sharing at the Federal level, and so I will focus on horizontal information sharing. However, we are posturing ourselves to support the FBI and DHS with their critical vertical information sharing responsibilities and I will be happy to address some of those initiatives during Q and A.

With regard to horizontal information sharing, TTIC has established a program office to implement the March 2003 information sharing memorandum of understanding. This office is working with our community partners in the full range of impediments associated with information sharing: originated control information, third agency rule, no double standard, terror lines and so forth. The community can detail progress across the board, I believe. For instance, pure terrorism reporting has grown by a factor of 6 since before September 11.

In terms of the technical advances to share terrorism information, TTIC's CIO has been leading community efforts. In August of last year, we launched the TTIC online Web site which is populated with terrorism-related information. This highly secured capability can reach virtually the entire structure of the Federal Government, hosting over 2,800 users. TTIC Online reaches all traditional Intelligence Community terrorism analytic elements, but also FBI headquarters, all JTTFs, Department of Homeland Security, the military commands and numerous other organizations that have a need for terrorism threat information: the Departments of Interior and Agriculture, for example.

The success of TTIC Online can be seen by a comparison with the analogous capabilities that existed in September of 01. The user base is six times greater. Five times as many organizations participate. The average number of document hits per week has grown by 500 times. And the total repository of documents has grown from 1 to 3.5 million. Just over a month ago, TTIC deployed a SIPRNet version of TTIC Online. This has the potential to dramatically increase situational awareness for those tens of thousands of individuals involved in the war against terrorism but don't have access to the Top Secret Network.

Moreover, to help support vertical information sharing, TTIC will be deploying a sensitive but unclassified presence of TTIC Online on the open-source information system network.

I hope it is apparent that TTIC is taking a very aggressive approach to improving information sharing across the government. And while we are second to none in espousing the importance of information sharing, I do want to close with a few cautionary words:

First, information sharing has become a bit of a bumper sticker; everybody supports it, but few appreciate the complexities of implementing it. There are almost invariably a complicated mix of technical security, policy, and legal issues associated with sharing information. Source sensitivity is real. Operational considerations do exist. Privacy matters do pertain. And the technical capabilities of government networks vary widely. There are always going to be impediments and reasonable people can and do disagree.

Second, I am increasingly concerned with something that could be called effective information sharing. As we see the explosion of networks and Web sites, organizations can post their data and legitimately say they have shared their information. Whether anyone on the other end knows it is there and reads it is an entirely different matter.

Third, information sharing is not and will never be a panacea. If we don't have a basic terrorism analytic business process right and have an established critical mass of analytic talent, we can pass information all over the government and still not connect the proper dots. Indeed we could face the prospect of being wrong faster. Terrorism is an extraordinarily difficult analytic problem and the key is having long-term expertise available to sort through the reams of information, much of which is inaccurate, contradictory, or utterly irrelevant. This in no way demeans the importance of information sharing, merely to point out that information sharing is necessary but not sufficient.

Thank you for your time. TTIC looks forward to continuing to work with the subcommittee and I will be happy to answer any questions.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Travers follows:]

13 July 2004

Statement for the Record of
Russell E. Travers

Deputy Director for Information Sharing and Knowledge Development
Terrorist Threat Integration Center (TTIC)

On
Facilitating an Enhanced Information Sharing Network that Links Law Enforcement and Homeland Security for Federal, State and Local Governments

Before
House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Washington D.C.

Good afternoon, Chairman Putnam and Members of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census.

I appreciate the opportunity to join my colleagues from the Department of Homeland Security and the Federal Bureau of Investigation to address the initiatives and strategies being implemented to enhance information sharing capabilities between and among Federal, State and local law enforcement agencies and Homeland Security activities. The role of the Terrorist Threat Integration Center in facilitating such sharing is directly related to our mission as laid out initially in the President's 2003 State of the Union Address and as clarified over the past 18 months. Accordingly, I will briefly lay out that mission, as well as TTIC's view of the way ahead. I'll then turn to Information Sharing, focusing on three major aspects: TTIC's access to information, TTIC's role in horizontal information sharing across the federal structures, and TTIC's support to vertical information sharing down to State and Local entities. Finally, I'll close with a few general observations about information sharing and what we should - and shouldn't - expect from it.

TTIC and the Way Ahead

As the Subcommittee knows, TTIC stood up in May of last year, four months after the President's speech. Chartered as a multi-agency joint venture, TTIC is tasked with integrating and analyzing terrorist threat-related information collected domestically and abroad, and then disseminating this information and analysis to appropriate recipients, consistent with applicable privacy and civil liberty requirements. We began operations with approximately fifty U.S. Government staff and have almost tripled in size since then. We have recently relocated from CIA Headquarters to a new facility where we will be joined by large elements of the Director of Central Intelligence's Counterterrorist Center and the FBI's Counterterrorism Division later this summer and fall. Along with very broad access to information, a great strength of TTIC is the fact that we have had analysts from 16 separate organizations carrying out the work of their parent organization, building bridges between departments and agencies, and enabling us to carry out our mission. These assignees come from a wide array of the key organizations involved in the war against global terrorism, including FBI, CIA, NSA, National Geospatial-Intelligence Agency, Defense Intelligence Agency, the Department of State, Department of Energy and DHS. We also have had a Capitol Police Officer and a representative of the Nuclear Regulatory Commission. This broad representation will continue to grow as TTIC expands. These individuals bring with them unique expertise and connectivity to their home organizations.

Despite the predictable challenges with the standup of such a complex organization, TTIC has enjoyed significant success in its primary analytic and reporting function; in the past 14 months we have produced over 300 Presidential Terrorist Threat Reports for our senior leadership, 400 Terrorist Threat Matrices, 500 Terrorist Situational Summaries as well as scores of unique products dealing with terrorist threat warning and other issues.

In the past, numerous organizations were trying to "do it all" regarding terrorism analysis, and with that came relatively shallow analysis and an inability to delve deeply into issues. TTIC's creation and stand-up has helped alleviate that problem by concentrating the responsibility for terrorism analysis within the USG. As described in the recent response to a letter from Senators Collins and Levin:

> "TTIC has the primary responsibility in the USG for terrorism analysis (except information relating solely to purely domestic terrorism) and is responsible for the day-to-day terrorism analysis provided to the President and other senior policy makers."

We are now working with the Community to gain the resourcing necessary to successfully carry out that mission. The CIA has already promised to detail 60 additional officers to TTIC as soon as possible. At the same time, Memoranda of Agreement are being staffed with the relevant Departments and Agencies in order that we might be assigned the necessary quantity and quality of experienced terrorism analysts. While additional work is required to fully determine the scope and migration of resources necessary to meet this expansive mission, we have, in partnership with other elements of the USG, made notable progress.

TTIC and Information Sharing

There is no question that information sharing is at the heart of TTIC's mission. As mandated in DCID 2/4, TTIC is to "create a structure to institutionalize sharing across appropriate federal agency lines of terrorist threat-related information, collected domestically or abroad in order to form the most comprehensive possible threat picture and minimize any seams between analysis of terrorist threat related information and minimize any seams between analysis of terrorist threat related information collected domestically or abroad." While this will always be a work in progress and much is yet to be accomplished, TTIC and the entire USG have made substantial progress since 9/11 overcoming numerous impediments to information sharing.

To begin with, a solid legal and policy groundwork for information sharing has been put in place since 2001: the USA PATRIOT Act; the Homeland Security Act; the Presidential decision to create the Terrorist Threat Integration Center; the Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security

Concerning Information Sharing; the Director of Central Intelligence Directive establishing TTIC; Homeland Security Presidential Directive 6 creating the Terrorist Screening Center; and the first of a new series of DCI Directives pertaining to Information Sharing, DCID 8/1 Intelligence Community Policy on Intelligence Information Sharing, have all played a role in driving the improvements in sharing terrorism-related information.

With the underlying legal and policy framework in place, the Community has been focusing on the new business practices, cultural changes, and technical systems needed to fully implement these policies. Both in terms of the absolute amounts of available reporting and the extent to which it is widely shared in the Community, the government has made substantial strides. For example, if we compare intelligence reporting on terrorism-related subjects now, with reporting in 2001, we see tremendous growth. Immediately after the terrorist attacks on September 11, 2001, purely terrorism-related intelligence reporting surged, from an average of roughly 300 per day in early 2001, to an average of approximately 850 reports per day in late 2001. Since that time, the amount of intelligence reporting on terrorism related issues has continued to increase to about 1,700 per day in 2004. More importantly, because of the technical, cultural and business practice changes that are starting to take place, that information is being widely disseminated to those intelligence, law enforcement, and homeland security analysts who need to see it.

TTIC takes its responsibilities in the information-sharing arena very seriously. Beyond the core business function of integrated analysis and the associated department focused on Analysis and Production for the entire Community, TTIC has three organizations that are directly involved in information sharing:

- TTIC's CIO has worked closely with the Community CIOs and all relevant partners to ensure that the proper architecture and standards are in place to support the mission of terrorism analysis. Our CIO's extraordinary work has been amongst the most visible of TTIC's successes, receiving wide acclaim across the community. In particular, TTIC Online, which will be discussed below, has become the principal source of all source terrorism analysis for the entire community.

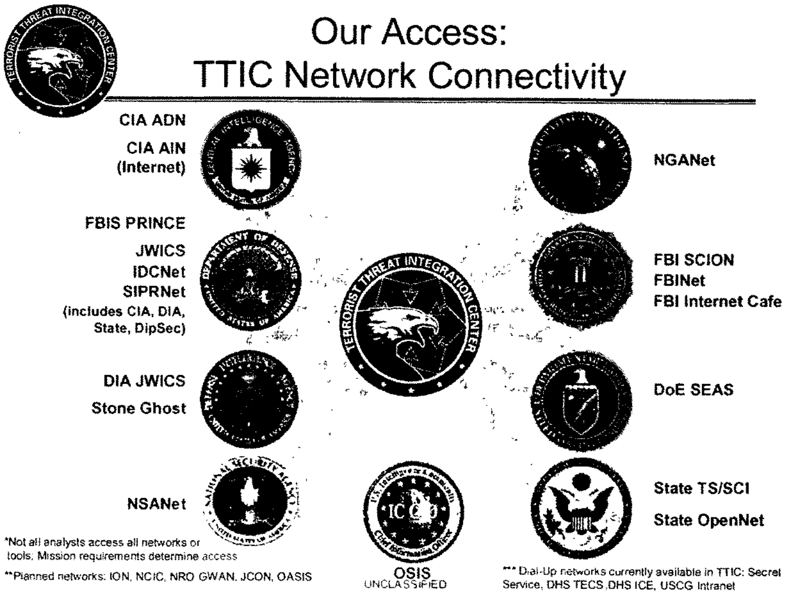
- TTIC stood up an Information Sharing Program Office in mid-2003 to oversee implementation of the Information Sharing MOU. Our focus has been on the key impediments to a free flow of terrorism-related information, including such issues as "Originator Controlled Information", "the Third Agency Rule", "No Double Standard" rule and so forth. Such control mechanisms have their place, if properly used, but by definition also impede information sharing. TTIC is working with the Community to reduce these impediments to the absolute minimum: one metric of success - the use of ORCON has declined across the Community by about 40% since 9/11.

- And recently, TTIC and DIA have established a Force Protection Cell, staffed by DoD assignees to TTIC. These individuals will have complete access to all information available to TTIC and will focus on that reporting that might be relevant to DoD's force protection requirements around the globe. Once identifying such reporting, they will work the modalities to ensure rapid dissemination to the Defense Department. TTIC believes this could be a useful model for other Departments and Agencies to follow.

TTIC and Access to Information

As the U.S. Government's Terrorist Threat Integration Center, it is imperative that TTIC have access to all relevant information. This notion was captured in our chartering document, Director of Central Intelligence Directive 2/4, which called for TTIC analysts to have "unfettered access" to terrorism threat-related information. Operating under that guidance, TTIC has been working with information providers from across the government to gain access to all appropriate information.

As depicted below, TTIC assignees with the appropriate need to know currently have access to up to 21 networks from across the Intelligence, Law Enforcement and Homeland Security communities. With our recent move to the new building this figure will soon grow to 26 separate networks.



Our Access: TTIC Network Connectivity

CIA ADN
CIA AIN (Internet)

FBIS PRINCE
JWICS
IDCNet
SIPRNet
(includes CIA, DIA, State, DipSec)

DIA JWICS
Stone Ghost

NSANet

NGANet

FBI SCION
FBINet
FBI Internet Cafe

DoE SEAS

State TS/SCI
State OpenNet

OSIS
UNCLASSIFIED

*Not all analysts access all networks or tools; Mission requirements determine access

**Planned networks: ION, NCIC, NRO GWAN, JCON, OASIS

*** Dial-Up networks currently available in TTIC: Secret Service, DHS TECS ,DHS ICE, USCG Intranet

Over the past year TTIC has worked with the various partner organizations to broaden individual analyst access to these 21 networks. At standup, for example, access to CIA operational traffic was limited largely to CIA analysts and access to FBI's network was limited to FBI analysts. This has changed dramatically, and now, appropriate analysts from across the Community, once they have received necessary training, are able to access other organizations' networks.

The upshot of such broad access is that an analyst may well have six or more CPUs under his or her desk - thereby raising an entirely separate set of problems: simply put, an analyst will have to switch from network to network in order to pursue a line of inquiry against various agency data bases and intelligence holdings. This is an extremely inefficient and time-consuming process, and runs the risk of incomplete analysis. Nevertheless, historically, this has been necessitated by the differing architectures and security protocols associated with the relevant Departments and Agencies.

TTIC's CIO recognized this problem very early on and has been working on an architectural solution that will allow a federated search - one query against the holdings on multiple systems. Expected to reach initial operating capability in the next month, our approach, called Sanctum, will allow analysts to search against the holdings of five systems; this will gradually expand over time and will help analysts deal with the information overload problem.

Mr. Chairman, it would be premature to declare victory regarding TTIC's access to information. We are still dealing with a host of challenges, ranging from a disparity in technical capabilities of networks across the government, to various Special Access Programs and other highly restricted categories of material, to basic questions about whether TTIC should have certain types of information, to protocols and procedures that govern the flow of information. And while we continue to work these issues, I am confident in saying that nowhere else in the government brings together such a diverse set of intelligence, law enforcement and homeland security information associated with the terrorism problem.

TTIC Initiatives in Information Sharing

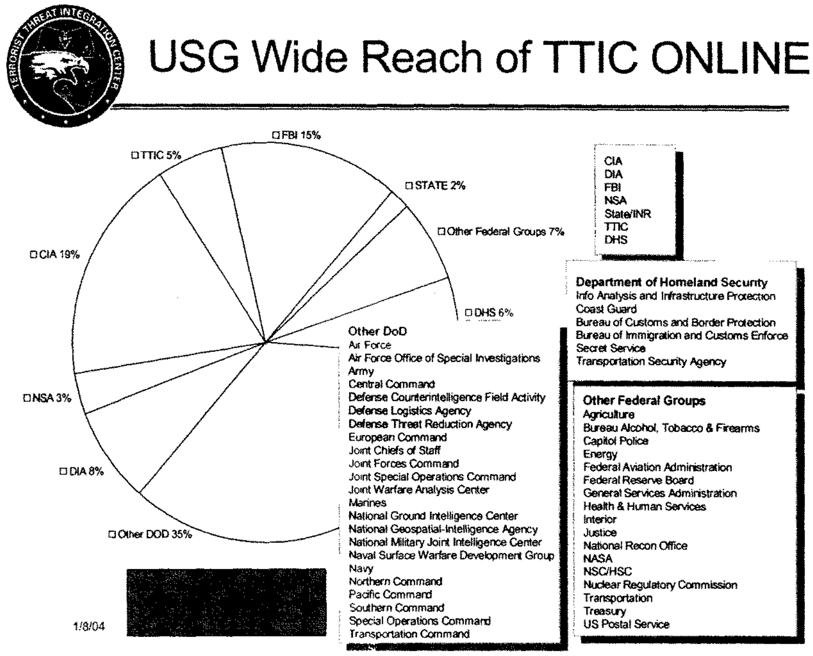
Information sharing has both horizontal and vertical components. TTIC's primary focus is on the horizontal aspects - ensuring that the Federal structures have the required information to fulfill their missions. Vertical information sharing is worked more directly by the FBI and DHS.

To begin to bridge the cultural gaps between the Intelligence, Law Enforcement and Homeland Security communities in the Federal Government, TTIC organized and sponsored its first Terrorism Information Sharing conference for the Federal Government in late March 2004. This classified conference was designed to attract professional mid-level decision makers from across the Federal Government who work in the fight against terrorism. The conference was a success, drawing over 260 participants from 40 different Federal organizations. We still have a long way to go to bridge the cultural gaps between different communities of counterterrorism professionals, but this conference was a good first step. It dispelled many misunderstandings, raised the general level of knowledge and mutual understanding among participants, and pointed out the areas where we still have work to do.

TTIC Online in Support of Horizontal Information Sharing

One key initiative that reflects our progress can be seen in the ability to electronically access terrorist-related information. Over the past 14 months TTIC has focused on the technical initiatives necessary to promote information sharing. Because of our mission, we are in the unique position of having to improve our ability to manage information, while creating an environment in which analysts can benefit from a diverse array of Intelligence Community and law enforcement sources. These demands require an architectural approach that makes best use of extant technology and legacy systems while ensuring smooth insertion of emerging technology in the future.

To promote horizontal information sharing across the entire Community of analysts working the terrorism problem, we launched the TTIC Online (TTOL) website in August 2003 leveraging and building upon CT Link, a secure community of interest created by CIA's Counterterrorist Center. The TTOL website now serves as the front door for the Intelligence, Law Enforcement, Homeland Security and Military communities to access a broad range of counterterrorism threat information. This highly secure capability can reach virtually the entire structure of the Federal Government, hosting over 2800 users in the JWICS Top Secret community. TTOL reaches not only the traditional national Intelligence Community terrorism analytic elements, but also the JTTFs, the military Commands, and numerous entities outside the Intelligence Community that have a need for terrorism- related information. The current breakout of the population of TTOL users and the full range of organizations that access the network can be seen below.



USG Wide Reach of TTIC ONLINE

CIA
DIA
FBI
NSA
State/INR
TTIC
DHS

Department of Homeland Security
Info Analysis and Infrastructure Protection
Coast Guard
Bureau of Customs and Border Protection
Bureau of Immigration and Customs Enforce
Secret Service
Transportation Security Agency

Other DoD
Air Force
Air Force Office of Special Investigations
Army
Central Command
Defense Counterintelligence Field Activity
Defense Logistics Agency
Defense Threat Reduction Agency
European Command
Joint Chiefs of Staff
Joint Forces Command
Joint Special Operations Command
Joint Warfare Analysis Center
Marines
National Ground Intelligence Center
National Geospatial-Intelligence Agency
National Military Joint Intelligence Center
Naval Surface Warfare Development Group
Navy
Northern Command
Pacific Command
Southern Command
Special Operations Command
Transportation Command

Other Federal Groups
Agriculture
Bureau Alcohol, Tobacco & Firearms
Capitol Police
Energy
Federal Aviation Administration
Federal Reserve Board
General Services Administration
Health & Human Services
Interior
Justice
National Recon Office
NASA
NSC/HSC
Nuclear Regulatory Commission
Transportation
Treasury
US Postal Service

1/8/04 [redacted]

TTIC Online contains approximately 3.5 million documents, including finished intelligence from CIA, TTIC, DHS, and FBI; disseminated reports from the Intelligence Community; access to a repository of tearlines from CIA, NSA, and DoD; warnings, alerts, and bulletins issued by FBI, DHS, and others; and links to other terrorist-threat resources on INTELINK. TTIC Online also hosts the USG database on known and suspected terrorists for which TTIC has responsibility; known as TIPOFF Web this provides, for the first time, a single, widely accessible database on known and suspected international terrorists.

The following chart further illustrates the extent to which our changing business practices, further enabled by technology, have substantially improved overall information sharing across the Community.

