FIXING THE HOMELAND SECURITY INFORMATION NETWORK: FINDING THE WAY FORWARD FOR BETTER INFORMATION SHARING

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MAY 10, 2007

Serial No. 110–34

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE
48–909 PDF WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chair*

NORMAN D. DICKS, Washington
JAMES R. LANGEVIN, Rhode Island
CHRISTOPHER P. CARNEY, Pennsylvania
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DAVID G. REICHERT, Washington
CHRISTOPHER SHAYS, Connecticut
CHARLES W. DENT, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

THOMAS M. FINAN, *Director and Counsel*
BRANDON DECLET, *Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
DERON MCELROY, *Minority Senior Professional Staff Member*

CONTENTS

FIXING THE HOMELAND SECURITY INFORMATION NETWORK: FINDING THE WAY FORWARD FOR BETTER INFORMATION SHARING

Thursday, May 10, 2007

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

The subcommittee met, pursuant to call, at 10:13 a.m., in Room 311, Cannon House Office Building, Hon. Jane Harman [chairwoman of the subcommittee] presiding.

Present: Representatives Harman, Langevin, Carney, Perlmutter, and Shays.

Ms. HARMAN. [Presiding.] The hearing will come to order.

My apologies to my colleague, Mr. Shays, and our witnesses, but of course the Democratic Caucus was called at precisely the same time. As yet, I have not mastered the ability to be in two places at the same time; maybe soon.

The Homeland Security Information Network, or HSIN for short, was supposed to be the department's main pipeline for sharing unclassified information with state, local and tribal partners. More than 3 years later, we are far from the robust system that was promised. What we have instead is kind of a mess. What we need is an effective fix. Sadly, I am not very hopeful.

I have in my hand a one-page memo dated April 17, 2007, from Admiral Roger Rufe, the director of the department's Office of Operations Coordination, to the undersecretary of management, Paul Schneider. I am frankly perplexed by what Admiral Rufe had to say about the HSIN just several weeks ago. Although he concedes that the system has "grown without sufficient planning and program management" for years, the admiral defends it, saying that "the HSIN, for better or worse"—sounds like a marriage—"is tied to DHS missions and operations."

Is the HSIN–DHS relationship, as I just said, some kind of bad marriage that we are all just supposed to accept?

Perhaps sensing that the long knives are out, the admiral goes on to say that he "fully embraces the concept of making decisive strategic changes to the program," but he urges Mr. Schneider "to fully consider the unintended consequences of programmatic decisions, particularly as they impact DHS operations and missions."

I am afraid that the admiral's plea for patience and fear of unintended consequences could be undermined by the rest of his comments. He notes that the HSIN working group last fall found that "DHS has not clearly defined the purpose and scope of HSIN nor designated roles and responsibilities for strategy development and implementation through a formal policy mechanism."

The admiral agrees, adding that "we continue to struggle with the lack of aligned DHS policy and established business rules." If only it were that simple. From what GAO is telling us and what the DHS IG told us last year, HSIN's troubles go far deeper, to day one of the program.

We are joined this morning by a person who saw all this coming almost 5 years ago—or we will be joined; he is not here yet—our colleague Congressman Jim Langevin of Rhode Island. Jim started asking Tom Ridge back in 2002 about why the department didn't first talk to state and local officials to find out what information-sharing systems were already working.

Today, we are asking Jim's question again. Why did the department choose not to partner with those working information-sharing systems and avoid the mess it finds itself in now? I have a strong suspicion that turf had something to do with the department's decision to go its own way, even if it meant duplicating tried and true information-sharing systems in the process.

Ignoring the experience, expertise and requirements of state and locals is unfortunately a common thing these days. With all due respect to the well-meaning men and women who work at DHS, many do not know what state and local needs are. We find time and again everywhere we look that there is an absence of consultation at the front end, and then we end up with a mess at the back end. I suppose we shouldn't be surprised, then, that they didn't talk to the state and locals who were building an information network that would have worked.

The needs of end-users should have been the starting point, as they should be the starting point with intelligence products and a lot of other things that DHS is doing. Because DHS got it backwards, the HSIN problems were cooked in from the beginning.

What do we have to show for it? A flawed information system with core problems that have continued to fester. I note that the HSIN has the dubious distinction of being on both the OMB watch list for poorly planned IT projects and the OMB high-risk list for poorly performing IT projects. In fact, the HSIN is one of 20 out of 900 IT systems across the federal government that makes both lists. For the mathematicians out there, that means that HSIN is among the top two percent worst IT systems. Almost 6 years after the largest terrorist attack in our country, this is totally unacceptable.