From CT Link to TTIC Online: 9/2001-6/2004	
September 2001	**June 2004**
471 Active users	2838 Active users
10 Users per month add rate	100 Users per month add rate
29 Active organizations	120 Active organizations
20 Sessions per week	1000+ Sessions per week
200 Document hits per week	88,000+ Document hits per week
4 Product types	92 Product types
14 FBI/LE reports per month	450 FBI/LE reports per month
1 Million document repository	3.5 Million document repository

In May of this year we launched a new version of TTIC Online at the SECRET-level that is available to a much wider group of users across the Federal Government. This new presence on SIPRNet makes SECRET-level counterterrorism information available to a wide array of DoD, DHS, Law Enforcement and Department of State users; this new audience is many times the size of the original user base, and as such, the SIPRNet version of TTIC Online will be of tremendous value to us in moving information outside of the Intelligence Community.

Vertical Information Sharing

As noted above, by DCID, TTIC is primarily focused on promoting horizontal information sharing with Federal organizations. Recognizing the importance of vertical information sharing, we are doing everything possible to support the FBI and DHS in their efforts to push information to state, local, and private sector entities. Two initiatives, in particular, bear mentioning:

- Along with the TOP SECRET and SECRET versions of TTIC Online, TTIC also plans to deploy a Sensitive But Unclassified (SBU) presence of TTIC Online on the Open Source Information System (OSIS) network. TTIC continues to solicit new users from across the Federal Government, and to add new sources of counterterrorism information. This should be instrumental in assisting FBI and DHS with their vertical information sharing efforts.

- TTIC has been working closely with the Community to increase the use of "Tear Lines", a means by which sanitized material can be shared much more widely with audiences that don't have high-level clearances. By leading the effort to establish common formats and content standards, we anticipate being able to automate tear line procedures and expedite the passage of material.

TTIC also is interested in vertical information sharing from the standpoint of receiving information that could originate at the local level. With the assistance of DHS and FBI there have been successes and advances in this area, however there is a great deal of work to be done. We look forward to working as appropriate with DHS and FBI to further the creation of an over-arching architecture that addresses the full range of issues associated with vertical information flow.

Information Sharing In Context: Some Final Observations

TTIC is second to none when it comes to espousing the importance of information sharing. And, as noted above, while much work is yet to be done, there is absolutely no question that the USG has made huge strides in this area since 9/11. However, having been immersed in the issue since the standup of TTIC, a few cautionary words are in order:

--*Be wary of the bumper sticker*: There seems to be complete agreement across the government on the need for better "information sharing". Conferences are held, editorials are written and pundits wax eloquently, but in reality, once we get below the low hanging fruit, there are very difficult issues involved. The Intelligence, Law Enforcement and Homeland Security communities are invariably faced with a complicated mix of technical, security, policy and legal challenges associated with improved sharing of information. There are very few easy fixes.

--*Information must be protected as well as shared*:

Attaining the proper balance is the key. There seems to be an underlying current suggesting that all "terrorism-related" information should go to all people that are somehow involved in the USG counterterrorism effort. Such an approach would likely put at risk sources of information and operations critical to winning the war on terrorism. There will always be source sensitivity issues, operational considerations, counter-intelligence aspects and a host of other security related problems, as well as important privacy issues that will reasonably limit free flow of information.

--*Information Sharing is not a panacea*: In short, information sharing is necessary but not sufficient. If we don't have the basic business process for terrorism analysis right, and haven't established critical mass of analytic talent, we can pass information all over the government and still not connect the proper dots; indeed we could even face the prospect of simply being wrong faster. Terrorism is an extraordinarily difficult analytic problem and the key is having long-term expertise and state-of-the art technical analytic tools able to sort through reams of information, much of which is inaccurate, contradictory or utterly irrelevant.

--*"Effective information sharing"* is critical: We are seeing an explosion of networks and websites, containing terabytes upon terabytes of information. Data tagging may be a small part of the solution (though it has far more applicability to the data end of the spectrum rather than the knowledge end). As Agencies "post" their information, they can legitimately say they have shared the information. Whether anyone on the other end knows how to find it and read it is an entirely different matter.

Conclusion

In conclusion, Mr. Chairman, any objective observer of the situation across the USG would conclude that substantial progress has been made over the past three years. Whether it takes the form of multiple daily secret daily videoconferences among the entire Federal counterterrorism community, the creation of organizations specifically devoted to addressing information sharing impediments, the technological advances allowing increased access to the USG's most sensitive information, or the improvements in policies and procedures to facilitate the flow of information, far more terrorism information is being shared than ever before. Nevertheless, we have much work to do and have many basic questions to resolve: for example, what is "need to know" in an era of globalization? We believe TTIC provides a forcing function to address many of these complex questions and look forward to working with this subcommittee as we confront these difficult issues.

Thank you and I look forward to any questions you may have.

Mr. PUTNAM. Our third witness is Mr. Willy Hulon. Mr. Hulon is the Deputy Assistant Director of the Counterterrorism Division at the Federal Bureau of Investigation. He began his career as an FBI Special Agent in September 1983. In July 2001, Mr. Hulon was designated Chief Inspector for the FBI. In October 2002, Director Mueller appointed Mr. Hulon as Special Agent in Charge of the FBI's Detroit Division. In his capacity, he worked closely with the Detroit JTTF and oversaw a wide range of investigations.

Delighted to have him here today to discuss all of the FBI's information sharing initiatives and welcome you to the subcommittee, and you are recognized for 5 minutes.

Mr. HULON. Good afternoon, Chairman Putnam, Ranking Member Clay, and members of the subcommittee. Thank you for inviting me to speak to you on the information sharing issues that face the Federal Bureau of Investigation and members of the intelligence and law enforcement communities.

The terrorist threat of today poses complex challenges. Today's terrorists operate seamlessly across borders and continents. Aided by sophisticated communications technologies, they finance their operations with elaborate funding schemes and patiently and methodically plan and prepare their attacks. To meet and defeat this threat, the FBI must have several critical capabilities. First, we must be intelligence driven. To defeat the terrorists, we must develop intelligence about their plans and use that intelligence to disrupt those plans. We must be global. We must continue our efforts to develop our overseas law enforcement options, our partnerships with foreign law enforcement and intelligence services, and our knowledge and expertise about foreign cultures and terrorists adversaries overseas. We must have networked information technology systems. We need the capacity to manage and share our information effectively. Finally, we must remain accountable under the Constitution and the rule of law. We must respect human rights and civil liberties as we protect the American people.

The FBI has an information and intelligence sharing strategy. The strategy recognizes that we have a responsibility to the Nation to disseminate information broadly, that we will share information by rule and withhold by exception, and the sharing is cross-community in nature. The FBI will protect sources and methods by separating what needs to be shared from how the information was obtained. Our strategy is implemented through both collaborative initiatives and information system connectivity initiatives both on a national scale and in local projects. Collaborative initiatives bring together personnel and processes in a common setting to facilitate information sharing through each agency's information systems. Information system connectivity initiatives share data electronically by combining the respective agency's data technologically in some form.

As local and regional collaborative intelligence centers are being established across the country, the FBI has been asked to take an active role in building the intelligence processes in these initiatives. Through our field intelligence groups in each field office, we are contributing personnel, intelligence process development, information access and funding. To further strengthen our collaborative efforts with both local and national benefits, we have established an intelligence reporting capability in each of our joint terrorism task forces through the assignment of field intelligence group personnel. We can ensure that terrorist threat information collected by the JTTFs is quickly disseminated to all who need it to protect the country.

On a national scale, the Law Enforcement National Data Exchange, or NDEX, is being developed by the FBI as the principal nationwide system for sharing criminal incident report data to link law enforcement interests and enhance law enforcement strategic planning. NDEX prototypes are being tested now and we are seeking new Department of Justice policy for Federal crime reporting to match local and State crime reporting. Other examples of national intelligence and information sharing systems are Law Enforcement Online, or LEO, and the Homeland Security Information Network. The FBI is using LEO to post and disseminate a variety of intelligence products to State and local police as well as to publish its intelligence priorities. We are working closely with DHS to support its mission by collaborating on information and intelligence sharing on DHS information networks.

The FBI supports and participates in local and regional information sharing projects such as LINX in Seattle, WA, which was conceived by the Naval Criminal Investigative Service. LINX is an innovative example of an initiative to integrate disparate law enforcement information into a single data warehouse with the latest analytical tools to produce valuable intelligence that will help prevent terrorism and other crimes. Other examples are the upstate New York Regional Intelligence Center and the California State Warning Center.

Thank you again for inviting me to speak to you today on the information sharing issues that face the Federal Bureau of Investigation and other members of the intelligence and law enforcement communities. It will be my pleasure to answer any questions you may have at this time.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Hulon follows:]

STATEMENT OF

WILLIE T. HULON

DEPUTY ASSISTANT DIRECTOR

COUNTERTERRORISM DIVISION

FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

HOUSE GOVERNMENT REFORM SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

"Facilitating an Enhanced Information Sharing Network That Links Law Enforcement and Homeland Security for Federal, State and Local Governments"

July 13, 2004

Good afternoon Chairman Putnam, Ranking Member Clay and members of the subcommittee. Thank you for inviting me to speak to you today on the information sharing issues that face the Federal Bureau of Investigation and other members of the Intelligence and Law Enforcement communities. The terrorist threat of today poses complex challenges. Today's terrorists operate seamlessly across borders and continents, aided by sophisticated communications technologies; they finance their operations with elaborate funding schemes; and they patiently and methodically plan and prepare their attacks. To meet and defeat this threat, the FBI must have several critical capabilities:

- First, we must be intelligence-driven. To defeat the terrorists, we must develop intelligence about their plans and use that intelligence to disrupt those plans.
- We must be global. We must continue our efforts to develop our overseas law enforcement operations, our partnerships with foreign law enforcement and intelligence services, and our knowledge and expertise about foreign cultures and our terrorist adversaries overseas.
- We must have networked information technology systems. We need the capacity to manage and share our information effectively.
- Finally, we must remain accountable under the Constitution and the rule of law. We must respect human rights and civil liberties as we protect the American people.

Since September 11th, the FBI has investigated thousands of threats to the U.S., and the number of active FBI investigations into potential terrorist activity has quadrupled. Working with our partners, we have also disrupted terrorist activities on multiple occasions inside the U.S., primarily terrorist financing operations.

To achieve success in this war on terror, we have transformed the FBI's Counterterrorism Division (CTD) and CT program to one that is more collaborative and proactive; we have transformed the Intelligence Program and integrated our investigative and intelligence operations; we have improved information sharing with other federal agencies and state and local law enforcement entities; and enhanced our operational capabilities within FBIHQ and all local Field Offices.

A major element of the Bureau's transformation of our Counterterrorism Program is our increasing integration and coordination with our partners in the U.S. and international law enforcement and intelligence communities. More than any other type of enforcement mission, counterterrorism requires the participation of every level of local, state, national, and international government. A good example is the case of the Lackawanna terrorist cell outside Buffalo, New York. From the police officers who helped to identify and conduct surveillance on the cell members; to the information obtained from sources overseas; to the diplomatic personnel who coordinated our efforts with foreign governments; to the FBI agents and federal prosecutors who conducted the investigation leading to the arrests and indictment, everyone played a significant role.

We recognize that a prerequisite for any operational coordination is the full and free exchange of information. Without procedures and mechanisms that allow information sharing on a regular and timely basis, we and our partners cannot expect to align our operational efforts to best accomplish our shared mission. Accordingly, we have taken steps to establish unified FBI-wide policies for sharing information and intelligence.

Interagency Information Sharing

To ensure a coordinated, enterprise-wide approach, Director Mueller recently designated the Executive Assistant Director of Intelligence (EAD-I) to serve as the principal FBI official for information and intelligence sharing policy. In this capacity, the EAD-I functions as an advisor to the Director and provides policy direction on information and intelligence sharing within and outside the FBI with the law enforcement and intelligence communities, as well as foreign governments.

The FBI shares intelligence with other members of the Intelligence Community, to include the intelligence components of the Department of Homeland Security (DHS), through direct classified and unclassified dissemination and through websites on classified Intelligence Community networks. The FBI also shares intelligence with representatives of other elements of the Intelligence Community who participate in Joint Terrorism Task Forces (JTTFs) in the United States or with whom the FBI collaborates in activities abroad. FBI intelligence products shared with the Intelligence Community include both raw and finished intelligence reports.

The FBI uses the Intelligence Community's Intelink-TS to facilitate sharing intelligence products up to the Top Secret Sensitive Compartmented Information (SCI) level. Intelink-TS is carried on the Defense Department's Joint Worldwide Intelligence Communications System (JWICS) and is known in the FBI as the SCI Operational Network (SCION). SCION is currently available to over 1000 users at FBI Headquarters, and the FBI has initiated a pilot deployment project to the following Field Offices: New York, Boston, and Kansas City. The plan is to deliver SCION to all FBI Field Offices, as funding becomes available. Wider access to SCION within the FBI is planned for the future and will enable more extensive on-line collaboration with other intelligence agencies. Limited access to Intelink from other Field Offices is available through the old FBI Intelligence Information System Network (IISNET). Most of the Field Offices have two workstations which have a connection to FBI headquarters.

FBI offices have access to the Secret-level Intelligence Community network SIPRNET, and the FBI website on SIPRNET has been upgraded to provide more information to a wider range of users.

The FBI has established a robust channel for sharing information with the Terrorist Threat Integration Center (TTIC) by providing direct electronic access to classified and unclassified internal FBI investigative and operational databases, with narrow exceptions for certain types of sensitive domestic criminal cases unrelated to terrorism. TTIC also has direct electronic access to internal FBI headquarters division websites and e-mail capabilities on the FBI's classified intranet system. Both FBI and non-FBI personnel assigned to TTIC have access to this information.

The FBI has agreed to provide a substantial permanent staff to TTIC. By the end of this year, there will be 65 FBI personnel allocated to the TTIC. TTIC's mission is to enable full integration of terrorist threat-related information and analysis. It creates a structure to institutionalize sharing across appropriate federal agency lines of terrorist threat-related information in order to form the most comprehensive threat picture.

Although the FBI retains authority to approve dissemination of raw FBI information by TTIC to other agencies, the FBI authorizes the TTIC to share FBI intelligence products by posting them on the TTIC Online website on Intelink-TS. The TTIC Online website provides additional security safeguards, and access is granted to Intelligence Community users who have a need-to-know for more sensitive classified intelligence on international terrorism from the FBI and other agencies. The FBI also authorizes the National Counterintelligence Executive (NCIX) to share FBI counterintelligence products on the Intelink-CI(iCI) website with similar safeguards and access by users who have a need-to-know for more sensitive classified counterintelligence products.

The Bureau fully contributes intelligence analysis to the President's Terrorist Threat Report (PTTR). These products are coordinated with the CIA, DHS, and other federal agencies. In addition to the PTTR, the FBI provides Presidential Intelligence

Assessments directly to the President and the White House Executive Staff on subjects other than terrorism.

The FBI is also committed to providing those tools which assist law enforcement in intelligence-led policing -- from the National Crime Information Center, the Integrated Automated Fingerprint Identification System, and the Interstate Identification Index, to Law Enforcement Online (LEO), a virtual private network that reaches federal, state, and law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO users total nearly 30,000 and that number is increasing. That total includes more than 17,000 state and local law enforcement members. LEO makes finished FBI intelligence products available, including Intelligence Assessments resulting from analysis of criminal, cyber, and terrorism intelligence. Our LEO Intelligence Bulletins are used to disseminate finished intelligence on significant developments or trends. Intelligence Information Reports also are available on LEO at the Law Enforcement Sensitive classification level. The FBI has also posted its terrorism intelligence priorities on LEO as well.

In addition, classified intelligence and other sensitive FBI data are shared with federal, state, and local law enforcement officials with appropriate security clearances who participate in the Joint Terrorism Task Forces (JTTFs). The JTTFs partner FBI personnel with hundreds of investigators from various federal, state, and local agencies, and are important force multipliers in the fight against terrorism. Since September 11, 2001, the FBI has increased the number of JTTFs from 35 to 84 nationwide. We also established the National Joint Terrorism Task Force (NJTTF) at FBI Headquarters, staffed by representatives from 38 federal, state, and local agencies. The mission of the NJTTF is to enhance communication, coordination, and cooperation by acting as the hub of support for the JTTFs throughout the United States, providing a point of fusion for intelligence acquired in support of counterterrorism operations. The FBI will continue to create new avenues of communication between law enforcement agencies to better fight the terrorist threat.

With the creation of the Office of Intelligence at the FBI, each FBI field office has established a Field Intelligence Group (FIG). It is the responsibility of these FIGS to manage, execute and maintain the FBI's intelligence functions within the FBI field office. FIG personnel have access to TS and SCI information so they will be able to receive, analyze, review and recommend sharing this information with entities within the FBI as well as our customers and partners within the Intelligence and Law enforcement communities. The FIGs are our field centerpiece in managing the intelligence cycle within field operations. They will complement the JTTFs and other squads and task forces through the management of the intelligence cycle functions of requirements; planning and direction; collection processing and exploitation; analysis and production and dissemination. The FIGs play a major role in ensuring that from now on, "we know what we know" and we tell others in the Intelligence Community and our federal, state, local and tribal law enforcement partners "what we know".

On February 11, 2004 the Attorney General announced the creation of the DOJ Intelligence Coordinating Council. The Council is comprised of the heads of DOJ agencies with intelligence responsibilities, and is currently chaired by the FBI's EAD-I. The Council will work to improve information sharing within the Department of Justice (DOJ) and to ensure that DOJ meets the intelligence needs of outside customers and acts in accordance with intelligence priorities. It will also identify common challenges (such as electronic connectivity, collaborative analytic tools, and intelligence skills training) and establish policies and programs to address them.

On February 20, 2004 the FBI formed an information sharing policy group, comprised of Executive Assistant Directors, Assistant Directors and other senior executive managers. Under the Direction of the EAD-I, this group is establishing FBI information and intelligence sharing policies.

Intelligence and Analytical Products and Services

In the past year, the FBI has produced more than 3,000 intelligence products, including "raw" reports, intelligence memoranda, in-depth strategic analysis assessments, special event threat assessments, and focused Presidential briefings. We also conducted numerous intelligence briefings to members of Congress, other government agencies, and the law enforcement and intelligence communities. These efforts mark a new beginning for the FBI's intelligence production capability.

Prior to September 11, 2001, the FBI produced very few raw intelligence reports. In FY 2003, we produced and disseminated 2,425 Intelligence Information Reports (IIRs) containing raw intelligence derived from FBI investigations and intelligence collection. The majority of these IIRs contained intelligence related to international terrorism; the next greatest number contained foreign intelligence and counterintelligence information; and the remainder concerned criminal activities and cyber crime. These IIRs were disseminated to a wide customer set in FBI field offices, the Intelligence Community, Defense Community, other federal law enforcement agencies, and U.S. policy entities.

In addition to these raw intelligence reports, the FBI has begun producing analytic assessments on a par with those of other Intelligence Community agencies. The FBI developed and issued, in January 2003, a classified comprehensive assessment of the terrorist threat to the U.S. This assessment focuses on the threats that the FBI sees developing over the next two years, based on an analysis of information regarding the motivations, objectives, methods, and capabilities of existing terrorist groups and the potential for the emergence of new terrorist groups and threats throughout the world. This threat assessment is used as a guide in the allocation of investigative resources, as a useful compilation of threat information for investigators and intelligence personnel within and without the FBI, and as a resource for decision-makers elsewhere in the government. The 2004 threat assessment was released in April 2004. FBI analysts have produced over 100 in-depth analyses and several hundred current intelligence articles in addition to the work they do supporting FBI investigations.

We are preparing to produce, in the near future, the *FBI Daily Report* and the *FBI National Report* to provide daily intelligence briefings to personnel in the field and external customers. One will be produced at the classified level and limited in distribution to upper-level field managers. The other will be unclassified and widely distributed to field office personnel and our partners in the law enforcement community.

A good example of our ability to exploit evidence for its intelligence value and share that intelligence with appropriate members of the law enforcement and Intelligence Communities, is our use of the al-Qa'ida terrorism handbook. A terrorism handbook seized from an al-Qa'ida location overseas in the mid-1990's was declassified and released by DOJ shortly after the events of September 11, 2001. We determined that intelligence gleaned from the handbook could provide useful guidance about al-Qa'ida's interests and capabilities. Accordingly, we produced and disseminated a series of intelligence products to share this intelligence with our personnel in the field and with our law enforcement partners. Nine Intelligence Bulletins were based in whole or in part on this intelligence. In addition, we used information derived from the al-Qa'ida Handbook to update our counterterrorism training, including the Intelligence Analyst Basic Course at the College of Analytical Studies, the Introduction to Counterterrorism Course at the National Academy, and sessions on Terrorism Indicators and Officer Safety in our State/Local Anti-Terrorism Training (SLATT). The unclassified version of the handbook is now maintained as a reference in the FBI Library and is accessible to all the students at the Academy. It also is included in the reference manual CD-Rom distributed as part of SLATT training.

One telling measure of our improved counterterrorism operations is the development of our capability to brief the daily terrorist threat information. The development of this capability reflects the maturing of our centralized Counterterrorism Program.

Prior to September 11th, the FBI lacked the capacity to provide a comprehensive daily terrorism briefing – to assemble the current threat information, to determine what steps were being taken to address each threat, and to present a clear picture of each threat and the Bureau's response to that threat to the Director, senior managers, the Attorney General, and others in the Administration who make operational and policy decisions. With a decentralized program in which investigations were run by individual field offices, the Bureau never had to develop this specialized skill. With the need for centralized management, however, it became an imperative.

In the aftermath of the September 11th terrorist attacks, we were asked to begin sending to the White House each morning daily reports on counterterrorism-related events. We had no mechanism in place for collecting that information, so preparation of the reports was initially haphazard. During the past 34 months, with the assistance of veterans from the Intelligence Community, we have established the infrastructure and the cadre of professionals to produce effective daily briefings and to share briefing materials more widely within the Bureau and with our partners.

In 2002 we established the Presidential Support Group within the Counterterrorism Division to prepare daily briefing materials. In the summer of 2003, this group was renamed the Strategic Analysis Unit and moved to the Office of Intelligence. Beginning in August 2003, the Strategic Analysis Unit began producing the Director's Daily Report (DDR), a daily intelligence briefing that includes information on counterterrorism operations, terrorism threats, and information related to all areas of FBI investigative activity.

To produce the DDR, the Strategic Analysis Unit consolidates and refines information provided in a standardized format by intelligence personnel in each division. Each morning, information about new threats is added, and information about threats that have been thoroughly vetted during the night is removed. The DDR is distributed to executives in all FBI operational divisions. The Director uses the DDR to brief the President nearly every weekday morning. The FBI also produces the *Presidential Intelligence Assessment*, a finished FBI intelligence product covering topics of particular interest to the President, and as noted earlier, our personnel at TTIC and at FBI Headquarters contribute to the formulation of the daily *President's Terrorist Threat Report.*

Beyond these information sharing initiatives, we are increasing our operational coordination with our state, federal, and international partners on a number of fronts.

We have established much stronger working relationships with the CIA and other members of the Intelligence Community. From the Director's daily meetings with the Director of Central Intelligence and CIA briefers, to our regular exchange of personnel among agencies, to our joint efforts in specific investigations and in the Terrorist Threat Integration Center, the Terrorist Screening Center, and other multiagency entities, the FBI and its partners in the Intelligence Community are now integrated at virtually every level of our operations. In addition, the FBI is a participant in the Gang of Eight meetings.

The FBI currently has Agents and Analysts detailed to CIA entities, including the DCI's Counter Terrorist Center (CTC). We also have FBI agents and intelligence analysts detailed to the NSA, the National Security Council, DIA, the Defense Logistics Agency, DOD's Regional Commands, the Department of Energy, and other federal and state agencies.

The Terrorist Threat Integration Center is a good example of our collaborative relationship with our federal partners. Established on May 1, 2003 at the direction of President Bush, TTIC has the primary responsibility in the USG for terrorism analysis (except information relating solely to domestic terrorism, which is the responsibility of the FBI. Analysts from the FBI, CIA, DHS and DOD work side-by-side at TTIC to piece together the big picture of threats to the U.S. and our interests. TTIC analysts synthesize government-wide information regarding current terrorist threats and produce the Presidential Terrorism Threat Report for the President, the Threat Matrix and other analytic products. The FBI personnel at TTIC are part of the Office of Intelligence and work closely with analysts at FBI Headquarters in combining domestic and international terrorism developments in to a comprehensive analysis of terrorist threats. In addition to the analysis developed by FBI analysts detailed to TTIC, FBI analysts at Headquarters regularly contribute articles to the President's Terrorist Threat Report.

At the same time, we have intelligence analysts from other agencies working in key positions throughout the Bureau. The Associate Deputy Assistant Director for Operations in the Counterterrorism Division is a CIA detailee. CIA officers are detailed to the Security Division, including the Assistant Director, the Chief of the Personnel Security Section, and managers working with the SCI program and the FBI Police. An experienced manager from the CIA's Directorate of Science and Technology now heads the Investigative Technologies Division and a Section Chief in that division is on rotation from CIA. This exchange of personnel is taking place in our field offices as well.

We have also worked closely with DHS to ensure that we have the integration and comprehensive information sharing between our agencies that are vital to the success of our missions. The FBI and DHS share database access at TTIC, in the National JTTF at FBI Headquarters, in the Foreign Terrorist Tracking Task Force (FTTTF) and the Terrorist Screening Center (TSC), and in local JTTFs in our field offices around the country. We worked closely together to get the new Terrorist Screening Center up and running. We hold weekly briefings in which our CTD analysts brief their DHS counterparts on current terrorism developments. The FBI and DHS now coordinate all joint warnings through the Homeland Security Advisory System to address our customers' concerns about multiple and duplicative warnings. We designated an experienced executive from the Transportation Security Administration to run the TSC and a senior DHS executive was detailed to the FBI's Office of Intelligence to ensure coordination and transparency between the agencies.

The FBI is committed to participating in the Attorney General's 94 Antiterrorism Advisory Councils that bring together federal, state and local law enforcement, first responders and other federal, state, and local homeland security entities with an interest in preventing and responding to terrorist threats.

Improving the compatibility of information technology systems throughout the Intelligence Community, meanwhile, will increase the speed and ease of information sharing and collaboration. Accordingly, the FBI's information technology team has worked closely with the Chief Information Officers (CIOs) of DHS and other Intelligence Community agencies, to develop our recent and ongoing technology upgrades. This coordination has affected our decisions on several key technology upgrades.

To facilitate further coordination, the FBI CIO sits on the Intelligence Community CIO Executive Council. The Council develops and recommends technical requirements, policies and procedures, and coordinates initiatives to improve the interoperability of information technology systems within the Intelligence Community. It was established by Director of Central Intelligence directive and is chaired by the CIA's CIO.

On March 4, 2003, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence signed a comprehensive Memorandum of

Understanding (MOU) establishing policies and procedures for information sharing, handling, and use. Pursuant to that MOU, information related to terrorist threats and vulnerabilities is provided to DHS automatically without DHS having to request it. Consistent with the protection of sensitive sources and methods and the protection of privacy rights, we now share as a rule, and withhold by exception.

With terrorists traveling, communicating, and planning attacks all around the world, coordination has become more critical than ever before. We have steadily increased our overseas presence and now routinely deploy agents and crime scene experts to assist in the investigation of overseas attacks, such as the May 2003 bombings in Saudi Arabia and Morocco. As of January 7, 2004, 413 FBI personnel were assigned overseas, over 200 of whom are permanently assigned. Their efforts have played a critical role in the successful international operations we have conducted over the past 34 months.

Bureau personnel have participated in numerous investigations of terrorist attacks in foreign countries over the past 34 months. Our approach to those investigations differs from the approach we traditionally have taken. Prior to September 11th, our overseas investigations primarily focused on building cases for prosecution in the U.S. Today, our focus has broadened to providing investigative, forensic, and other types of support. This is paying dividends with greater reciprocal cooperation and more effective joint investigations.

Information Sharing Systems

The FBI has a responsibility to the nation, Intelligence Community, and federal, state and local law enforcement to disseminate information, and to do so is an inherent part of our mission. Sharing FBI information will be the rule; filtering the information will be the exception, where sharing is legally or procedurally unacceptable. The FBI will deliver its information through the systems the FBI and its customers and partners use.

In the area of organizational message traffic for dissemination of official information and taskings to other agencies, the FBI has just implemented its new FBI Automated Messaging System (FAMS) which is based on the Defense Messaging System (DMS). FAMS will provide on-line message creation, review, and search capabilities to everyone connected to FBINET. FAMS gives us the capability to send and receive critical organizational message traffic to any of the 40,000+ addresses on DMS or Automated Digital Network (AUTODIN). The TS/SCI version of FAMS is currently in testing and will provide the same capability to everyone on SCION or IISNET in the near future. The FBI's implementation of the DMS will provide writer-to-reader secure e-mail to internal and external users. Within the government, DMS will replace AUTODIN and a diverse array of e-mail systems currently in use throughout the Department of Defense and Intelligence Agencies. In its final form, DMS could become the government's global secure e-mail system. It will provide certified interoperability of various commercially off-the-shelf software products and connect over 2 million civilian and military users. The system will permit multi-media attachments to messages and provide end-to-end security.

The FBI Chief Information Officer is also working with the Department of Justice on interfaces between the Intelligence Community System for Information Sharing (ICSIS) and the Law Enforcement Information Sharing initiative, and with the FBI Criminal Justice Information Services (CJIS) Division to increase the sharing of intelligence related information to and from state and local officials.

The FBI is currently deploying the SECRET versions of FAMS, which uses DMS and secure Outlook-like e-mail for organizational messages, so that our analysts and reports officers can send and receive timely intelligence with other agencies in near real time. The FBI is also working on a digital production capability for IIRs using extended markup language (XML) that will interface with FAMS and support on-line digital production of intelligence reports. The FBI is applying XML data standards and meta-data tagging to facilitate the exchange of information with the intelligence community. The FBI is also applying new security technology to deploy a Protection Level 3 Data Mart capability with discretionary access controls and Public Key Infrastructure certificates in support of closed Community of Interests, which will permit secure sharing of our most sensitive data with trusted members of other agencies. The FBI is also investigating the use of secure one-way transfers to move information between security domains and to permit all-source intelligence analysis. The use of next-generation, community High Assurance Guards is being planned to provide for the two-way transfer of critical intelligence between security domains. Secure wireless connectivity and Virtual Private Networks are also being looked at to provide increased access to intelligence to deployed personnel. The FBI is also starting to use On-line, desktop collaboration tools such as Info Work Space which is the foundation for the Intelligence Community Collaboration Portal to increase intelligence collaboration.

The FBI plans to use additional systems as the foundation for additional information sharing with the Intelligence Community, Federal, State and Local entities.

The CJIS National Data Exchange (NDEx) has plans for developing a systems approach to the operation, and maintenance of several interconnected IT and supporting telecommunications systems including Law Enforcement On-line (LEO) and CJIS Wide Area Network (WAN). The NDEx is to be a repository of national indices and a pointer system for state/local/federal and inter-governmental law enforcement entities. The NDEx will also be a fusion point for the correlation of nationally-based criminal justice information with certain national security data.

Law Enforcement On-Line provides web-based communications to the law enforcement community to exchange information, conduct on-line education programs, and participate in professional special interest and topically focused dialog. The system has been operational since 1995 and presently serves about 30,000 users. LEO has secure connectivity to the Regional Information Sharing Systems network (riss.net). The FBI Intelligence products are disseminated weekly via LEO to over 17,000 law enforcement agencies and to

60 federal agencies, providing information about terrorism, criminal and cyber threats to patrol officers and other local law enforcement personnel who have direct daily contacts with the general public. The FBI plans to enhance LEO for robust, high-availability operation. The FBI will use the enhanced LEO as the primary channel for sensitive but unclassified communications with other federal, state and local agencies. LEO and the Department of Homeland Security's Joint Regional Information Exchange System (JRIES) will be interoperable.

The Investigative Data Warehouse (IDW) is following a multiple-phased approach to quickly provide support to FBI investigators, and JTTF members in the form of a spirally-developed operational prototype system, the *Secure Counterterrorism Operational Prototype Environment* (SCOPE). The IDW provides the Bureau with a single access point to several data sources that were previously available only through separate, stove-piped systems. By providing consolidated access to the data, for the first time analytical tools can be used across data sources to provide a more complete view of the information possessed by the Bureau.

The IDW, delivered in its first phase in January 2004, now provides analysts with full access to investigative information within FBI files, including ACS and VGTOF data, open source news feeds, and the files of other federal agencies such as DHS. The IDW provides physical storage for data and allows users to access that data without needing to know its physical location or format. The data in the IDW is at the Secret level, and the addition of TS/SCI level data is in the planning stages.

Later this year, we plan to enhance the IDW by adding additional data sources, such as Suspicious Activity Reports, and by making it easier to search. When the IDW is complete, Agents, JTTF members and analysts, using new analytical tools, will be able to search rapidly for pictures of known terrorists and match or compare the pictures with other individuals in minutes rather than days. They will be able to extract subjects' addresses, phone numbers, and other data in seconds, rather than searching for it manually. They will have the ability to identify relationships across cases. They will be able to search up to 100 million pages of international terrorism-related documents in seconds. The IDW will help meet the law enforcement and the IC need for rapid, secure, dependable indexed data and will provide data mining access to FBI investigative files.

We are introducing advanced analytical tools to help us make the most of the data stored in the IDW. These tools allow FBI agents and analysts to look across multiple cases and multiple data sources to identify relationships and other pieces of information that were not readily available using older FBI systems. These tools 1) make database searches simple and effective; 2) give analysts new visualization, geo-mapping, link-chart capabilities and reporting capabilities; and 3) allow analysts to request automatic updates to their query results whenever new, relevant data is downloaded into the database.

Another information sharing project, the Multi-agency Information Sharing Initiative (MIS), is intended to enable Federal, state, and local law enforcement agencies to share regional investigative files and provide powerful tools for cross-file analyses. A proof-of-concept effort is underway in St. Louis; additional demonstration sites are being planned.

The goal of the demonstrations is to (1) show the value of sharing investigative data which can be analyzed by modern software tools; and (2) help define technical and organizational approaches for regional shared systems. Final decisions about deployment of the MIS will be based on the results of the demonstrations and the department wide plan for law enforcement information sharing being developed by the Department of Justice.

Thank you for allowing me the opportunity to testify before you today and I will be happy to entertain any questions you may have.

Mr. PUTNAM. Mr. Clay, do you have a statement you would like to place in the record?

Mr. CLAY. I do, Mr. Chairman. And I will forego reading if we can get right into the questions and I ask that my remarks be inserted into the record.

Mr. PUTNAM. Without objection, your opening statement will be inserted into the record and you are recognized for 5 minutes of questioning.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

STATEMENT OF THE HONORABLE WM. LACY CLAY
HEARING ON INFORMATION SHARING

JULY 13, 2004

Thank you Mr. Chairman for calling this hearing, and I thank the witnesses for their testimony. Although this is not the first time our subcommittee has taken up the issues of information sharing and technological limitations facing first responders, we seem to be making little headway in formatting a comprehensive mode of communications and information exchange for both the public and private sectors.

Recent events overseas and continued terrorist threats at home leave us little choice in establishing a seamless network for first responders and law enforcement agencies, but turf wars and inadequate resources continue to hamper our efforts. As we continue to focus our efforts in strengthening the Department of Homeland Security, other vital stakeholders seem to be forgotten or not held accountable.

From an administrative standpoint, the problems are obvious to identify, but painstakingly difficult to resolve. To begin, there are too many stakeholders in the federal agency community unwilling to trust or cooperate with their counterparts, leaving the needs of states and local governments untended to. Furthermore, we have chronic friction among the states and localities, as resources are limited and the needs of urban, suburban, and rural stakeholders vary greatly.

Information sharing, broadly speaking, requires coordinated effort and trustworthiness among all federal agencies. This goes beyond the often referenced "turf wars" taking place between the many components which make up our nation's intelligence community. More appropriately, it extends to diverse participants not accustomed to having a role in law enforcement, such as the Federal Communications Commission or the Federal Aviation Administration. Money alone will not solve our information sharing deficiencies unless our bureaucracy begins to work in concert for achieving its mission of establishing adequate information sharing policies.

Again, I thank the Chairman and our witnesses, and ask that my remarks be inserted into the record.

Mr. CLAY. Thank you, Mr. Chairman. I would like to start with Mr. Hughes. Does DHS plan to replace existing systems with a new national communications infrastructure? And if so, what are the specific milestones for implementing a national infrastructure?

General HUGHES. To the best of my knowledge, we do not have any intent to replace what you have referred to there, sir, as the national communications infrastructure. We plan to use it and ride upon it, connect using the capabilities that exist now and those that come in the future. But the Homeland Security Information Network does not duplicate most of that structure. It merely rides upon it.

Mr. CLAY. Mr. Hughes, let me ask you about TSA. Are we safer in our airports now since September 11 with TSA? Do they have the adequate information in order to be able to detect what probably shouldn't be on an airplane?

General HUGHES. Yes, we are safer. And they do have information that tips them off to persons that we call persons of interest. It happens many, many times every day that persons who have come to our attention through intelligence or other information channels are sent to the Transportation Security Agency screeners and to the Customs and Border Protection officers that man the points of entry. TSA, itself, as you know is not an armed law enforcement organization, but Customs and Border Protection, Immigration and Customs Enforcement and the Federal Bureau of Investigation and local police, of course, take care of the law enforcement portion of that activity.

Mr. CLAY. I notice that in some airports TSA interacts with private security companies.

General HUGHES. That is true.

Mr. CLAY. How does that work?

General HUGHES. I think it is a cooperative association where some of the functions of screening passengers for their documentation especially—I will use as an example when you get into a line at the airport to approach the TSA screening point, you have to present a photo identification and your ticket in order to pass into the screening point, and often those persons are local security people who have been contract hired to perform that function. But the function of screening the individual, their carry-on luggage and person, is the TSA's function.

Mr. CLAY. I thank you for that explanation.

Let me ask a question of the entire panel and we can start with Mr. Hulon. It seems to me that the goals for information sharing among stakeholders are well established, but the emergence of new threats make determining what our domestic or international threats are less clear. Are the stakeholder agencies such as DOJ, DHS and DOD working on methods to refine their determinants for what constitutes domestic or international-related incidents?

Mr. HULON. Yes, sir. Actually, Federal law enforcement is working collectively to identify those threats as we develop the intelligence. I think the thing that is really key is that through various relationships that are established specifically at the State and local level with the JTTFs, that information is passed to the appropriate local agencies so that we can take the right precautionary action to either disrupt or to gain additional information in regards to the potential threat.

Mr. TRAVERS. Yes, sir. I believe TTIC is a manifestation of exactly the phenomena about which you speak. We are represented with partner agencies to include the three you mentioned and we have 16 organizations within TTIC. And our job is to bring together threat information whether it is collected domestically or abroad. So we are precisely attentive to that problem with a blurriness between domestic and foreign threats.

General HUGHES. I think, first of all, Mr. Hulon's characterization is one that I would certainly agree with and certainly Mr. Travers, that this is a cooperative group effort and it is largely about human beings. It is largely about identifying persons who have for some reason come to our attention, and then processing them appropriately.

In order to do that every day, we have to engage in some form of interaction. Quite often it is at a meeting, or sending a message to each other alerting one or another agency involved in this process about those people of interest. And that is working well, however it is not perfect. And frankly, it is about as dynamic as the traveling public who comes to America and travels inside America is. It is a very large body of activity and human beings to deal with.

Mr. CLAY. Thank you. Mr. Travers, since TTIC is not actually under the domain of the CIA or FBI, can its efforts to break down the barriers for information sharing between the two agencies be successful over the long term of its operation, and has TTIC had any managerial or strategic disagreements with its participating agencies on how to pursue its mission or goals?

Mr. TRAVERS. Two part question. With regard to information sharing barriers, I believe that we have enjoyed extraordinary success working with our partners across the government. As I suggested in my statement, none of these issues, at least in our view, lends itself to an easy fix. They have multiple components. There are, as suggested, source sensitivities, operational considerations, and there is always a balance; and we work with our partner organizations on a daily basis to break down the institutional barriers that exist and we have enjoyed substantial success.

With regard to disagreements, I think it's fair to say that there is ambiguity in TTIC's mission relative to many other terrorism analytic organizations' missions across the government. I believe that is to be expected. We are dealing with organizations, departments, and agencies that go back to the National Security Act. We are dealing with some that go back to September 11. The government is not of one mind on precisely how best to sort this out, and so we are working through that on a daily basis.

Mr. CLAY. Just as a followup, my concern would be that we would not gum up the works to the point that it would hamper our ability to apprehend someone or to point out the real threat or to just make law enforcement that more ineffective. I mean that would be my concern, and hopefully——

Mr. TRAVERS. TTIC has no operational responsibilities. I don't believe you would find any of our operational partners has gummed up the works.