So what do we do? First, we need an information-sharing system that gets buy-in from state and locals, that includes accurate, reliable and timely information, and helps them protect their communities. Second, we need an information-sharing system that complements existing systems that will work for decades, in some cases for more than 30 years. Third, we need an information-sharing system that not only helps safeguard the American people, but also operates within the bounds of the U.S. Constitution.

I look forward to hearing from our witnesses today about how to get there, what benchmarks we should be establishing so we can conduct rigorous oversight of the HSIN that is so plainly needed. Let me just conclude by saying this: It is no pleasure to sit up here and say these things. It makes me quite uncomfortable. I don't play "gotcha" and I don't want you to feel that that is what we are trying to do up here.

What we are trying to do up here is get it right. I think we have wasted a lot of time and resources and human talent in duplication because we don't effectively coordinate. So this subcommittee has said for a long time that we are going to start at the other end. We are going to talk to the users of information, find out what they need, find out if they have tools that work, and then on a vertical basis coming back from the end-point to Washington, we are going to make sure that Washington is providing those things and adopting processes that will keep our communities safe.

Only if we have really robust information sharing; only if we have a full understanding at the local level of what to look for and what to do, are we going to find the people in Cherry Hill, New Jersey, or pick a place of interest. I know you all want to do that, and I know you all want to get it right. So I am just telling you that is our intention.

The ranking member is not here, so I would like to ask Mr. Shays if he has some opening remarks.

Mr. SHAYS. Thank you, Madam Chairperson. I first want to say that this committee is very fortunate to have you chair the Subcommittee on Intelligence, Information, and Terrorism Risk Assessment, with your background on the Intelligence Committee. It is just really wonderful to have you chair this committee and to have this hearing.

I have a statement that I am going to read—it is Mr. Reichert's—and then I am going to be leaving. I do apologize for that, because I think this is a very important hearing.

Good morning. We meet today to examine the Homeland Security Information Network, or HSIN, the DHS information system network.

By virtually all accounts, HSIN was poorly planned and implemented by the department. There have been several reports by the DHS inspector general and the General Accountability Office to catalogue the failings of the HSIN program. A recent example includes the June 2006 inspector general report indicating that HSIN is not effectively supporting state and local information sharing.

Today, GAO is releasing a report with similar conclusions. We have also heard, though, that the situation with HSIN is improving. While this is good news, we must focus intently on how to move forward more quickly and make the federal information-sharing environment, including HSIN, a success. The story of HSIN is a story of the federal government trying to impose a one-size-fits-all approach on states and locals. It is no wonder that in many states and localities, it is not working.

In any homeland security endeavor, but especially in the realm of information sharing, DHS has need to get state and local buy-in and cooperation. A federal-first, top-down approach simply does

VerDate Nov 24 2008 10:59 Jun 24, 2009 Jkt 000000 PO 00000 Frm 00007 Fmt 6633 Sfmt 6633 H:\DOCS\110-HRGS\110-34\48909.TXT HSEC PsN: DIANE

not work in an environment where state and local law enforcement are America's first preventers.

It is also important to realize that DHS will never be able to please every state and locality across America. While there will never be 100 percent satisfaction, DHS needs to get the message loud and clear that Congress expects substantial progress in the relations with states and localities.

On our first panel, we especially want to hear from Mr. Parent on how DHS can improve its cooperation with state and local stakeholders. On the second panel, we expect to hear that in some states, the HSIN system duplicates ongoing efforts. In other states, it simply gathers dust.

We will also hear that HSIN is being used by some as an essential tool for information sharing. It is critical that DHS gets information sharing right and does so in a cooperative manner. It is a fundamental element of our homeland security and vital to protecting our nation.

That is the statement of our ranking member. I would also like to say that evidently he is not feeling very well, so that is part of the reason why he is not here today. So I thank you all.

Ms. HARMAN. I thank you, Mr. Shays. All compliments are welcome. Please stay here and offer more.

[Laughter.]

And to the ranking member, please send him our best wishes. I hope he will be feeling better.

I am told that we will be joined by other members. Unfortunately, this morning was a very hectic one for everyone, and they are on their way over. I especially hope that Mr. Langevin will be able to be here soon.

Let me welcome the first panel of witnesses.