Mr. CLAY. Thank you for your response. And thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, Mr. Clay.

Last couple of weeks, the press has reported on a number of DHS initiatives to promote information sharing—including the expansion of the HSIN, which was launched in February—to the Secret level and the upgrading of the new Homeland Security Operational Center to promote information sharing.

With these and other efforts underway, how does the Department envision itself promoting information sharing between levels of government? And how far a reach does the DHS plan to have, and what role or other law enforcement agencies pulling in that?

General HUGHES. I need to correct something about the information there. We have not yet secured the Homeland Security Information Network to the Secret level. It is our attempt to do so by December of this year. But we put the first part of the Information Network Online at the Sensitive but Unclassified level. And we do pass law enforcement Sensitive but Unclassified information over that system. But the Secret classification will have to come in the next few months.

Our intent is to connect to all States and we are now connected to all 50 States to the governance level, either the State Governor's Office or the Homeland Security Office, or both, to all territories and possessions. And I believe we have one or two of those remaining. But generally we are connected. We intend to connect to many counties, if not all; all major cities; some municipalities which are complex organisms like themselves, like Los Angeles and Los Angeles County. New York would fit in that category, too. We would at some point connect to the tribal organizations, especially those that have administrative burdens on the borders of our country with Canada and Mexico. And last if not least, we intend to extend the Homeland Security Information Network into the private sector, especially to those companies and business organizations which have a nexus to their work ethic and national or homeland security.

Mr. PUTNAM. Let me ask each of you to answer this. Who determines what information is passed along the chain and who determines to whom it is passed? Is that TTIC's responsibility? Who makes that decision ultimately? And I want to begin with the FBI.

Mr. HULON. It would depend on the nature of the information. But there are various systems in place to pass information. At the FBI, we have an Office of Intelligence that is basically responsible for assimulating and working with the other Federal agencies as well as State agencies with the collection and analysis of that information. Depending on the nature of that information as far as what it entails, what the threat might be or what the intelligence value of that information is, decisions will be made on where it goes.

For example, if it is threat-related information that impacts a certain jurisdiction, then that information would go directly through the FBI and the other agencies that are involved to the appropriate law enforcement agencies at the level that they could effect whatever action that needs to be taken. And that information will be passed, say, to a JTTF, say, in Jacksonville, Florida. If there was information that impacted Jacksonville, Florida, that information would come into the FBI and come into the appropriate headquarters entity and then be disseminated to our appropriate channels down to that field office and go to the field intelligence group that we have there that is responsible for assessing that information, and then it would be disseminated to the appropriate JTTF members or the appropriate law enforcement agency that should get that information.

Mr. PUTNAM. Mr. Travers.

Mr. TRAVERS. TTIC is not a collection organization. I have to distinguish between raw material and analyzed product. To the degree we receive products from the collection organizations, be they FBI, DHS or NSA or CIA, we will make that material as broadly available as the collector will allow us. If there are originator control restrictions, then, that may in fact restrict the amount of information that can go on a TTIC Online, for example. But to the degree we can make it available, we make it available as broadly as we can. Our finished products will be the same in that some product will be limited for very narrow audiences at the most senior levels of the government, but in general what we try to do is make information as broadly available across the Federal structures as possible.

Mr. PUTNAM. General.

General HUGHES. I think first, I think both answers are correct and bear on DHS. I would like to give you two other perspectives. Some information has to be sensitively applied, and so the answer to the question who makes this determination, the answer I think should be given as leadership often has to make that determination. We decide very specifically at the leadership level, and sometimes the Secretary will decide where information goes and who it goes to and how it goes. And that would be the exception rather than the rule. But we often find ourselves dealing with exceptional information which if it didn't go to the right place at the right time, may have an unintended effect or consequence. That is especially true of our constituency, much like the FBI's. It is broad throughout the country. But in our case, it is not to Federal officials who are of longstanding experience in the intelligence and law enforcement system, but instead to persons who might have even a year or two of fairly spotty experience in handling federally originated information. So this is, once again, I think the point was made earlier, it is a complete organism.

The last point I would like to make is that we are beginning now—and I think the FBI and DHS have set the standard here but others are doing this to, as frequently as we can, where it is appropriate, act jointly. Indeed, Mr. Hulon and I have recently acted jointly to inform local officials about various circumstances. And that communication mechanism, whether it is by secure telephone or open telephone or message or however it's done, gives added weight and importance and perhaps motivation to those we communicate with about the information. It's up to us to put it in the right context. But that joint effort from the Federal Government speaking together in some ways or collectively is vital to making this information meaningful and clarifying it to the respondents and people who receive it.

Mr. PUTNAM. Let me followup on that. TTIC does not generate information, you disseminate it. That's the point you wanted to make earlier, correct?

Mr. TRAVERS. We do not collect information. We do have analysts who will pull together all source products and disseminate those.

Mr. PUTNAM. If there is information about a potential event in a given city, what I'm really getting at, there are dozens of Federal and State law enforcement agencies that would immediately be involved. Where do you stop? You know, if you take Mr. Hulon's example of something in Jacksonville, you only do the city of Jacksonville, or do you do the county or surrounding counties, particularly if the airport for that city is in a different county? What point does it stop?

And we can get into this with the second panel, when we have some of our State and local representatives, but it is the most common complaint is that folks still aren't getting the information. But when you look at the number of agencies only in the Federal Government that might have an interest in that piece of information and then to extrapolate it down to the boots in the alley, is there a technological system for disseminating that information or does it boil down to a judgment call by a human being?

Mr. TRAVERS. If that is directed to me, just a point of clarification. I don't deal with State and local organizations. I pass my information to the Bureau and to DHS, and they are much more intimately involved in the vertical information sharing, so over to them.

Mr. HULON. I can respond to that. Actually, it is twofold. We have networks that we can use, such as inlets, if we have a general message to get out, say if we are reporting something relative to threats or trends that all of law enforcement should be on the lookout for, general information, that could go out over the inlets and that is available to all law enforcement. Anybody can go on that's in law enforcement and get on to the inlets.

Mr. PUTNAM. They could. You make them aware that information is posted that they ought to go read more about? Is that the way that it works?

Mr. HULON. With inlets, though, you would have a local law enforcement agency, a State agency. There are dispatchers monitoring the inlets. They would see that and pull it off and it would go to the appropriate person in that department. If we have something more specific, say to a general area, like a city or surrounding counties, you know, if that information should go to the city and the surrounding counties, we will make a judgment call that this information needs to be in this general area or this region, and we would make the notifications primarily for the FBI through our law enforcement networks which would be the JTTFs, which is what we rely on. And we have a lot of agencies that are involved in the joint terrorism task forces.

And what happens on the field level—and I can kind of speak to that—we would make those notifications based on other associations that we have in that law enforcement community, whether that would be with the sheriff's association, police chief's association or whatever. And that is one mechanism we can use to put general information out to the entire law enforcement community: you should be on the look out for this.

If it's threat information that's relative to an investigation or something we need to disrupt, then, of course, that information decision will be made on who does this information need to go to so we can effectively disrupt this operation or conduct this investigation without compromising it. And decisions have to be made there. And those are human decisions that, you know, basically the field office agent in charge is responsible for and we have networks to really facilitate that.

And we talk about networks and we talk about IT systems, a lot of it depends on what we have in place, and that is a collective effort of law enforcement. You see it a lot when you get outside the D.C. area where you have State and local agencies working together, you have various associations, you have various law enforcement head working groups where there is a constant exchange of information.

Now, could there be times where something might fall through the cracks and one particular agency might not get informed of some general information? That could in fact happen, but for the most part, it is really the relationships and the liaisons that are established among all the law enforcement that really helps to facilitate a lot of this information getting out.

Mr. PUTNAM. In a post September 11 world, if one of your agents in Detroit made an observation, they had a hunch that was backed up by some facts that there was an unusual interest in flight schools, how would someone in Pahokee, Florida, where another flight school was, know that someone halfway across the country had made an observation that was relevant to them?

Mr. HULON. That information, say coming from Detroit, would go through the Detroit field office and make its way back through FBI headquarters to the Office of Intelligence where the information is assessed, assimilated, shared with the components of the Office of Intelligence which has participants from all the other agencies; all that information would be put back together to bring it into some type of understanding of this is a potential threat or this is a trend we should be aware of.

And that is where sometimes TTIC will come in because they would have access to that information. We might have someone put an analytical piece together that would go out at TTIC or could go out in the form of an intelligence bulletin from the FBI. And the FBI intelligence bulletins are disseminated through LEO Law Enforcement Online where we have several thousand police agencies access that information that are members of that network to where they can get that information off. So information would be disseminated that way.

Mr. PUTNAM. At what point would TTIC be involved?

Mr. HULON. When the information comes back to headquarters, TTIC would have access to that information also. And it could be a collaborative effort where this would be shared with TTIC. And they could work along with the other intelligence agencies to put together an analytical piece.

Mr. PUTNAM. How long are we talking about? From the time this report is filed until the time that other law enforcement agencies around the country have the opportunity to pick up on it, how much time has elapsed?

Mr. HULON. It depends. And another way this could work also is information coming back to headquarters. It could go out as an intelligence requirement where we would disseminate this from the Office of Intelligence to State and local agencies where we have intelligence requirements that go out, to ask them to report certain information or be on the lookout for certain information. If you have that backed up through the FBI, it could go out through those channels. A lot of it depends on the nature of the information.

Mr. TRAVERS. I would concur with that entirely. TTIC would have instantaneous access to that information given that many of our analysts have access to FBI Net. It becomes part of the analytic grist mill that is occurring amongst the various intelligence organizations dealing with terrorism analysis and then is put out as a product, and then the organization that's responsible for vertical information sharing to push it down in the various ways that Willie talked about.

Mr. PUTNAM. Let me approach this from a different angle. A telephone number is found in a cave in Afghanistan. How long does it take before that telephone number is in all these data bases that it then becomes actionable, or an address is discovered? How long between the time that some marine picks it up in the bottom of the cave in Afghanistan until the time that it winds up—let's say it is a Detroit area code, and ends up on one of his agent's desk—how much time elapses?

Mr. TRAVERS. It is going to depend on the medium in which we get that telephone number, and I think I would rather talk about this in closed session, if we could, but it's going to move its way back to Washington and be made available. But it could be some period of time, or maybe very little period of time, in terms of the amount of effort that goes into getting that number out of whatever the mechanism is in which we recovered it. I will need to talk to you about that off line, sir.

Mr. PUTNAM. We will do that, because it is the key to your existence. I mean, the whole point of TTIC is to rapidly assimilate and then analyze and disseminate information to guys like Mr. Hulon in Detroit when things are being discovered or heard or overheard or whatever. Let me move onto the next question.

The volume of information that all three of your departments or agencies generate, how much are we talking about here so that the average FBI agent, the average police chief in a medium-sized city, or the average intelligence law enforcement officer in a major police department, are they just being covered up in threats all day every day? Are there e-mails coming in every hour on the hour? Is that something that is condensed into a weekly bulletin? If you take all this data that's out there, how much information does it become when it reaches the end of the pipe?

General HUGHES. I will go ahead and start. First, this kind of refers in part to the previous discussion. I think this is a collective attempt here—we're trying to get specific information to the right place, not every piece of information every place. I believe that moderates the effect, the larger effect of so much information. But I don't know of a good way to characterize the volume except to say that it is large and it is growing, because we are now getting information from the civilian population here in the United States as well as from the traditional law enforcement and security organizations and from the Federal Government's activities.

That large body of information is representing a much larger influx of information at some level, that I would imagine that there are still some police departments, some homeland security elements and others, who don't get too much information. And to be honest with you, that may be a function and part of who they are and where they are. It is just some places are much more active than others.

If you went to the New York City Police Department, let me tell you, the information flow is large but probably not as large as they would like. I think they would like to have more; at least that is what they tell me. So I don't think there is an answer.

Mr. PUTNAM. Mr. Clay.

Mr. CLAY. Mr. Hughes, since September 11, funds have gone to States and localities to improve emergency response planning. Many of these funds request the States to submit an emergency preparedness plan. For example, the Office of Domestic Preparedness is requesting the States submit a statewide strategic plan for fiscal year 2004 funds. Can you tell us what DHS is doing to ensure coordination among other Federal agencies that request emergency preparedness plans?

General HUGHES. I know we give the agencies and organizations that submit those plans as much help as we can with regard to the preparation of them. I would say probably not a happy constituency out there. I know there are complaints about the application of these funds, but it is frankly, quite difficult to do on a basis that makes everyone happy.

But I am not sure if I understood your question exactly beyond help to prepare the plan. Once we get the plan, we try to administer it appropriately with the other agencies in government here in Washington.

Mr. CLAY. That was the question. I thank you for that answer.

Mr. Travers, although TTIC is funded through several agencies' budgets, are there specific resource allocation concerns that Congress needs to be concerned in order for the TTIC to fulfill its objectives?

Mr. TRAVERS. No, sir, I don't believe so. We are funded out of the community management account for operations and maintenance and our building and so forth and our personal services are handled, given that we are assignees. DIA continues to pay my salary. We are working a memorandum of agreement with all of the partner organizations to ensure adequate manning of TTIC, and I believe we are in good shape.

Mr. CLAY. According to recent GAO studies, there are still more than 12 Federal agencies with more than nine different watch lists, and that doesn't include the CIA. Further, the GAO cites that in spite of congressional direction, information sharing remains inconsistent and limited. What role is DHS claiming to make information sharing more seamless among Federal agencies?

Mr. TRAVERS. Asking me about DHS?

Mr. CLAY. You are familiar with their operation, like you are familiar with yours. How is information seamless among the agencies?

Mr. TRAVERS. Let me use the watch list example, then, if we go back to that. TTIC has responsibility under HSPD 6 with maintaining an all source data base for the U.S. Government on all known and suspected terrorists. So all sources of information, be they from the Bureau, DHS, CIA, FBI comes into TTIC.

We maintain the data base on known and suspected terrorists that is available to the community. Under HSPD 6, we then provide to the Terrorist Screening Center unclassified data elements so they can make those available to any screening opportunities that occur, be they in the United States or external. So it is a vast simplification of what occurred in the period leading up to September 11.

Mr. CLAY. How do citizens who may show up erroneously on a list, how do they address that?

Mr. TRAVERS. This data base will for the first time have U.S. persons in it. We are being assigned 15 FBI officers to maintain the U.S.-person portion of that data base, and electronic communication will come in to TTIC. If an investigation is started up on a U.S. person, if it is determined that person is no longer under investigation, we will get an electronic communication in to ensure that we pull that person out.

Mr. CLAY. All of the lists from all of the agencies.

Mr. TRAVERS. For U.S. persons particularly. So we are very attentive to that.

Mr. CLAY. OK. Thank you for that answer.

Mr. Hulon, from your perspective, has the establishment of the TTIC aided in the information sharing practices between agencies, or is interagency coordination still inadequate?

Mr. HULON. I think there's always room for improvement. However, I would like to state that I think, today, after September 11, we are much better off than we were in the past, because what we have is, collectively, you have a lot of agencies coming together and actually, really making efforts to share information, just like some of the cross-designations, when we talk about the various agencies having representatives at other agencies, shops. Like in my division, in the Counter Terrorism Division at the FBI, the associate deputy director is from an intelligence agency that works with us.

So, I think, collectively, we are really pulling together to make sure that we are sharing information better. We are looking for ways that we can do it that doesn't violate any laws, that doesn't violate any privacy acts, and things of that matter. And I think, with TTIC, what they are doing, like has been reported, they are taking this information and going to a lot of public-source information and putting together analytical pieces that go out to the law enforcement and intelligence communities that assist and enhance our abilities to look at information overall. So I think, collectively, we are moving down the road, and we are going to get where we need to be.

Mr. CLAY. And you are comfortable that the coordination is there and that the information is valid and good?

Mr. HULON. Yes, sir, I am confident that we are really working toward that. We have made a lot of improvements in the last 2½ years.

Mr. CLAY. I thank you for your response and thank the panel for your response.

Thank you.

Mr. PUTNAM. Thank you.

Mr. Travers, you mentioned in your opening statement that information sharing is not just a bumper sticker, and I think that's well put. I mean, it's terribly complicated, and the more you peel the onion, the more layers there are as we get through this.

I believe you also were the one who said that technical capabilities vary between the agencies who need to be talking to each other? And since this is the tech subcommittee, let me peel that onion a little bit.

Mr. Hulon, the FBI is notorious for having lousy computer systems. Has your technology improved post September 11? Do you now have the tools that you need, whether it's in an office in Detroit or here at the headquarters, to be able to send and receive information in the 21st century?

Mr. HULON. First of all, I would like to maybe make a disclaimer. I am not a real technical person. However, I do know that the FBI technical systems are not quite where they should be.

Efforts are being made to improve those systems. However, we are continuing to work through the problem. So, actually, I am just not the best person to really get into the technical aspects of the systems themselves.

Mr. PUTNAM. General, is that a problem? I mean, if you look at all the agencies that used to be on their own and that are now just under DHS and add to that all of the other agencies that DHS needs to be listening to or talking to, how frequently, I mean, you pointed out correctly that legal and cultural barriers are the biggest problems, but how often is technology the problem?

General HUGHES. I think it's kind of a different question, if I may rephrase it. Technology is what it is, and if we had the best technology the world can provide, we wouldn't have that kind of problem.

It is true that some agencies are more technologically advanced than others, but the FBI and TTIC and DHS sitting here, we probably have different variations on the theme of technological capability. But I personally believe that they could, all of us could, interact, given the decision to do so. That's my view.

My personal viewpoint—I don't think I should speak for DHS here—is that what prevents us from doing that is making a decision to do it, and that's my personal view. I guess like you, sir, I am a creature of the automation system I have at home. And the only impediment I can see to interaction with virtually the world is someone deciding not to interact with me.

Mr. PUTNAM. So, are all of the agencies now at a technological point of equivalence that everyone is now adequate, everyone has the tools they need to send and receive the information on an interagency basis?

General HUGHES. No. I don't think I should go that far. Once again, some agencies and some organizations are behind, technologically.

Mr. PUTNAM. And who is? Who is ahead, and who is behind?

General HUGHES. I don't think it's appropriate for me to answer your question, because I would have to characterize organizations specifically to talk about things that I may not fully understand. I can look you in the eye and tell you that the Department I represent is technologically advanced. We are capable of interacting on every level.

Mr. PUTNAM. You as the Department of Homeland Security?

General HUGHES. That is correct.

Mr. PUTNAM. And everyone that got folded up inside of you is now technologically advanced and capable of communicating technologically?

General HUGHES. No.

Mr. PUTNAM. Well, then, who is you?

General HUGHES. Actually, I speak for myself, and my organization here. The intelligence side of the house is very, very good, very, very capable.

But some other administrative developments are not—elements are not, and some other organizational elements may have organizational shortcomings in this regard.

But, once again, I hasten to tell you, the technology is there. It may not have been installed or it may not have been acquired for installation, but it can be, and, in my view, it should be.

Mr. PUTNAM. Well, in my view, it should be, too, but you won't tell me where I am supposed to do it.

General HUGHES. Well, I will be glad to talk about DHS, if that will help you.

Mr. PUTNAM. That will. That's a start.

General HUGHES. Inside the Department of Homeland Security, the organizations that were folded in under the large DHS umbrella include the U.S. Secret Service, the U.S. Coast Guard, the former Bureau of Customs, the former Department of Immigration and Naturalization, the Federal Protective Service, the Federal Air Marshals and some other organizational entities. Each of those has their own system.

Not every part of that system is compatible or fully interoperable, because it is composed of a set of legacy systems that were designed some years ago, perhaps even as long as 10 years ago, and other parts of that system are newly provided. They are newly engineered into this amalgam.

So, across the Department of Homeland Security, we need to—and we are, we have a program to do this, which I mentioned, the information sharing and collaboration program, which is a formal effort to normalize for purposes of interoperability and compatibility, across the organization, internal to DHS.

With regard to our external communication, the Homeland Security Operation Center, and the information analysis element that I had, those two organizations between them do not have any compatibility problems with anyone else; we could make it work.

Mr. PUTNAM. Well, that's all. That's fantastic. That's what we are after. I mean, the title of this hearing is, Facilitating Information

Exchange, and we need to know where, where the information exchange is working particularly well, and where it's not. And we had a number of hearings prior to September 11th that pointed out an awful lot of problems in communications, and I don't think they went away immediately, but I would like to know that we are on some plan to make them go away.