A ha, right on time. Here is Mr. Perlmutter.

Let me welcome the first panel of witnesses, just in time for votes.

Our first witness, David Powner, is the director of information technology management issues for the GAO. Mr. Powner is responsible for a large segment of GAO's IT work, including systems development, IT investment management, health IT, and cyber-critical infrastructure protection and reviews. That is a mouthful.

Mr. Powner has led teams reviewing major IT modernization efforts at Cheyenne Mountain Air Force Station, the National Weather Service, the FAA, and the IRS. These reviews covered many IT areas, including software development and maturity, information security, and enterprise security.

His team's fine work on the HSIN is one of the reasons we are holding this hearing today. I would mention that we met with Mr. Powner just a couple of days ago and reviewed some aspects of this report. It is a very important report, and we thank you for it.

Our second witness, Donald Kennedy, is the executive director of the New England State Police Information Network, or NESPIN. NESPIN is one of the six regional information-sharing system risk centers that are funded through DOJ's Office of Justice programs in the Bureau of Justice Assistance. Mr. Kennedy is currently the vice chairman of the RISS National Directors Association.

Prior to being named executive director in 2006—wonderful; here he is just in time, a hero's welcome—he served as NESPIN's deputy director of field services. Mr. Kennedy is a retired captain from the Rhode Island State Police where he served for 24 years and has served in all bureaus and divisions within the state police.

We are very pleased you are here.

I want to welcome Mr. Langevin, because he is truly the godfather of this hearing and the issues that we are raising today.

Our third witness—and we put you in this order, Mr. Parent; I just want to explain that—is Wayne Parent, the deputy director of DHS's Office of Operations Coordination. Mr. Parent previously served as the director of current operations for the Border and Transportation Security Directorate within the department.

On the BTS operations staff, Mr. Parent was responsible for current operational issues including coordinating the execution of both interdepartmental and interagency operations plans. He supervised the BTS Watch Sector in the Homeland Security Operations Center and managed planning and exercise participation for BTS. He was also responsible for coordination of intelligence-sharing between DHS's Information Analysis and Infrastructure Protection Directorate and the agencies within the BTS Directorate.

The vote lights seem to have gone off, so I would like someone to tell me where we are with anticipated votes. If they are not happening immediately, I would like to go directly into testimony, and then hopefully we can get through your testimony and some member questions before we have to adjourn briefly for votes.

I thank you, and I will recognize our first witness.

STATEMENT OF DAVID POWNER, DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. POWNER. Madam Chair, members of the subcommittee, we appreciate the opportunity to testify on the Homeland Security Information Network.

HSIN is a communications application that is to serve as DHS's primary nationwide information-sharing tool for transmitting sensitive, but unclassified, information. HSIN's problems to date have been well publicized. DHS's IG reported last year that it does not effectively support state and local information sharing.

In addition, it is on the Office of Management and Budget's radar screen, having made both OMB's management watch list and high-risk list, meaning that according to the administration, HSIN is a poorly planned and poorly performing project.

This morning, as requested, I will summarize the results of a report that we recently completed at the request of Chairman Thompson that identified nearly a dozen homeland security networks within DHS that now cost over $300 million annually to develop, operate and maintain.

Specifically, I will address the lack of coordination between HSIN and the regional information sharing program, a key nationwide information-sharing initiative operated and maintained by state and local officials. I will also address key efforts needed to improve coordination and to avoid this problem from reoccurring.

First, DHS did not effectively coordinate HSIN and the RISS program. RISS officials met with DHS in late 2003 and early 2004 to demonstrate that their application could be used by DHS to share homeland security information. Communications stopped shortly after these meetings with no explanation. When we questioned why this communication stopped, we were told that DHS officials involved in these initial meetings are no longer with the department.

Instead of leveraging the existing RISS application, DHS developed its own. The reasons for this lack of coordination are several, and include DHS rushing into HSIN without understanding key state and local initiatives. Until DHS coordinates key information-sharing initiatives better, it faces the risk of ineffective information sharing associated with terrorist threats, vulnerabilities and warnings.

In addition, DHS is developing and deploying HSIN capabilities that duplicate those associated with the RISS program. Both programs target similar users. For example, both are used and marketed for use at state fusion centers. In addition, both offer similar community-based portals such as those associated with emergency management in our nation's critical infrastructure sectors.