And that's just within the Department of Homeland Security, not to mention the new monsters that have been created since then, in addition to the DHS, like TTIC, and certainly the radical transformation that's going on in the FBI, both culturally and in terms of the scope of their responsibilities.

So, that's why we are picking that scab, is because we are trying to get to the bottom of this to try to figure out what we can do to improve this thing.

And, you know, I know everybody suits up and goes to work every day trying to figure out new ways to protect the American people. We just want to know if you have the tools you need to do it. That's where we are going with this.

General HUGHES. I think that's an admirable goal. And, speaking for my organization—not others—you have done a good job of providing us with both money and technical capability to do the job. We have taken advantage of it.

Mr. PUTNAM. Let me ask a final question as a segue into our second panel. Any or all three of you would certainly be welcome to answer. How much good, actionable information do you receive from the bottom up? We have spent most of this time talking about how effectively you pass along your tips down to local law enforcement. How much good stuff is coming back up the pipe?

Mr. Hulon.

Mr. HULON. Mr. Chairman, I can speak to that, solely reflecting back on my former duty as the agent in charge in Detroit. We do get a lot of information coming up, and a lot of it might be relative to preoperational type surveillances or suspicious-type activity that's reported back up to the FBI from some police officers on the street. You know, they might see something that seems out of the ordinary. And because of the relationships that are established in the field offices, between the FBI, State and local law enforcement agencies, as well as other agencies, that information is provided back to that police department's intelligence bureau, if they have one, or directly to someone in investigations who might be associated or affiliated with the JTTFs.

That information comes into the JTTFs. It goes to the intelligence components in the field offices for immediate action if it's necessary, and then, of course, then, it can be channeled back to headquarters, FBI headquarters, and goes to the Office of Intelligence to be assimilated in the total overall intelligence, as being gathered and analyzed. So, it does come back up, too. I can't really quantify that for you, though, but there are situations where it does happen.

Mr. PUTNAM. General Hughes.

General HUGHES. I think, once again, I think Russ Travers didn't answer, because he is not in that category. But we receive quite a lot of information—it's a growing body of information—from local input. But it is not as good as it can be or will be in the future.

Part of that issue is the fielding of connectivity, and the case of the Homeland Security is slightly different from the FBI's in that we are not dealing just with the law enforcement mechanism or the security mechanisms who usually do have good communications, mechanisms, even if it's interpersonal. We are dealing with a new body and a broader body of individuals, down to the citizen level.

We are getting reports from individual citizens who note something suspicious. They communicate that to the appropriate authority. Quite often, it's law enforcement. But, whatever the mechanism, whatever the authority they communicate it to, that is now finding its way, often in parallel, to the Federal Bureau of Investigation or other Federal law enforcement like ATF or DEA or somebody like that and to the Homeland Security headquarters, and that's, I think, a very good thing. That will improve and grow over time as we develop the mechanisms to interact with these people, and they understand their role, too.

And I would hasten to add to the explanation that Secretary Ridge, on several occasions now, and in his most recent pronouncement, has noted the importance of an aware and involved citizenry who begins to pass this kind of information to local authorities, and then local authorities pass it to State and Federal authorities. And in a digital, interactive environment, when the information gets into the digital system, unless we, by some policy or procedural mechanism limit it, it will appear everywhere.

It will appear kind of, sort of, let's call it ubiquitously, throughout the digital interactive system, and that's, I think, our goal. That's what we would like, so that everyone has this information, knows about the problem or the issue and then follows up on it or acts on it according to their own responsibilities.

Mr. PUTNAM. Very good. Thank you very much.

Again, I apologize for the fact that we were an hour late beginning. I want to thank all three of you gentlemen for the work that you do and for the time that you have taken to prepare for this hearing and joining us today. Your information was very helpful, and we will be following up with you in a closed-door session to pursue some of the other lines that we were unable to pursue in this environment. So thank you very much.

The subcommittee will stand in recess for a couple of moments while we set up the second panel.

[Recess.]

Mr. PUTNAM. The subcommittee will reconvene.

If our second panel of witnesses will please rise for the administration of the oath.

[Witnesses sworn.]

Mr. PUTNAM. I would note for the record that all of the witnesses responded in the affirmative. We will move immediately to their testimony.

Our first witness is Mr. Gerard Lynch. Mr. Lynch serves as chairman of the Regional Information Security Systems Center Directors Association and is currently the executive director of the Middle Atlantic Great Lakes Organized Crime Law Enforcement Network. Formerly, Mr. Lynch served as counsel to the New Jersey State Commission of Investigation where he was in charge of the Organized Crime Unit for the State of New Jersey. While serving as counsel, Mr. Lynch helped create and organize the MAGLOCLEN Concept, later serving as the association's secretary, vice chairman and chairman. During his tenure with the commission, Mr. Lynch worked on the infiltration of organized crime in the casino, construction, trucking and boxing industries.

You are a busy man.

Mr. GERARD LYNCH. Yes, sir.

Mr. PUTNAM. Welcome to the subcommittee. You are recognized for 5 minutes.

STATEMENTS OF GERARD LYNCH, CHAIRMAN, REGIONAL INFORMATION SECURITY SYSTEMS POLICY BOARD; MARK ZADRA, CHIEF OF INVESTIGATIONS, FLORIDA DEPARTMENT OF LAW ENFORCEMENT; AND SUZANNE PECK, CHIEF TECHNOLOGY OFFICER, GOVERNMENT OF THE DISTRICT OF COLUMBIA

Mr. GERARD LYNCH. Thank you, Mr. Chairman. Mr. Chairman, it is indeed a pleasure to testify before this subcommittee. I am going to try to lead my 5 minutes——

Mr. PUTNAM. Please pull the mic a little built closer to you so our reporter can be sure to pick it up.

Mr. GERARD LYNCH. OK, I'm sorry. I am going to lead it into how technology developed into the information sharing that we know today as the RISSNET. In the early 1970's, through the early 1980's, the way we shared information—and that's what the RISS system is all about—was through the telephone line. We would share information, talk to one another. The information would then be relayed back to the inquiring officer. If need be, we would telephonically contact each one of the six RISS centers across the country.

Subsequent to that, we decided to seek approval from the Federal Government to give us the ability to electronically connect our systems together, and that became the RISSNET I system, and subsequent to that the RISSNET II system, where, when an agency then calls us up, we didn't have to call the other RISS centers; we would just do it over a wide area of network. It worked very well, but it was still behind the times.

Shortly thereafter, we had a meeting in Baltimore, Maryland, where we discussed how we could possibly use the internet for technology exchange, and that's where we really blossomed into the system that we now know as the RISSNET system. The RISS system is comprised of about 7,000 law enforcement agencies on the RISSNET system. We have approximately 70,000 individuals that can use the system and use it well.

The RISSNET provides secure connectivity and electronic access to law enforcement SBU information, encrypted e-mail, electronic collaboration and data bases known as RISSINTEL, successfully to all of the law enforcement agencies, criminal justice agencies, from the Federal, State and local and tribal agencies.

We operate a current state-of-the-art technical capabilities and systems architecture that allows member agencies to interact electronically in a secure environment.

We, the system and the architecture that we developed, was adopted and endorsed by the National Criminal Intelligence Sharing Plan, which was created not too long ago. When we decided to hook up the system, we were very successful, and then we started to look at other partners in order to avoid duplication.

We were approached by the High Intensity Drug Trafficking Area Centers across the country, known as the HIDTAs, and their main goal was to see if they could talk to each other electronically, which they didn't have the ability to do at that point.

Since RISS had at that point the only national communication system around the country, they approached us. And in order to avoid duplication and to save money, all of the HIDTA systems partnered with the RISS systems, and they are now today seamlessly working on the RISSNET systems. And each one of the HIDTA centers are connected. There are 16 node centers on as well as all 32 HIDTA centers around the country.

And that's a partnership that has been working exceptionally well since its inception. Besides the 16 HIDTAs, we have 15 State law enforcement systems that have also hooked onto our system. And what we have done is basically started creating nodes, and a node is a system-to-system communication.

In order to enable that to work out, we had to develop using the current technology, XML technology, which would allow system A to talk to system B. So, for instance, if you are going to hook up the Colorado State Police with the RISS system, we created this XML translator that allows the Colorado system to transfer information over the RISS system that's being requested by someone maybe down in Florida. So it has been working and working out well. And we were the first law enforcement entity to use the XML technology, and we used it very well.

We are also have 16 HIDTAs that are hooked up. We have 93 U.S. Attorney's offices around the country that are hooked up, the Criminal Division of Department of Justice, the EPIC Crime Lab Seizure System, law enforcement intelligence units across the country, the National White Collar Crime Center, The National Drug Pointer Index Center, the National Telecommunications System or NLETS, and the National Drug Intelligence Center.

We are also in talks with the Postal Services, Postal Inspection Services, and with the Department of Defense ADNET, with the Open Source Network of CIA and also the Department of State's OpenNet Plus system, and these systems are coming on, as we speak, very, very rapidly.

We also developed the RISS ATIX system to talk to the first-responder communities, the Governors across the State, the mayors, then the various critical infrastructures. And we have roughly 47,000 users of the RISS ATIX system, and we have RISS ATIX online. We can go into more and more of that, but we are very pleased with what the RISS system has developed to date.

[The prepared statement of Mr. Lynch follows:]

Testimony Submitted by

The Regional Information Sharing Systems (RISS) Program

Before the

Subcommittee on Technology, Information Policy,
Intergovernmental Relations, and the Census

Of the Government Reform Committee

Submitted by

Gerard P. Lynch, Esq., Executive Director

Middle Atlantic – Great Lakes Organized Crime
Law Enforcement Network (MAGLOCLEN)

Chairman of the RISS Directors Association

On Behalf of the

Regional Information Sharing Systems (RISS) Program

The events of September 11, 2001, changed much of the historical attitude about sharing data among agencies and across levels of government. Law enforcement and other public safety officials recognize the need for interagency cooperation and coordination in sharing information among local, state, federal, and tribal agencies. The effective coordination and sharing of law enforcement intelligence has proven to be the best method to combat the increasing criminal activity and is paramount to successful counterterrorism and public safety operations.

The Regional Information Sharing Systems (RISS) Program is a nationwide communications and information sharing network that serves nearly 7,000 local, state, federal, and tribal law enforcement member agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England. In operation for approximately 25 years through U.S. Department of Justice funding, RISS serves as a force multiplier in fighting increased violent criminal activity by terrorists, drug traffickers, sophisticated cyber criminals, street gangs, and emerging criminal groups that require interagency cooperation. The RISS centers provide support services to facilitate law enforcement investigative and prosecution efforts in combating multijurisdictional criminal activity. The six regional intelligence centers operate in exclusive, multistate geographic regions. This regional orientation allows each center to offer support services that are tailored to the investigative and prosecution needs of member agencies, though the centers also provide services and products that are national in scope and significance. The RISS centers fill law enforcement's need for rapid but controlled sharing of information and intelligence pertaining to known or suspected terrorists, drug traffickers, and other criminals.

The RISS Program provides secure connectivity and electronic access to law enforcement sensitive but unclassified (SBU) information, encrypted e-mail, electronic collaboration, and databases of criminal intelligence information to more than 75,000 law enforcement and criminal justice professionals from nearly 7,000 member agencies. RISS is operating current state-of-the-art technical capabilities and systems architecture that allow local, state, federal, and tribal law enforcement member agencies to interact electronically with one another in a secure environment. Using a secure Web-based nationwide network known as RISSNET, law enforcement users connect to all RISS criminal intelligence databases and resources 24 hours a day, 7 days a week. RISSNET is a proven, highly effective communications and information sharing system that improves the quality of criminal intelligence information available to law enforcement officers to make key decisions at critical points in their investigation. In addition, the technical architecture adopted by RISS requires proper authorization to access information, but also provides flexibility in the levels of electronic access assigned to individual users based on security and need-to-know issues. This type system and architecture are endorsed by the *National Criminal Intelligence Sharing Plan.*

RISS has expanded its user base by electronically connecting existing state and federal agency information sharing systems to RISSNET to share and expand intelligence capabilities. Currently, 15 state law enforcement systems and 16 High Intensity Drug Trafficking Areas (HIDTA) network systems are electronically connected as nodes to RISSNET. The Executive Office for United States Attorneys has connected staff to RISSNET at each of the 93 U.S. Attorneys' Offices' Anti-Terrorism Task Forces throughout the U.S. Staffs at the U.S. Department of Justice, Criminal Division, have connected to RISSNET. RISS and the El Paso Intelligence Center (EPIC) officials entered into a partnership and have electronically connected EPIC as a node to RISSNET, to capture clandestine laboratory seizure data from RISS state and local law enforcement member agencies. Other systems connected to RISSNET include the Law Enforcement Intelligence Unit, the National Drug Pointer Index, the National White Collar Crime Center, the National Law Enforcement Telecommunication System, and the Criminal Information Sharing Alliance, formerly the Southwest Border States Anti-Drug Information System. The United States Postal Inspection Service is currently pending connection to RISSNET as a node. The National Drug Intelligence Center uses the RISS network as a communications mechanism for publishing counterdrug intelligence products to federal, state, local, and tribal law enforcement members. RISSNET is in the process of achieving connectivity to the intelligence community's Open Source Information System (100,000 users) and the U.S. Department of Defense Information Systems Agency's ADNET-U system (5,000 users), and anticipates connectivity with the U.S. Department of State's OpenNet Plus system (43,500 users worldwide). Other state systems and HIDTAs are currently in various stages of connection as nodes to RISSNET. The integration of the above-mentioned state, regional, and federal agencies and systems with the RISSNET secure nationwide communications backbone has increased the sharing of criminal intelligence, alerts, and homeland security information within their own agencies and among the other agencies. RISS uses current Extensible Markup Language (XML) technology to assist state law enforcement agencies in electronically connecting their state criminal intelligence databases to RISSNET for access by all RISS member agencies.

The RISS system and the FBI Law Enforcement Online (LEO) system interconnected as a "virtual single system" in 2002 for distribution of SBU homeland security information to authorized users of both LEO and RISS. The value of this interconnection was recognized in 2003 by the *National Criminal Intelligence Sharing Plan*, which is sponsored by the U.S. Department of Justice. The Plan designates the RISS/LEO interconnection as the initial SBU communications backbone for implementation of a nationwide criminal intelligence sharing capability. This nationwide SBU communications backbone supports fully functional, bidirectional information sharing capabilities that leverage existing local, state, tribal, regional, and federal infrastructure investments. The Plan recommends that interoperability of existing systems with the RISS/LEO communications capability proceed immediately to leverage information sharing systems and expand intelligence sharing. The International Association of Chiefs of Police, the U.S. Attorney General, and other federal agency administrators endorse the Plan and have adopted it as a national model for all law enforcement agencies, organizations, and associations. RISS officials are working to implement the Plan recommendations within current budgetary restraints. Due to the interest of many law enforcement agency systems to electronically connect to the RISS/LEO backbone, RISS is testing a security architecture solution to allow users with various types of security credentials to connect and traverse RISSNET to share information and access resources without being required to use the RISS-specific security credentials.

In addition, RISS has recognized that the need for the exchange of information extends beyond law enforcement and the RISS/LEO virtual single system. During 2003, RISS implemented a service available over RISSNET to link law enforcement with the public safety and first responder agencies involved in securing our nation from terrorism. This service is known as the RISS Anti-Terrorism Information Exchange, or RISS ATIX, and includes a secure ATIX Web site, secure ATIX bulletin board, ATIXLive, and secure e-mail. ATIXLive is an online, real-time, collaborative communications information sharing tool for exchange of information by law enforcement and other first responders. The operation of RISS ATIX provides first responders and critical infrastructure personnel with a secure means via RISSNET to communicate, share information, and receive terrorist threat information, including that provided by the U.S. Department of Homeland Security. Through this capability, users can post timely threat information, view and respond to messages posted by government, police, fire, emergency, and infrastructure security personnel, and collaborate with law enforcement partners. These additional groups of users include public service, public safety, emergency management, utility, and other critical infrastructure personnel that have traditionally not been served by RISS. Currently, more than 47,000 RISS law enforcement members and other public safety participants have access to RISS ATIX services.

Even in its first year of connectivity, ATIX is already proving to be a prized, flexible law enforcement and first responder tool. The team in charge of G8 Summit security and communications this summer, which included the FBI, the U.S. Secret Service, the Georgia Bureau of Investigation, the Georgia Office of Homeland Security, and the Georgia Information Sharing and Analysis Group, selected RISS ATIX as their official system for secure communication and information sharing during the summit. RISS ATIX has also been asked to assist at both the Republican and Democratic national conventions. Amtrak is using the system to request that ATIX participants send reports of suspicious activity around their trains and report to Amtrak and local law enforcement officials. Amtrak has posted accompanying precautions and indicators of suspicious activity on ATIX. Local emergency management services were able to take advantage of the ATIX link to the National Hurricane Center during Hurricane Isabel to track the storm and issue up-to-date warnings and alerts. Water and electric companies have expressed appreciation for the timely, credible information now being shared over ATIX. The Director of Security and Safety of a water utilities company in Newark, Delaware, specifically praised ATIX as a "one-stop shop" for local, regional, and national intelligence data which can be obtained on a daily basis, as well as a source of vital security information that he either could not find previously or which required querying a number of sites.

RISS has also developed and deployed other law enforcement investigative resources available over RISSNET to include RISSLinks, RISSLeads, and RISSLive. RISSLinks is a data visualization tool that instantly creates a link analysis chart of search results from the RISS criminal intelligence databases. Through the click of a button, visual data is provided that instantly displays associations of the suspects that were not previously known and provides the contact information for other agencies that are working the same suspects. This saves valuable law enforcement resources. RISSLeads is a collaborative bulletin board for all types of criminal activity, including terrorism. RISSLive is an online, real-time communications forum which provides RISS law enforcement members the ability to ask questions and receive answers to specific crime topics of interest or for members involved in an operational event requiring an online, real-time communications capability.

The Bureau of Justice Assistance administers the RISS Program and has established guidelines for the provision of services to member agencies. The RISS regional intelligence centers are subject to oversight, monitoring, and auditing by the U.S. Congress; the General Accounting

Office, a federally funded program evaluation office; the U.S. Department of Justice, Bureau of Justice Assistance; and state and local governmental units. The RISS center criminal intelligence databases comply with federal regulation 28 CFR Part 23 (Criminal Intelligence Systems Operating Policies). The 28 CFR Part 23 regulation emphasizes adherence to individual constitutional and privacy rights and places stricter controls on the RISS intelligence sharing function than those placed on most local, state, or federal agencies. RISS supports and has fully operated in compliance with 28 CFR Part 23 since inception. RISS firmly recognizes the need to ensure that individuals' constitutional rights, civil liberties, civil rights, and privacy interests are protected throughout the intelligence process. In this regard, RISS officials recently adopted a RISS Privacy Policy to further strengthen their commitment and support of 28 CFR Part 23 and the protection of individual privacy rights.

RISS continues to provide solutions to the need for enhanced information sharing capabilities between local, state, federal, and tribal law enforcement agencies and homeland security partners. This effort to increase cross-agency and intergovernmental collaboration is demonstrated through the RISS promotion and participation in many initiatives and partnerships to electronically connect additional, existing agency systems as nodes on RISSNET for secure communication and information sharing nationwide. By connecting states and other information sharing systems to the existing RISSNET backbone, rather than funding the build-out of infrastructure for each stand-alone information system, millions of dollars can be saved, and millions of data records can be easily and quickly available to local, state, federal, and tribal law enforcement at little or no cost to the user.

Thank you for this opportunity to provide the subcommittee with this testimony.

THE REGIONAL INFORMATION SHARING SYSTEMS

In addition to RISS technology services, the following are traditional services implemented and maintained by each RISS center to facilitate information sharing and member agency investigation and prosecution efforts:

1. Analysis Services Component: Each center operates an analytical component to assist participating agencies in the compilation, interpretation, and presentation of case investigative and prosecution information provided to the center. This component responds to participating agency requests for analysis of investigative data and data needed for prosecution.

2. Investigative Support Component: Each center operates an investigative support component by providing financial assistance to participating agencies for their conduct of multijurisdictional investigations. Financial resources may include funds for the purchase of information, contraband that may be used as evidence, services, investigative travel and per diem, and overtime compensation. Funds expended and activities conducted under this component must directly support the operation of the information sharing and analytical components.