DHS acknowledges the lack of coordination and several improvements efforts are under way. These include developing an integration strategy so that HSIN can work with other applications and networks; improving the content that HSIN provides; and forming multiple committees that are to define operational priorities for DHS users and advise DHS on how HSIN can better meet user needs.

These are positive steps that should help, but these efforts have either just begun or are in the early planning stages. For example, the membership of the committees mentioned are still being established. Further, implementation milestones for these improvements efforts have yet to be defined. In addition to these planned improvements, we recommended that that the department conduct an inventory of state and local information-sharing initiatives like RISS and assess opportunities for the HSIN program to improve information sharing and avoid duplication.

Addressing the HSIN coordination issues with state and local initiatives should be the immediate focus, but on a broader scale, DHS has many networks and associated systems that need to be coordinated to effectively share critical information and to avoid duplicative efforts. We made recommendations to address this larger coordination challenge and to ensure that these efforts are consistent with the information-sharing environment called for in the 2004 Intel Reform Act.

In summary, HSIN has many hurdles to overcome. It has been poorly managed and poorly coordinated. Although some overlap in our nation's initiatives is prudent to adequately protect the homeland, duplication is not and is a waste of taxpayers' dollars.

Moving forward, it is essential that DHS clearly define HSIN requirements with input from users; improve its content; strengthen its program management; and implement an integration strategy so that it can work with other applications. Otherwise, it will not be the key information-sharing network it is intended to be.

Madam Chair, this concludes my statement. I will be pleased to answer questions.

[The statement of Mr. Powner follows:]

PREPARED STATEMENT OF DAVID A. POWNER

Madame Chair and Members of the Subcommittee:

I appreciate the opportunity to be here today to discuss challenges facing the Department of Homeland Security (DHS) in coordinating efforts on its Homeland Security Information Network (HSIN) with state and local governments and other parties involved in the mission of keeping our nation secure. As you know, DHS is responsible for coordinating the federal government's homeland security communications with all levels of government—including state and local. In support of this mission, the department developed HSIN as part of its goal to establish an infrastructure for sharing homeland security information.[1] Besides HSIN, an Internet-based application, DHS also operates at least 11 other networks in support of its homeland security mission. The department reported that in fiscal years 2005 and 2006, these investments cost $611.8 million to develop, operate, and maintain.

As agreed, in my remarks today I will discuss the department's efforts to coordinate its development and use of HSIN with key state and local information-sharing initiatives. These remarks are based on our recent report on homeland security networks and applications.[2] That report focused on two key initiatives under the Regional Information Sharing Systems program. This nationwide program, operated and managed by state and local officials, provides services (including information sharing) to support law enforcement and criminal justice agencies. Its information-sharing efforts also include emergency responders and public safety officials.

In performing the work for the report, we analyzed descriptive data (e.g., type of network, estimated costs) on major networks and Internet-based systems identified by DHS as supporting its homeland security mission, including information sharing. We also reviewed documentation on HSIN and state and local initiatives; compared it against the requirements of the Homeland Security Act, federal guidance, and related best practices; and interviewed DHS officials and state and local officials. This work was performed in accordance with generally accepted government auditing standards.

Results in Brief

In developing HSIN, DHS did not effectively coordinate with key state and local initiatives that are part of the Regional Information Sharing Systems program. Specifically, the department did not fully develop joint strategies and coordinated policies, procedures, and other means to operate across agency boundaries and meet mutual needs, which are key practices for effective coordination and collaboration and are a means to enhance information sharing and avoid duplication of effort. For example, DHS did not engage the program in ongoing dialogue to determine how resources could be leveraged to meet mutual needs or work through technical issues and differences in what each organization considers to be terrorism information.

A major factor contributing to the limited coordination was that after September 11, 2001, the department expedited its schedule for deploying HSIN. In its haste, it did not develop a comprehensive inventory of key state and local information-sharing initiatives.

Consequently, DHS faces the risk that effective information sharing is not occurring. It also faces the risk that the HSIN system may be duplicating state and local capabilities. Specifically, both HSIN and one of the key initiatives target similar user groups, such as emergency management agencies, and all have similar features, such as Web portals,[3] electronic bulletin boards, "chat" tools, and document libraries.

The department has efforts planned and under way to improve coordination and collaboration. For example, it is forming an HSIN Mission Coordinating Committee and an HSIN Advisory Committee to help ensure that HSIN meets the information-sharing needs of DHS and other users. However, these activities have either just

[1] The Homeland Security Act of 2002 directed DHS to establish communications to share homeland security information with federal agencies, state and local governments, and other specified groups.