3. Specialized Equipment Component: Each center maintains a pool of special investigative equipment for loan to participating agencies. The loan of such equipment must directly support the operation of the information sharing and analytical components.

4. Technical Assistance Component: Each center maintains a component to provide technical assistance to member agencies. Through use of center personnel and others in participating agencies, consultation, advice, and information may be made available to member agencies concerning use of specialized equipment; investigative procedures; accounting of center funds, if provided by the center in support of investigations; and information analysis. This component will emphasize use of technical resources among the centers as necessary and available. Technical assistance in the form of active participation by center personnel in member agency investigations is prohibited.

5. Training Component: Each center maintains a training component to upgrade investigative skills of personnel from participating agencies. Such training assistance may consist of financial support to send personnel to training courses, seminars, and conferences or, more commonly, the design and delivery of special training courses by center staff. Training provided under this component must support the center goals and objectives.

To further enhance the coordination and exchange of information among member law enforcement agencies, the centers have initiated additional support service activities, including distribution of criminal activity publications/digests and sponsorship of membership information sharing conferences.

RISSNET RESOURCES

RISS operates the only secure Web-based nationwide network (RISSNET) for communication and exchange of criminal intelligence.

RISSNET gives law enforcement member agencies secure Web browser access to:

- RISS Investigative Leads Bulletin Board (RISSLeads): special emphasis on terrorism information and alerts
- RISS Criminal Intelligence Databases (RISSIntel)
- RISS National Gang Database (RISSGang)
- Secure e-mail
- RISSTraining: emphasis on electronic delivery of anti-terrorism training
- RISSSearch
- RISS criminal activity publications
- RISS training calendars
- Investigative equipment information
- Member contact directories
- State, federal, and regional systems and resources electronically connected
- RISS ATIX: Terrorist threat resources for first responders and law enforcement
- RISSLinks
- RISSLive
- ATIXLive

THE REGIONAL INFORMATION SHARING SYSTEMS (RISS) REGIONAL INTELLIGENCE CENTERS

The Office of Justice Programs' Regional Information Sharing Systems (RISS) Program is a federally funded program comprised of six regional intelligence centers. The six RISS centers provide criminal information exchange and other related operational support services to local, state, federal, and tribal law enforcement agencies located in all 50 states, the District of Columbia, U.S. territories, Canada, Australia, and England. These centers are:

Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN) serving Delaware, District of Columbia, Indiana, Maryland, Michigan, Pennsylvania, Ohio, New Jersey, and New York, as well as Australia, Canada, and England
Phone: 800-345-1322
E-mail: info@magloclen.riss.net

Mid-States Organized Crime Information Center (MOCIC) serving Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin, as well as Canada
Phone: 800-846-6242
E-mail: info@mocic.riss.net

New England State Police Information Network (NESPIN) serving Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont, as well as Canada
Phone: 800-343-5682
E-mail: info@nespin.riss.net

Regional Organized Crime Information Center (ROCIC) serving Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, and West Virginia, as well as Puerto Rico and the U.S. Virgin Islands
Phone: 800-238-7985
E-mail: info@rocic.riss.net

Rocky Mountain Information Network (RMIN) serving Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming, as well as Canada
Phone: 800-821-0640
E-mail: info@rmin.riss.net

Western States Information Network (WSIN) serving Alaska, California, Hawaii, Oregon, and Washington, as well as Canada, Guam, and Australia
Phone: 800-952-5258
E-mail: info@wsin.riss.net

Mr. PUTNAM. Thank you very much. I appreciate your testimony and for your recognition of the clock. We will put all of your testimony in the record and get to the rest of it in questions.

Mr. GERARD LYNCH. Thank you.

Mr. PUTNAM. Our second witness is Mr. Mark Zadra. Is that correct?

Mr. ZADRA. Zadra.

Mr. PUTNAM. Zadra.

Mr. PUTNAM. I am sorry, Mr. Mark Zadra.

Mr. Zadra currently serves as chief of investigations for the Florida Department of Law Enforcement Office of Statewide Intelligence. In this role, Chief Zadra provides oversight for investigations, intelligence and business functions. This includes oversight of automated intelligence systems, the Counter Terrorism Intelligence Center, Financial Crime Analysis Center, Computer Crime Center, Investigative Intelligence Support and Publications.

Chief Zadra provides administrative oversight of Florida's effort in the implementation of the MATRIX project. He also chairs the State of Florida Data Integration Committee, which functions to insure data interoperability and efficiency in data collection maintenance, analysis and dissemination. In addition, he insures coordination and consistency of intelligence components of Florida's seven Regional Domestic Security Task Forces.

Welcome to the subcommittee. You are recognized.

Mr. ZADRA. Thank you, Chairman Putnam, and the staff and for the opportunity to speak with you today about some of Florida's efforts in conjunction with our local, State and Federal partners in information sharing across our State and Nation.

Following September 11th and the horrific events of that day, it soon became quite apparent that local law enforcement in the State had a role in ensuring security in our Nation. State law enforcement representatives began meeting from all over the country to talk about how we could share the right types of information necessary to do that.

Resulting from those discussions were the development of the MATRIX project, which stands for Multistate Anti-Terrorism Information Exchange. This project is to increase and enhance the exchange of terrorism and other criminal activity information among local, State and Federal agencies. The project is funded by two Federal grants, and it currently involves five States—Connecticut, Florida, Michigan, Ohio and Pennsylvania—four States, I would note, which are represented by members of your subcommittee. There are other agencies that are, States that are continuing to involve in discussions regarding joining.

The funding was used to purchase hardware, software, communication support, to make each State a member of RISS, through a RISS node, also develop secure Web sites and for data integration efforts.

There are three main objectives of the MATRIX project. One is connectivity. The other is Web-based access to data intelligence, and the third is factual data analysis. On the connectivity side, as Mr. Lynch had indicated, the RISSNET is used by all the MATRIX participants for all their secure connectivity. And it's graphically displayed there, the six RISS centers.

Florida is a node directly to that. The importance to that is that the Criminal Justice Network within the State of Florida is a trusted, secure intranet which connects all of Florida's criminal justice agencies, over 1,000 of those. It provides e-mail services in a secure environment, the ability to have interagency files and image transfers and, as importantly, it allows access to all different types of applications that local agencies and State agencies make available over the CJNet. And some of those are displayed on the materials that have been provided to you.

The second objective, as I mentioned, was Web-based access. And in that, we have, within each State, the desire is to be a secure Web site, and that would leverage existing systems that are already built. There's been too much time, money and effort placed into putting in systems; those do not need to be duplicated.

You will see in the next slide, the Office of Statewide Intelligence, Florida Department of Law Enforcement. We do have a secure Web site, which allows us to provide law enforcement sensitive information to all of our local, State and Federal partners in the State of Florida.

And regarding the first panel and the ability to push information, you will see, in the middle of that, the daily brief. That's something that we do every day. We provide a daily brief to all of our partners, including the Homeland Security Operation Center, about what is going on this day in Florida.

The third objective was factual data analysis, and that is the ability to take information, which we discovered as a result of a specific investigation of September 11, where the data aggregators have commercially, public-available information. We discovered, when that can be dynamically linked with data that States collect and maintain—and those are drivers license and digital images, motor vehicle information, criminal history, sexual offender information, Department of Corrections, that when you combine that data, you can take what would be disparate data and make it very meaningful for law enforcement purposes.

You will see displayed in the next slide, there is actual screen shots from the FACTS program, and it shows that we can produce information regarding subjects who are the subjects of criminal investigations, their relationships can be shown between individuals of that criminal organization as well as photo lineups and thosetype of things. The system has numerous security considerations in place.

The MATRIX board, which may represent each State and oversees the activities of the MATRIX participant, they, as well, address the privacy concerns.

And you will see graphically displayed there information that when each member signs on to the system, it again acknowledges again the purpose they are there and the guidelines that they are to operate under. It also requests the need to identify a case number and the type of activity that is being examined.

The searches that are done within the FACTS application—drivers license, vehicles, corporations, telephone directory assistance, property, deed, assessments, those types of things—it is used to investigate domestic security concerns as well as other types of domestic criminal activity.

I would like to point out, too, the project has had a lot of misconceptions that have been attached to it. I would like to highlight just one or two of those. Primarily, the FACTS application does not do predictive analysis. It does not track or monitor individuals. It does not collect the types of information that I believe our citizens would be concerned about, such as their health records, where it is that they shop, their credit information and thosetype of things.

Simply put, FACTS, within the MATRIX project, was designed simply to allow law enforcement investigators to work more efficiently, pulling information that they have always had access to, legally, and it's not unlike an internet search engine that you use to conduct internet searches. It is a tool; it is not a substitute for investigative work.

Thank you, Mr. Chairman, for the opportunity to address you.

[The prepared statement of Mr. Zadra follows:]

STATEMENT

OF

MARK A. ZADRA

Chief of Investigations
Office of Statewide Intelligence
Florida Department of Law Enforcement

REGARDING A HEARING ON

Facilitating an Enhanced Information Sharing Network That Links Law Enforcement and Homeland Security for Federal, State and Local Law Governments

BEFORE THE

CONGRESS OF THE UNITED STATES
HOUSE OF REPRESENTATIVES

COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL

RELATIONS AND THE CENSUS

July 13, 2004
2:00 PM
Room 2154 Rayburn House Office Building

Good afternoon, Chairman Putnam and distinguished Members of the Subcommittee. My name is Mark Zadra, and I am a 26-year member of the Florida Department of Law Enforcement (FDLE). I serve in a leadership capacity as Chief of Investigations within the Office of Statewide Intelligence.

FDLE is a statewide law enforcement agency that offers a wide range of investigative, technical and informational services to criminal justice agencies through its seven Regional Operations Centers, fifteen Field Offices, and seven Crime Laboratories. Its primary mission is to promote public safety and strengthen domestic security by providing services in partnership with local, state, and federal criminal justice agencies to prevent, investigate, and solve crimes while protecting Florida's citizens and visitors. FDLE utilizes an investigative strategy that comprises five primary focus areas including Domestic Security, Violent Crime, Major Drugs, Economic Crimes and Public Integrity. FDLE's Criminal Justice Information Program provides criminal identification screening services to criminal justice agencies, non-criminal justice agencies, and private citizens to identify persons with criminal warrants, arrests, and convictions. FDLE further meets the information needs of Florida's criminal justice community by providing network services including computer hardware, software programming, telecommunication costs and computer technology necessary to maintain and share information.

The Office of Statewide Intelligence's mission is to provide FDLE and other Florida law enforcement leadership with the sufficient amount and types of information to make informed decisions regarding the deployment of their investigative resources. This is accomplished primarily by conducting and disseminating crime assessments. OSI is also instrumental in the development and maintenance of investigative automation both for FDLE and the Florida criminal justice community. In support of these roles OSI operates the Florida Computer Crime Center, the Counter Terrorism Intelligence Center, the Financial Crimes Analysis Center and the Dissemination and Special Projects Unit.

The Multistate Anti-Terrorism Information Exchange (MATRIX) and the Florida Criminal Justice Network (CJNet)

FDLE has for many years been a major leader and facilitator of information and intelligence sharing primarily within the State of Florida. In the wake of September 11, 2001 however, this role took on more of a national perspective as it was quickly evident that information sharing could no longer be considered effective on merely a local or regional basis. Following the horrific events of that day, a group of state law enforcement executives from throughout the United States began meeting to discuss domestic security problems and challenges, and to develop proposed solutions to increase information and intelligence sharing throughout all levels of law enforcement. With FDLE helping to lead the effort a multistate coalition of state law enforcement agencies emerged. The successes achieved and the information sharing lessons learned became the genesis for the idea behind the Multistate Anti-Terrorism Information Exchange (MATRIX) pilot project.

MATRIX is a pilot, proof-of-concept project initiated in response to the increased need for timely information sharing and exchange of terrorism and other related criminal information among members of the law enforcement community. The MATRIX project is a means that will help ensure that local and state law enforcement officers have timely, accurate, and effective information. The MATRIX project has three primary objectives:

1. Establish connectivity utilizing the existing Regional Information Sharing System (RISS) Network.
2. Secure web-based access to intelligence data and information sources contained in the participating states' intelligence systems with the objective to connect to federal systems where permitted.
3. Use data analysis and integration technology to improve the usefulness of the data contained in multiple types of record storage systems.

MATRIX is consistent with the policies and implementation guidelines detailed within the adopted National Criminal Intelligence Sharing Plan. This plan, developed at the urging of the International Association of Chiefs of Police's (IACP) by the Department of Justice's Global Justice Information Sharing Initiative, outlines specific "action steps" that can be taken immediately by almost any agency and what can be expected by performing those steps. The plan provides an in-depth discussion of the issues that hinder intelligence sharing and should serve as a guideline for any information sharing initiative.

The first objective of the MATRIX Project, connectivity, has been met through the utilization of an existing secure law enforcement communication backbone, the Regional Information Sharing System's (RISS) secure intranet known as RISSNet. This system is used by several law enforcement systems to facilitate information sharing within a secure environment.

The second objective, to provide secure web-based access to intelligence data and information sources, continues to evolve. For instance, in Florida, the Office of Statewide Intelligence maintains a secure intelligence website which previously was made available only to law enforcement within our state via Florida's secured Criminal Justice Network (CJNet). Now this secure website is available to other MATRIX participants over RISSNet. The Office of Statewide Intelligence also maintains the state's legislatively mandated Domestic Security and Counter Terrorism Database, known as ThreatNet, whereby local, state, and federal law enforcement agencies within Florida can report suspected terrorism activity and provide domestic security related intelligence. ThreatNet is accessed by all authorized participants via the CJNet.

Within Florida, CJNet serves as the infrastructure for statewide criminal justice information systems by providing secured connectivity that is limited to criminal justice agencies. This closed network or "intranet" connects approximately 700 Florida criminal justice sites at the local, state, and federal levels.

In addition to connectivity, CJNet provides electronic mail, transfer of data files and photographs, and access to various databases that are crucial or useful to the criminal justice community. Because of Florida's MATRIX participation and connectivity to RISS, the capability to access Florida's numerous CJNet applications and intelligence databases is now available to other participating states.

The third objective, factual data analysis, is being met through a very innovative and effective computer application. This application, known as the Factual Analysis Criminal Threat Solution (FACTS), provides law enforcement a technological investigative tool that allows query-based searches of state maintained and commercially available public records that are legally available to law enforcement.

State maintained and commercially available public databases have long been a source of valuable information to law enforcement investigations. The ability through FACTS to integrate state data sources such as driver license records, digital images, criminal history information, corrections data and sexual offender data, in conjunction with commercially available public data such as published telephone subscriber and property ownership records has exponentially increased its investigative value. This information can be used to help locate subjects of a criminal investigation saving countless investigative hours and significantly improving the opportunity for a successful investigative resolution. FACTS allows law enforcement officers and intelligence analysts to utilize their time more effectively and efficiently by concentrating on leads that have a greater potential for investigative relevancy. They can utilize known investigative information, however limited, and develop potential leads in seconds, versus traditional and manually intensive efforts which can take days, weeks, or months. Timeliness is crucial in life or death situations, especially when law enforcement is addressing investigations involving weapons of mass destruction, violent crime or abduction.

It is important to note that FACTS only contains information already available to law enforcement from commercially available public records and state-owned data. The application simply provides a single point of access to information, not unlike what Internet users do when they type in a query on an Internet search engine. The FACTS database contains information which, upon query, is dynamically combined from selected commercially available public information and information provided from participating states which resides on servers secured and controlled by FDLE (serving as the State Security Agent on behalf of the MATRIX Board). There are no intelligence records contained within the FACTS application.

Authorized law enforcement users are able to perform searches of the following data sets and obtain related information such as names, addresses, dates and numbers which all are, under applicable state or federal law, available to law enforcement without subpoena or court order.

- Person
- Driver License
- Motor Vehicle/Vessel
- Telephone Directory Assistance
- Company
- Criminal History
- Department of Corrections
- Sexual Offender
- Uniform Commercial Code
- Property Deed
- Property Assessment
- Civil Court including Bankruptcy
- Government Published Watch Lists
- Professional License
- Federal Aviation Administration Certifications and Aircraft ownership

FACTS does NOT contain:

- Telemarketing calling lists
- Direct mail mailing lists
- Airline reservations or travel records
- Frequent flyer/hotel stay program membership or activity
- Magazine subscriptions lists or reading lists
- Telephone calling logs or records
- Credit card or debit numbers or credit history information
- Purchases (e.g., retail store, Internet, or even gas stations)
- Mortgage or car payments
- Bank account numbers or account balances
- The costs of a home addition
- Birth certificates
- Marriage licenses
- Divorce decrees
- Utility bill payments (i.e., gas, electric, phone, heating oil, cable or satellite TV)
- Medical Records
- Fingerprints

The MATRIX Board, comprised of a law enforcement policy maker from each participating state, sets all policy for MATRIX participation and the use of the FACTS application. Security agreements between the states govern who can access the system and security of the information once it is retrieved from the system. By policy, access is granted only to law enforcement agency personnel who have been approved through their employing agency and properly screened with a state and national fingerprint-based background check. Each participating agency and individual user must complete an agreement and then be properly trained in system use including security and privacy considerations.

As also established by policy, any MATRIX computer application, including FACTS, can only be used for legitimate law enforcement investigative purposes. A legitimate law enforcement investigative purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation or to prevent a criminal act. The information obtained from any MATRIX application cannot be sold, published, or disclosed for commercial purposes. The FACTS application has no ability to monitor, track or surveil anyone. It is not similar to the Terrorist Information Awareness (a defunct federal program), nor is it a "data mining" program that sifts through information and then automatically suggests possible criminal activity or matches individuals to "profiles." The database is investigator-driven. Queries must be made by investigators or analysts to prompt responses. They utilize a "submit" button and not a "solve" button. Time honored investigative "shoe leather" and savvy are not replaced, but augmented. FACTS simply provides access to information in a centralized fashion that is already available to investigators at individual sites today. Each investigator still has to develop his or her investigative basis for a search or other enforcement action and is to independently verify data before relying upon it for arrests, searches or other significant enforcement action.

There are numerous protections and safeguards in place to ensure that the MATRIX system or its associated applications such as FACTS are not misused.

These include:

- Agency and user agreements that define system use
- The requirement for fingerprint based background checks on all users approved by participating agencies
- Project oversight and policy guidance (including a Privacy Policy) by the MATRIX Board
- Connectivity through a secured Regional Information Sharing System Network
- Use of encrypted tokens, user names and passwords for all users
- Sign on requirements that require the user to acknowledge use is for law enforcement purposes only and is in compliance with all established security and privacy considerations
- The requirement that users must verify data with originator prior to any official law enforcement action
- System Firewalls at numerous points of the secure network
- Logging of all user activity
- Maintenance of a system audit log for automated system dissemination. Each agency must maintain a secondary audit log of "secondary" disseminations to authorized agency staff
- Random and periodic audits of system use to identify potential misuse (misuse results in denial of further use of FACTS, discipline by the user's employing agency, and/or criminal prosecution)

FDLE at the request of the MATRIX Board serves as the MATRIX State Security Agent with members co-located on-site at the vendor's facility. MATRIX data is maintained on separate servers in an FDLE-controlled server room which is separately and securely isolated from the rest of the facility. FDLE has conducted a physical security audit/assessment of the housing facility including computer system and networking integrity. FDLE has also conducted backgrounds investigations on all vendor employees directly involved in MATRIX project

The Florida Legislature closely reviewed the MATRIX project and the FACTS application prior to authorizing Florida's participation. During March 2003, members of the Senate Homeland Defense, Public Security, and Ports Committee and the House Coordinating Committee on Public Security viewed this system firsthand at FDLE and were confident in the system's intent, purposes, and internal limitations to prevent abuse. It is believed that these efforts during the project's initiation phase contributed significantly to a better understanding of the project, and eliminated confusion and any misperceptions about the project.

The MATRIX project has helped law enforcement officers in Florida and the other participating states to quickly and more easily obtain the information needed to investigate terrorist threats and other criminal activity. While the FACTS tool was initially developed in response to counter-terrorism investigations, it quickly became established as a tool to significantly impact investigations of all types of criminal activity. There are numerous success stories associated with FACTS use. FACTS has assisted in solving homicides, cracking "cold cases," busting fraud rings, identifying drivers of vehicles involved in hit and run, and pinpointing participants in drug investigations. FACTS has been used in identifying and locating subjects involved in investigations and even witnesses for the prosecution phase of cases. It has further been used to identify associates of case targets and vehicles involved in criminal activity. Many consider FACTS to be a success each and every time it is utilized when considering due to nothing other than the amount of time saved by investigators and analysts pursuing investigative leads.

Having timely access to complete information not only assists investigators in taking enforcement actions against suspects, it also helps protect innocent persons and helps prevent enforcement actions taken on the basis of incomplete or out-of-date information. In this regard, FACTS helps protect persons against unwarranted police intervention.

There are many misconceptions surrounding the MATRIX program that have been publicized through various sources. The following comments are offered to help clear up any inaccuracies that have emerged regarding the project, particularly with respect to the FACTS application.

- MATRIX is controlled by the participating states and not a vendor.
- The vendor is not permitted to access law enforcement data provided by the states to the Florida Department of Law Enforcement (FDLE) other than in its supporting role to MATRIX.
- FACTS is not a substitute for the now defunct Total/Terrorism Information Awareness (TIA) Project and there is no relationship to that system. Instead, it is a query/response based information source for use by trained and screened civilian law enforcement as a part of an active criminal investigation.
- The MATRIX FACTS application is not an intelligence database nor does it contain intelligence information.
- The MATRIX FACTS application only contains information already accessible to law enforcement from commercially available public records and state-owned data.
- The MATRIX FACTS application does not track or monitor individuals.
- The MATRIX FACTS application does not contain magazine subscription lists, reading lists, telephone calling records, bank transactions, lists of credit cards or credit card transactions, and; therefore, such data is not provided by MATRIX to law enforcement. Under federal law, when such data is required in law enforcement investigations, it can only be obtained under a judicial order; i.e., subpoena.
- The MATRIX FACTS application does not perform "data mining" to produce unprompted information based on established profiles

In summary, MATRIX is a project that helps assure that state and local law enforcement officers—those most likely to come into contact with criminals or terrorists in our communities—will have timely, accurate and effective information. We must have the capacity to respond quickly to developing events to combat terror. As criminal enterprises are making use of computers and technology to assist their criminal activities law enforcement must avail itself of 21st century tools to combat 21st century threats. The MATRIX project expansion is paramount to equip law enforcement analysts and investigators with information and intelligence exchange capabilities consistent with the technology advancements integrated and woven into the fabric of our modern day society.

Florida's Data Integration Efforts

Many have identified the lack of information sharing as a contributing factor to our country's inability to prevent some of the terrorist attacks in America, most notably those that occurred on September 11, 2001. In response, numerous new information sharing systems and projects continue to emerge at the national, state, and local levels. These systems can generally be categorized as systems for communication (situational awareness), criminal intelligence gathering, data retrieval, and geographical and spatial data analysis. Florida is no exception as there are at least six (6) major "data fusion or data integration" projects in various stages of development and implementation, including the MATRIX Project.

While each of these information and/or intelligence exchange efforts are laudable, it is paramount that these projects do not become individual "information silos" incapable of integrating with or being interoperable with one another. For that reason, Florida created a Data Integration Committee comprised of members of the various projects and inclusive of all seven of its regions. This committee is in the process of developing a statewide strategy for intelligence and information sharing. Among the issues being considered within the strategy are the following:

- Oversight
- Funding
- Content of Data Sharing
- Participants
- System Architecture
- Integration and Sharing with Federal Agencies
- Security

- Data Standards
- Audits
- Risk Mitigation Strategy/Misuse Consequence
- Agency and User Agreements
- Privacy Policy

The National Criminal Intelligence Sharing Plan

The National Criminal Intelligence Sharing Plan outlines how collaboration could be achieved on a national level. Recommendation 2 of the Plan calls for the creation of a Criminal Intelligence Coordinating Council to advise Congress, the U.S. Attorney General, and the Secretary of the Homeland Security on the best use of criminal intelligence for which interoperability is certainly intertwined.

Recommendation 20 of the Plan encourages all law enforcement agencies to utilize an automated, incident-based criminal records tracking capability, in addition to traditional case management and intelligence systems, to use as an additional source for records management and statistical data.

Recommendation 21 of the Plan identifies the interconnected RISS/LEO (RISSNet and the FBI's Law Enforcement Online) systems as the "initial sensitive but unclassified secure communications backbone for implementation of a nationwide criminal intelligence sharing capability. This nationwide sensitive but unclassified communications backbone shall support fully functional, bi-directional information sharing capabilities that **maximize the reuse of existing local, state, tribal, regional, and federal infrastructure investments (emphasis added).** Further configuration of the nationwide sensitive but unclassified communications capability will continue to evolve in conjunction with industry and the development of additional standards, and the connection of other existing sensitive but unclassified networks."

Recommendation 22 of the Plan identifies interoperability with existing systems at the local, state, tribal, regional, and federal levels with the RISS/LEO communications capability as an immediate priority in order to leverage information sharing systems and expand intelligence sharing.

Closing

Around the nation, tremendous amounts of time, money and effort have been expended in attempts to gather information through the creation of databases. The time has come to shift the focus of effort, technology and funding to connecting what has already been established. Florida supports full implementation of the National Criminal Intelligence Sharing Plan.

Chairman Putnam and Members of the Sub Committee, thank you for the opportunity to have appeared and testified before you today. I can assure you the State of Florida is encouraged by the Sub Committee's interest in facilitating an enhanced information sharing network across the nation. It is our hope that this testimony, and the understanding of Florida's efforts at ensuring a secure and effective network for information and intelligence sharing, will be helpful in your endeavor.

Mr. PUTNAM. Thank you very much.

Sorry, Ms. Peck. We saved the best for last.

Ms. PECK. You did indeed.

Mr. PUTNAM. Our third witness on the panel is Ms. Suzanne Peck. She is chief technology officer for the District of Columbia. Prior to her appointment, she served as the senior technology and operations executive for several Fortune 500 companies. Ms. Peck is a recognized expert in the conception and implementation of large-scale technology operations.

Her decade-long service as senior vice president, chief information officer of the Student Loan Marketing Association of Sallie Mae helped transform the $46 billion corporation into one of the Nation's largest wholesale credit providers.

More recently, Ms. Peck was senior vice president of CoreStates Financial Corp. and chief executive officer of its $50 million technology startup subsidiary,

Welcome to the subcommittee. You are recognized for 5 minutes.

Ms. PECK. Thank you.

Good afternoon, Mr. Chairman. I am the District of Columbia's chief technology officer, leading the Office of the Chief Technology Officer, the central information technology and telecommunications agency of the District of Columbia Government. I am pleased to testify today on the District's leadership efforts in developing an enhanced information-sharing network that links law enforcement and homeland security for multi-jurisdictional use.

In the District, we have developed an integrated suite of information-sharing programs for local, regional and Federal public safety and domestic preparedness. This suite focuses on the exchange, transportation, presentation and coordination of important public safety and emergency preparedness data. And we are building this enhanced information-sharing network to be fully interoperable among District agencies, Federal agencies and regional and national municipalities.

In the area of data exchange, we are building a public safety and criminal justice data sharing system that easily integrates this data using only open-standard components which can be easily and quickly replicated by other jurisdictions. This initiative is underway under the name of SHIELD, Securing the Homeland By Integrating Existing Local Data bases.

SHIELD currently shares data among 14 District and Federal public safety criminal justice and court agencies and also shares this data with similar agencies in New York City, Pennsylvania, Maryland and Virginia. SHIELD provides access to available, unrestricted public safety and justice data through an interoperability partnership of independent city, State and regional information systems.

Through secure internet access, SHIELD allows justice and homeland security officials across the region and the Nation to share incident information and to perform comprehensive public safety analyses in real time and to respond more rapidly with better-informed decisions in first-responder and terrorist situations.

In the area of data transport, we are implementing broadband networks over which we are prepared to drive SHIELD shared-information data, both regionally and nationally.

One network we are supporting uses the internet as the broadband transport network. We're implementing secure internet connections, using existing components, such as browsers, ISP connections and commerciallyavailable authentication tokens.

Another network we are supporting is a pilot broadband public safety network in the 700 megahertz band that allows us to transport real-time video-streaming data from first responder incident sites to central command centers.

A third transport initiative we are underwriting is the District's leadership of the Spectrum Coalition, a national coalition of cities, States and counties formed to advocate for national legislation that would permanently allocate spectrum in the 700 megahertz band to public safety so that States and cities throughout the United States would have sufficient reserved spectrum to support vital public safety wireless applications.

A fourth key data network effort in which we are participating is the Capital Wireless Integrated Network, or CapWIN, a partnership among Maryland, Virginia and the District to develop an integrated transportation and criminal justice information wireless network.

In the area of data presentation, we are enhancing the uses and usefulness of the justice and emergency preparedness data we share and transport to municipal and Federal colleagues by presenting that data in innovative ways. The District's DCSTAT system provides both nearly daily and real time capabilities to collect, organize, report, and map data for use by local, regional and Federal agencies in the national capital region and, by extension, the Nation. DCSTAT will enable local and Federal agency executives and program managers to merge spatial data, that is map data, with traditional public safety data to better predict and manage public safety emergencies in a geographic mapped context.

In the area of data coordination, it's critical to effective homeland defense that first-responder and emergency management agencies coordinate data planning and deployment. Our Unified Communications Center, UCC, a 127,000-square-foot building on the East Campus of St. Elizabeths Hospital in Ward 8, will consolidate, when opened in early 2006, District emergency communications and traffic management functions and our 911 emergency, 311 non-emergency, and 727–1000 citizen service call centers.

But, in addition, the UCC will play a very key homeland defense role, serving as the Regional Incident Command and Control Communications Center [RICCC], for the 17 major jurisdictions in the national capital area. The RICCC will facilitate communication and coordination among local, State and Federal authorities for effective and timely response to regional and national emergencies.

In summary, the initiatives I have just spoken about address the public safety, criminal justice and homeland security data sharing, transportation, presentation and coordination needs that are critical and urgent for the Nation's capital and for the Nation. We have designed our programs from inception to serve not only the District but national homeland defense as well. Each of the elements of the District's enhanced information-sharing network can be easily expanded to local, State, regional and Federal agencies to meet homeland defense needs on a national scale.

And we look forward and, in fact, are already working with DHS and our county, State, regional and national partners in achieving this.

Thank you, Mr. Chairman.

[The prepared statement of Ms. Peck follows:]

GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE CHIEF TECHNOLOGY OFFICER

Testimony of

Suzanne J. Peck
Chief Technology Officer
Office of the Chief Technology Officer

Before the U.S. House of Representatives, Committee on Government Refoim, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Oversight Hearing on "Facilitating an Enhanced Information Sharing Network That Links Law Enforcement and Homeland Security for Federal, State and Local Governments"

Tuesday, July 13, 2004
2:00 p.m.
Rayburn House Office Building
Room 2154

STATEMENT OF SUZANNE PECK, CHIEF TECHNOLOGY OFFICER, DISTRICT OF COLUMBIA GOVERNMENT BEFORE THE SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS, OF THE GOVERNMENTAL REFORM COMMITTEE, UNITED STATES HOUSE OF REPRESENTATIVES ON FACILITATING AN ENHANCED INFORMATION SHARING NETWORK THAT LINKS LAW ENFORCEMENT AND HOMELAND SECURITY FOR FEDERAL, STATE AND LOCAL GOVERNMENTS

SUMMARY

Good afternoon, Mr. Chairman and members of the Subcommittee. My name is Suzanne Peck. I am the District of Columbia's Chief Technology Officer, leading the Office of the Chief Technology Officer (OCTO), the central information technology and telecommunications agency of the District of Columbia government. I'm pleased to testify today on the District's leadership efforts in developing an enhanced information sharing network that links law enforcement and homeland security for multi-jurisdictional use. We've developed an integrated suite of District information sharing programs for local, regional, and federal public safety and domestic preparedness that focus on exchange, transportation, presentation, and coordination of this important public safety data. And we're building this enhanced information sharing network suite to be fully interoperable among District agencies, federal agencies, and regional and nationwide municipalities.

In the area of **data exchange,** we're building a public safety and criminal justice data sharing system that easily integrates this data using only open-standard components which can be easily and quickly replicated by other jurisdictions. This initiative is underway under the name SHIELD (Securing the Homeland by Integrating Existing Local Databases). SHIELD currently shares data among 14 District and federal public safety, criminal justice, and court agencies, and also shares this data with similar agencies in New York City, Pennsylvania, Maryland, and Virginia. The mission of SHIELD is to provide access to available, unrestricted public safety and justice data through a partnership of independent city, state, and regional information systems. Through secure access, SHIELD allows justice and homeland security officials across the region and nation to share incident information and to perform comprehensive public safety analyses in real time and to respond more rapidly with better informed decisions in first responder and terrorist situations.

In the area of **data transport,** we're building broadband networks over which we're prepared to drive SHIELD shared information data, both regionally and nationally. One network we're supporting uses the Internet as the broadband transport network, implementing secure Internet connections using existing components such as browsers, ISP connections, and commercially available authentication tokens. Another network we're supporting is a pilot broadband public safety network in the 700 mHz band that allows us to transport real-time video streaming data from first responder incident sites to central command centers. A third data transport initiative we're underwriting is the District's leadership of the "Spectrum Coalition," a national coalition of states, cities, and counties formed to advocate for national legislation that would permanently allocate spectrum in the 700 MHz band to public safety so that states and cities throughout the U.S. would have sufficient reserved spectrum to support vital public safety wireless applications. A fourth key data network effort in which we're participating is the Capital Wireless Integrated Network (CapWIN) project, a partnership among Maryland, Virginia, and the District to develop an integrated transportation and criminal justice information wireless network.

In the area of **data presentation,** we're enhancing the uses, and usefulness, of the data we share and transport to municipal and federal colleagues by presenting it in innovative ways. The District's DCSTAT system provides both daily and near real-time capabilities to collect, organize, report, and map data for use by local, regional, and federal agencies in the National Capital Region (NCR) and, by extension, the nation. DCSTAT enables agency executives and program managers to merge spatial data (e.g. map data) with traditional public safety data to better predict and manage public safety and emergencies in a geographic, mapped context.

In the area of **data coordination,** it's critical to effective homeland defense that first responder and emergency management agencies coordinate data, planning, and deployment. Our Unified Communications Center (UCC), a 127,000-square-foot building on the East Campus of St. Elizabeths Hospital in Ward 8, will consolidate, when opened in early 2006, emergency communications and traffic management functions, and our 911 emergency, 311 non-emergency, and 727-1000 citizen service call centers. In addition, the UCC will play a key homeland defense role, serving as the Regional Incident Communication and Command Center (RICCC) for the 17 major jurisdictions of the National Capital Area. The RICCC will facilitate communication and coordination among local, state and federal authorities for effective and timely response to regional and national emergencies.

In summary, the initiatives I've just spoken about address the public safety and criminal justice data sharing, transportation, presentation, and coordination needs that are critical and urgent for the nation's capital, and for the nation. We've designed these programs from inception to serve not only the District, but national homeland defense as well. Each of the elements of the District's enhanced information sharing network can be easily expanded to local, state, regional, and federal agencies to meet homeland defense needs on a national scale, and we look forward to working with DHS and our other county, state, regional, and national partners in achieving this.

Mr. PUTNAM. Thank you, Ms. Peck.

I want to thank all of you for being here today and, in particular, for being here so long here today. We were an hour late starting, and you have been very patient, and fortunately, I am hopeful that we will be able to complete this without being interrupted by votes.

But the award, I guess, for your resilience is that you get the last word.

So my first question to each of you is to comment on what you heard in panel one and give us some sense if things are going well, not so well, and how you evaluate their observations from the Federal level on information sharing to prevent future terrorist acts, and where there may be some differences from your perspective at the State and local level.

So, Mr. Lynch, I will let you begin.

Mr. GERARD LYNCH. Thank you, Mr. Chairman.

I did listen very intently to the gentleman from the FBI as well as Homeland Security, and what they are saying, there is truth to it, although it was sometimes a little more difficult to get the information that we thought we would be getting sooner.

But, with regard to the FBI, just before September 11, we were in discussions with the FBI about marrying their system, the LEO system, with the RISS system so that we could have the Federal entities also hooked up with the State and local entities systemwide, not individualized.

And since September 11, that became a reality. We are still modifying it. We are still perfecting the relationship with the FBI and the LEO system, and we are very confident that's going to continue. We are getting the bulletins from the FBI that are needed to share among the 7,000 law enforcement agencies that I previously testified about, and we are getting them on a regular basis.

We are also working very intently with the Department of Homeland Security. As a matter of fact, just yesterday, we had a meeting with the IAIP section of the Homeland Security to see if we could get some more seamless cooperation between the two entities. And we seem to be on that road, and the road, I think, is going to be leading to more and more cooperation and more and more sharing of information.

In fact, on Monday, I have another meeting with the Department of Homeland Security, and the purpose of that is to work out ways that we can share information, use the systems that are out there, the existing systems, and get the information to the entire community.

As you know, since RISS system has already developed RISS ATIX, we have been there for several years. Homeland Security is now getting into that field. And what we want to do is, once they are in it, we want to marry those two systems up. And we are in those discussions to make that occur.

So we are cautiously optimistic that things are improving, and will continue to improve in the future.

Mr. PUTNAM. Mr. Zadra.

Mr. ZADRA. Mr. Chairman, I believe that you would be pleased to hear from the State standpoint that things are greatly improved, as each of the gentlemen indicated.

Probably would not be so pleased to hear, as was also indicated, that we are not there yet with everything that needs to be done. From the State's perspective, it's our belief and representative of our local agencies, that what we need the Federal Government to do is to help bring all of these systems together. As you can see, they have sprung up all across the Nation. There were existing systems before.

What we don't need is to go to a desktop and have to go check 120 different systems from across the country to connect those puzzle pieces.

What we need to do is to have the Federal Government, hopefully through the—was mentioned through the National Intelligence Criminal Sharing Plan, they indicated in their Criminal Intelligence Coordinating Council, which would be made up of representatives of the right organizations, to help us as a country come together, and so that we can take and integrate all of the existing systems, to leverage what we have and not take all of this funding that is going forward to the States and to the locals to build, again, disparate silos of information. So there is a lot of work that really needs to be done, and we would hope that the Federal Government would help with that.

Also, I think it's critical that what we need the Federal Government to do, and all of the agencies that were represented here today, is we don't need to query their data bases. We need information pushed to us. We should not be where we have to make individual phone calls to all of them. So that information that TTIC is analyzing, it needs to be disseminated, and it's currently, how it's structure is now that it goes to the Federal Bureau of Investigation, which goes to their Joint Terrorism Task Forces or, first, to the intelligence center and then to the respective Joint Terrorism Task Force.

Within Florida, we have seven regional district domestic task forces that have liaisons with each of the two JTFFs, and in fact, in two of our regions, they are co-located with them. So we depend a lot on Homeland Security for situation awareness. As there are events unfolding in Florida, we make notification to their command center. Likewise, they make notice to us and, through Jay Reeves, as incidents that are occuring, issues of concern across the country. On the intelligence side, we depend a lot on the intelligence coming from—internationally coupled with the domestic—from other areas of the country to funnel us from the FBI, in addition to the information and intelligence mechanisms from the Department of Homeland Security.

Mr. PUTNAM. Ms. Peck.

Ms. PECK. The District of Columbia is in the unique position, not only of being the Nation's capital, but of being the single municipality in the Nation which is a city, a county and a State. So the perspective I bring is of all three of those. And our perspective is that, finally, all terrorism is local.

DHS, I think, is doing an extraordinary job at the Federal and national level, and the system that we bring to the party is a system that we have implemented for ourselves to make sure that all of our local public safety, criminal justice and court information is shared within the District; 14 criminal public safety and court entities in the District are now sharing their data for the first time ever in the history of the District.

That system can be replicated through using commercially available components, in every municipality in the United States, and the funding for that replication can be taken from local funding. If, theoretically, every individual municipality in the State created only just their own local information-sharing system, and brought that system to a national consortium, all they would need, in addition to that system, is a browser capability, an ISP, a secure ISP connection, and some authentication token so that integration would be the only additional expense to making all local information in the major municipalities in the United States available.

What the District of Columbia is doing and believes very strongly in is that system, where we don't create monolithic new systems and structures of communications but take locally funded information-sharing systems in municipalities across the Nation, connect via commercial, secure internet connections and have data available in any kind of emergency preparedness or terrorist incident where any combination of city, States, counties across the Nation can converse with each other, local data availability.

DHS then adds the component that each of these systems, local information systems, can also connect, as the gentleman from the FBI told you earlier, with NWCCC, with NCIC, with LEO, with HSIN, with all of the DHS systems and the Federal systems.

But a system of local data-sharing across the United States does not have to be invented and implemented whole cloth. It already exists. We are proving that and have proved it in the District and have taken that system, already regionally, to the September 11 municipalities, to New York City, to Virginia, to Maryland and to Pennsylvania and have piloted data exchange of local information among all of those elements.

Our next step in this system, in showing that every jurisdiction could build the system very quickly, and for very little marginal cost, is to do what the first panel—you queried the first panel about notification and alerts. The very next thing we are putting into place is that system, so that system, nationwide, of notifications on alerts would exist at a local level, and we are also going to the next production pilot. What we are doing is to connect the entire eastern seaboard and have them exchange information. From the Eastern Seaboard, it's just one easy step to the Nation.

So the systems that we have built really are a pilot to show how to have local data available in any permutation and combination, available between and among localities across the Nation and available to DHS.

So we look at DHS as the Federal information consortium, and we are looking at local municipalities and connecting local municipalities.

Mr. PUTNAM. It sounds like what you just said, please correct me if I am wrong, is that if DHS would just get out of the way, you would have this thing done in a year or two?

Ms. PECK. Local, there—no, what I am saying is, our focuses are different. The focus of DHS is Federal, national information. Our focus is in working with them, and we are working closely with them on these initiatives. And our focus is to have—when I say local information, DHS is not currently focusing on having local mug shots, local fingerprints, local criminal records, local incarceration records at a very, very detailed level. Those are the kinds of things we say, when terrorism occurs, are kinds of information you are very likely to need as well.

And so we are, as I look at us, DHS's partner in helping get that information into the bundle without extraordinary expense, from scrap expense.

We have simply shown how you can have all of that information made available at very little incremental cost; only integration is the incremental cost.

Mr. PUTNAM. Mr. Zadra, MATRIX, a very innovative program that you have brought up to speed in Florida, does DHS have access to that, or do they have to go through you?

Mr. ZADRA. We are still awaiting a final policy decision from DHS. We have members of DHS, such as the Immigration, Customs, Enforcement representatives, within this State of Florida who are assigned to our Domestic Security Task Forces. They have access to the FACTS application, the MATRIX project.

One complicating factor, Mr. Chairman, since this is under a pilot project and is funded by Federal grants, the information that's been provided to us is that Federal agencies, therefore, cannot benefit from the Federal funds for the position that it possibly could be supplanting congressional funding. That's a policy decision that's still being waited on.

Within Florida, however, the Federal partners to our task forces, the State of Florida, our State legislature authorized additional funding for us to purchase additional licenses, if you will, for use by the task force members, and, therefore, we can provide those licenses to our Federal partners and not be in conflict with, perhaps, that policy decision.

Mr. PUTNAM. Have you had an opportunity, post September 11, to take this thing out for a spin and really see how it works in a real live threat situation? Has there been an operation where there was either a threat or a situation that required you to really exercise the system that has grown up since September 11?

Mr. ZADRA. Respect to FACTS, sir?

Mr. PUTNAM. Yes.

Mr. ZADRA. Yes, sir. Let me say that FACTS is utilized by the regional domestic security task forces with the subject of concern relating to criminal organizations involved in, perhaps, terrorist activities. So it is used every day by them.

An actual incident that happened, that I was personally involved in, is we received a request from a Federal agency who had been advised that there were a certain number of individuals who were on their way to an airport within the State of Florida to bomb it. And they had partial descriptions of vehicles but no tag numbers. Some very suspicious circumstances regarding the individuals observed with those vehicles and the activities that they were involved in.

The request to the State of Florida was to provide for them, if you will, the universe of those type vehicles that are registered in the State of Florida.

Prior to being able to utilize FACTS, the ability to do that would have required an offline search through our Department of Motor Vehicles which, in the past, has taken 24 to 48 hours to do. Within less than 2 minutes, we provided a list of—and the numbers, our round numbers of approximately 80 of one vehicle and 70 of the other vehicle to them within 2 minutes.

The importance of that, however, is by dynamically combining the State-owned data, which is the vehicle registrants, the drivers licenses but, more importantly, the drivers license photographs, when that material was provided to the Federal agency, it had the list of all known vehicles that met that description within a 25-mile radius of where the incident was reported. It had the motor vehicle registration information, the address for each of those.

But, more importantly, it had the drivers license photographs for those registered owners. And the Federal agency could go to their witness, provide this and ask that witness, do you recognize any of the following as that? Now, compare minutes to what really would have taken weeks or, I should say, days if not weeks of a table full of analysts and agents sorting through stacks of computer printouts, only then to find a vehicle that may match the description. But then have to go make a separate query to identify the registered owner, make a second query to then identify the actual drivers license photograph associated with that.

Now, I will tell you that, in that particular circumstance that I just referenced, that it turned out to be a hoax, so you might ask me, why, Mr. Zadra, would you be discussing that as a success story? And I would say this, it's a success story from this standpoint, that every time it's used, it enhances the investigator's ability with respect to not only the hopeful successful conclusion of that investigative league, but timeliness is what's critical. And when you are talking about a weapons of mass destruction, it's the time, it's those minutes and seconds that count. So any time you utilize FACTS is a success story, in my personal view.

And the other thing is that, if you think about this particular circumstance, of the hours that were saved by not having that table full of analysts and agents pursuing leads relating to a hoax—this all—there are numerous success stories, Mr. Chairman, regarding all types of criminal activity. And if I could mention one more to give you an idea of how successful of a tool it is.

Within Florida, we had a 15-year-old female who was victimized by a sexual offender who was going around exposing himself to young females within the State. A call came from local law enforcement. And this one young female, there was an attempted actual abduction, so it went beyond just exposing himself to now attempted abduction. Fortunately, this young female was very heady, used good technique, was able to obtain a partial description of attack, observe the facial description of the individual and was able to escape from being abducted, provided that information to local law enforcement. The call to us was, "We have a partial tag. We have a color of a vehicle. That's all we know. Is there anything you can do?"

Within minutes, we provided a list of, because you can do what is referred to as a wildcard search within FACTS on a partial tag number. But, again, it brought back the registered owner of just a few vehicles now that met that within, again, a mile radius of that, where it was reported, and now, again, we had the photograph. It was shown to the victim, immediately identified the subject, and warrants were issued for its arrest. So that is how the system is used effectively in pursuit of not only terrorism investigations, which are certainly critical, but all types of criminal activity. What we had found was we developed a tool which obviously was brought about from the standpoint of and addressing counter terrorism efforts, but certainly, I don't think any of us would find, if we had a tool in our tool box that was multipurpose, that we would not utilize that tool for any other use.

Mr. PUTNAM. Well, that's interesting that you are so willing to disclose that your search took 2 minutes, and TTIC was reluctant to disclose how long theirs took. I suspect, if it was as efficient as 2 minutes, they might have been more willing to disclose it in open forum. I think that is a perfect example of technology being utilized in a nonintrusive way to keep people safe, either from the traditional bad guys and as well as the, the new terrorist threat that's even greater in this post September 11.

Are you satisfied with the level of coordination from the Federal level on these threats? And the example I would use is sort of a nontraditional example, but it's a big deal for Florida, and the example is the recent unrest and humanitarian crisis, actually, in Haiti, that for several days bordered on what could have been a massive migration to Florida. And in the middle of that, I can remember getting a briefing from the State Department on the preparations that were being made in anticipation of a refugee crisis.

And my first question was, "Are you, have you talked to Florida about this?" and they said, "Well, no, we haven't." Well, then I said, "You don't have a plan if you are not talking to the people who are about to be on the shores, receiving thousands of people who are going to be in need of medical treatment and food and shelter and clothing and all of these things." And it really sort of set off a red light that they still don't get it.

Are you satisfied with the level of coordination that exists on major, major efforts like that?

Mr. ZADRA. Mr. Chairman, I would say that I am encouraged to say I am completely satisfied, I do not think would be the case. There is room for improvement. Perhaps if it would make you feel better with respect to that Haitian situation, we were very well aware and were planning very diligently and were reaching out and we're involving our homeland security partners, the U.S. Coast Guard, the Maritime Intelligence Center out of south Florida.

Fortunately within the State of Florida, we were the first State to engage in a very innovative project where we actually have 35 of our regional domestic security task force members who are cross-trained and designated and have detention and arrest authority for immigration issues with respect to domestic security.

So we had in place not only with our local law enforcement, but also regional and domestic security task forces to have those representatives and members available to assist in that particular situation. We are continuing dialog and there is still a lot of work to be done to ensure that the State of Florida, particularly our local law enforcement, because as was mentioned, the issues always occur locally. So when you have boatloads of those that are migrating to our shores, they come to local jurisdictions as they pass through the international waters, obviously. But when they get to our shore, local law enforcement is the first to intervene. So we are working through and we are in the process of finalizing some training, which would be for those jurisdictions that line, particularly our south Florida coast line, where there would be specific individuals that would be trained and have the ability to do nothing else but to stop and detain and wait for the proper Federal law enforcement representatives to effectively deal with that situation.

Mr. PUTNAM. Perhaps Ms. Peck or Mr. Lynch could comment on what cyber security assurances are in place to protect the sensitive information that is being transferred between jurisdictions, whether it is between the States and the Federal Government or between States.

Mr. GERARD LYNCH. I think the cyber security issue is being addressed by the law enforcement communities that are members of the RISS system. And not only do we put on trainings for the law enforcement community about cyber crime and how cyber crime is affecting the lives of the average citizens, but we are also posting on not only RISSLEADS, or RISSLIVE bulletin board incidences of cyber crime identity theft. We are finding out that more and more of these State and local agencies are becoming aware of the effect that cyber crime has had on the relationships of the citizens of this country. And we really looked at it as part of a major crime, whether it is narcotics trafficking or gang activity. Cyber crime is just as important, just as debilitating and just as an effective means of the criminals to perpetrate crimes on the citizens of this country. So we are up to date on that. We are looking constantly to ways that we can combat it and we will continue that training of our law enforcement personnel throughout the country to ensure that cyber crime does, in fact, become an entity.

Mr. PUTNAM. In your organized crime work in New Jersey, had you ever come across an organized crime influence in cyber crime?

Mr. GERARD LYNCH. Such as identity theft?

Mr. PUTNAM. No. I would kind of lump, unfortunately, identity theft into the more traditional basket of crimes. But utilizing cyberspace perhaps to affect infrastructure, bring confusion or affect perhaps local response capabilities or things like that.

Mr. GERARD LYNCH. The traditional organized crime members were not involved in that. That was not even—I don't think I've seen any indications that the traditional organized crime was involved in cyber crime to the effect that they want to disrupt the Internet and do something to shut down the communications, such as the banking industry. What we are seeing and what RISS has done is we have basically made our system very secure, so that when they had that last attack on the cyber community, we were being banged almost 20 to 30,000 times an hour from Russia, from Belarus, from all the European countries, so it is a very severe thing.

And if the private community does not pick up on it and constantly stay on top of it, they will be shut down as Citibank was done during the last cyber crime attack. We are aware of it and the member agencies are aware of it and we are doing everything to educate and see to it that the criminal information is not affected by it. And I am sure that homeland security will be doing the same thing. It is a very serious issue that could face us in a very dangerous way down the road. But I see it more and more being protected as we protect our system.

Mr. PUTNAM. Sitting here listening to the different acronyms, MAGLOCLEN, RISS, MATRIX, FAX, CJNet, CRIMES, CLEAR, recognizing that it is always kind of a good thing to have your States or localities be the laboratories for innovation, have we reached the point that we are reinventing the wheel in different States? And is the technology mature enough that we really could be just replicating successful programs in other States instead of funding a bunch of new pilot programs?

Mr. GERARD LYNCH. There will always be regional interests for regional purposes that will be drafted, but we have been in constant contact with Members of Congress who appropriate funding for the RISS program or some similar programs. And what they have put in language now is language that would instruct those grant issuing agencies a directive that if they are going to be setting up any kind of a regional data base or regional telecommunications system that they use existing systems out there and they don't reinvent the wheel so that the existing systems can operate in a very effective manner. And that has been happening. Most of the technology that we have today can be developed so that it can marry most systems up.

When we decided to hook up the U.S. attorney's offices nationwide so that we could give them secure e-mail and encrypted translation of information back and forth, it was done because we developed a system that would allow that. And I think that what we are seeing here is that systems are being developed such as the RISS system that allow other systems to seamlessly, if not transfer information, but at least talk to one another and we are seeing that. We in MAGLOCLEN oppose constant duplication, because not only does it affect law enforcement when they want to talk to other agencies and the systems don't talk to each other, but also it costs money when you are developing new systems.

So when new systems are coming up and they are coming up—I don't think we can stop that—we want to make sure that if those systems come up, that they are compatible with the systems that are out there. And what I see in the future is that we are going to have a system of systems whether it's RISS system hooked up to the homeland security system, hooked up to RISS/LEO, there are many systems out there that will be able to communicate. Technology is not the issue. Policy is the issue.

Mr. PUTNAM. Ms. Peck.

Ms. PECK. I would absolutely concur with that. It is the position of DHS that they support a number of these State-based initiatives and that they follow these initiatives to the logical conclusion of the successful initiatives. So, you know, you plant your beans and you see which ones come up and which ones grow the highest and the best. So I think it makes a great deal of sense to support a number of State systems.

We all come to more or less the same conclusion so if you look at MATRIX's technology and SHIELD's technology, we come to a single place that says let's not build it from scratch. Let's use components that already exist. We have used exactly the same kinds of components. The only place I think in which we differ and we both come from a place that says it's the local data that needs to be integrated into the national DHS system. I think the only place that we disagree knowing what I know of MATRIX is knowing what kind of data is included and how that data is used. But in terms of the technology and recognizing that we need to build very cost sensitive systems from existing components and not ask the national government to attach all local data on their expense, we need to ask localities to do that.

We have come to exactly the same place. SHIELD's next focus is governments and national security and the security rules that will govern national data sharing and regional data sharing. So again, the technology can be easily replicated at very low costs and we need to have governance structures that say what kind of data, who is authorized to access that data and under what circumstances the data will be used and for what purposes, those kinds of governance, and the security rules as well in terms of the kinds of data and who has access to it. So it's those policy issues that are the things that we are looking at now and I am sure every other State-based system is looking at the same thing. The technology is the easy part, getting people to play together and to agree under which rules they play is much more focused now.

Mr. PUTNAM. Thank you very much. And before we bring this to a close, I want to give all of you the opportunity to have any final comments, it is the least we can do after this long afternoon. Ms. Peck, we will begin with you and end with Mr. Lynch and we will bring this subcommittee hearing to close. Any final thoughts?

Ms. PECK. I would like to thank you very much as chairman for the opportunity to highlight the leadership work that the District of Columbia has done in the area of local to national information sharing of public safety, criminal justice. Thank you very much for the opportunity.

Mr. PUTNAM. Chief.

Mr. ZADRA. Mr. Chairman, I thank you for the opportunity to be here today and I applaud the efforts of this subcommittee. It is the leadership. And we need, speaking from a State and local perspective on bringing all this together. I concur with both the last statements of Ms. Peck and Mr. Lynch in that the technology is not the problem. We have all the systems there that really what we need.

What we need to do is figure out how to connect them together. We need them not only regional strategies, we need a State strategy for each of our States so that each of the projects that they have within their major municipalities or sheriff's offices that they can bring those together from a State perspective, and as Mr. Lynch said, we will connect systems to other systems. I am 26-year member of the department of the law enforcement and been involved in criminal investigations for years. What I would like to see on my desk stop is instead of Mark Zadra having to query every police jurisdiction in the United States of America, I believe that we need a national index to where Mark Zadra could query a name and if nothing else, if it was just a pointer—because we are going to have to work through all of the security issues, policy issues, those are privacy issues that need to catch up to the technology, but we need, if nothing else, so I can connect those puzzle pieces.

When you go to a store now and you buy a puzzle, you come home and it has a picture on the box and it tells you how many puzzle pieces are in there and you know they're all in that box and you can put your puzzle together. Law enforcement's problem is that we don't have the picture. We don't even know how many pieces there are and our pieces don't come in a box but are spread across the country. So each of those jurisdictions may have that puzzle piece that we need. We shouldn't have to go individually and make phone calls in the way that we used to do business 10 years ago, including just most recently prior to September 11. What we really need to do is collapse all those tools on our desk. We don't need to be a multitasking disorder.

Having information is good, but what is important is making it meaningful to us and figure out whether that information fits that puzzle piece. What we would like to see and it needs, from the national perspective, and hopefully, this coordinating council can pull this off, but we need to be in a position that when I sit as investigator at my desktop, I need homeland security to be dealing with me and also me with them as to what is the situational awareness issues that are going on across our country as they are developing.

We need to know about them so that when something happens in another State, we in Florida can take that and apply the same protective and necessary protective measures to our critical infrastructure that is the issue. The other thing we need to do is we realize everyday there are individuals that come into contact with our criminal justice agencies as what talked about in SHIELD, that information is sitting out there and being collected already in systems that are already existing.

I need the ability to determine with a single query who and where have they come in contact with the criminal justice community, realizing that there are others that have a different type of job and that is intelligence. And intelligence really isn't intended to be shared at all levels with everyone in the criminal justice community or law enforcement. And this plan again speaks to that. We need the ability to hook up to those criminal intelligence systems as well.

So again, I thank you for your what you're doing with your subcommittee because I think that is the leadership we need is to pull all of this together, someone to put their hands around it and assist us. We have 40,000 law enforcement officers in the State of Florida who everyday have eyes and ears that are trained on domestic security issues and those things do happen locally. And we need to make sure that not only are we capturing it but we are sending that information and making available to others that have a need for that as well. So again, thank you, sir.

Mr. PUTNAM. Mr. Lynch.

Mr. GERARD LYNCH. Thank you, Mr. Chairman and thank the committee for bringing this to the forefront. I think that in the followup to the last statement, we are getting closer to that realm. If you saw where we were 2 years ago to where we are today, we are light years ahead of that, but yet we are still a long way from seeing total connectivity. What we have seen as we have seen with the RISS system is that our member agencies such as the Florida Department of Law Enforcement as well as New York City Police Department, are participating more and more because they are seeing a lot more advantages coming out of these systems out there.

And with our RISSLive and our RISS ATIXLive, we are seeing a lot more of the agencies starting to talk real-time to each other on key issues, whether it is a fire marshal talking to a fire marshal across the country or a police officer talking to a fire marshal across the country, we are seeing the communities of interest marry each other. And we are seeing a very fruitful end to all of this. We have ventured into the first responder community and we have seen a lot of positive feedback from the electrical critical events individuals to the railroad associations to the trucking industry. They are now working together to share information to shore up our homeland. And not only are the eyes and ears of the local police department alerted, but now we have the truck drivers, the electrical meter readers knowing more about what is going on in this country as far as security and posting threat information.

You know, the pilot program we have with the Department of Homeland Security on nuclear power plants is crucial that these pilot plans are developed and our country is much safer, when we see homeland security talking to the FEMA or the Federal management of each State and the local police departments and talking about suspicious activity around nuclear power plants.

So I see a lot more happening, but we still have a long way to go. And I think we have to make sure that the systems that are out there are funded properly and moved forward and that these connections such as the NODE activity and the NODE connection with the Florida Department of Law Enforcement can be spread throughout the entire country. And maybe this committee might be a spear head in moving that forward. Again, I thank you.

Mr. PUTNAM. Thank you very much. I want to thank all of our witnesses for your outstanding participation today. Your testimony is vital to helping us to better understand this issue and move toward solutions and better interoperability. Thank you for your patience and your willingness to wait us out. I want to thank the staff for pulling together an outstanding hearing, in particular one of our committee interns who we are losing, Kaitlin Jarling's last day and we appreciate the work that she has done on this hearing and a number of others this summer. In the event that there may be additional questions we did not have time for today, the record will remain open for 2 weeks for submitted questions and answers. Thank you all very much. Subcommittee stands adjourned.

[Whereupon, at 5:25 p.m., the subcommittee was adjourned.]

○