[2] GAO, *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated wth Key State and Local Information Sharing Initiatives,* GAO–07–455 (Washington, D.C.: Apr. 16, 2007).

[3] A Web portal is generally a site that offers several resources or services, such as search engines, news articles, forums, and other tools.

begun or are being planned, with implementation milestones yet to be defined. In addition to the planned improvements, DHS has agreed to implement our recommendations to take steps to ensure that HSIN is effectively coordinated with key state and local government information-sharing initiatives, which include identifying and inventorying such initiatives. We also recommended that DHS determine whether there are coordination and duplication issues with its other homeland security networks and associated systems and applications. Until DHS completes these activities, including developing an inventory of key state and local initiatives, and fully implementing and institutionalizing key practices and guidance for effective coordination and collaboration, it will continue to be at risk of not effectively sharing information with other key state and local information initiatives and duplicating state and local capabilities.

Background

DHS is the lead department involved in securing our nation's homeland. Its mission includes, among other things, leading the unified national effort to secure the United States, preventing and deterring terrorist attacks, and protecting against and responding to threats and hazards to the nation. As part of its mission and as required by the Homeland Security Act of 2002,[4] the department is also responsible for coordinating efforts across all levels of government and throughout the nation, including with federal, state, tribal, local, and private sector homeland security resources.

As we have previously reported, DHS relies extensively on information technology (IT), such as networks and associated system applications, to carry out its mission.[5] Specifically, in our recent report, we reported that the department identified 11 major networks it uses to support its homeland security functions, including sharing information with state and local governments.[6] Examples of such DHS networks include the Homeland Secure Data Network, the Immigration and Customs Enforcement Network, and the Customs and Border Protection Network. In addition, the department has deployed HSIN, a homeland security information-sharing application that operates on the public Internet. As shown in table 1, of the 11 networks, 1 is categorized as Top Secret, 1 is Secret, 8 are Sensitive but Unclassified, and 1 is unclassified. HSIN is considered Sensitive but Unclassified.

Table 1: DHS Information-Sharing Networks and HSIN Application

Name	Categories	Users outside DHS	Reported cost per fiscal year (dollars in millions)		
			2005	2006	Total
C Local Area Network (C–LAN)	Top Secret	—	(a)	(a)	—
Homeland Secure Data Network (HSDN)	Secret	Other federal, state, local	$46.2	$32.6	$78.8
Coast Guard Data Network Plus (CGDN+).	Sensitive but Unclassified	Other federal	15.0	15.0	30.0
Critical Infrastructure Warning Information Network (CWIN).	Sensitive but Unclassified	Other federal, state	12.1	12.0	24.1
Customs and Border Protection (CBP) Network.	Sensitive but Unclassified	—	58.7	63.0	121.7
DHS Core Network (DCN)	Sensitive but Unclassified	—	13.4	10.3	23.7
Homeland Security Information Network (HSIN).	Sensitive but Unclassified	Other federal, state, local	11.9	20.5	32.4

[4] Homeland Security Act of 2002, Pub. L. No. 107–296, 116 Stat. 2135 (Nov. 25, 2002).

[5] See, for example, GAO, *Information Technology: Major Federal Networks That Support Homeland Security Functions,* GAO–04–375 (Washington, D.C.: Sept. 17, 2004) and *Information Technology: DHS Needs to Fully Deine and Implement Polices and Procedures for Effectively Managing Investments,* GAO–07–424 (Washington, D.C.: April 27, 2007).

[6] GAO–07–455.

Name	Categories	Users outside DHS	Reported cost per fiscal year (dollars in millions)		
			2005	2006	Total
Immigration and Customs Enforcement Network (ICENet).	Sensitive but Unclassified	Other federal, state, local	14.4	19.2	33.6
ONENet	Sensitive but Unclassified	—	34.6	40.0	74.6
Secret Service Wide Area Network (WAN).	Sensitive but Unclassified	—	2.8	3.1	5.9
Transportation Security Administration Network (TSANet).	Sensitive but Unclassified	Other federal	70.0	105.0	175.0
Federal Emergency Management Agency (FEMA) Switched Network.	Unclassified	—	6.0	6.0	12.0
Total[a]			$285.1	$326.7	$611.8

Source: GAO analysis of agency data.

[a] Costs for C–LAN are not included, as the information is not publicly available.

As the table shows, some of these networks are used solely within DHS, while others are also used by other federal agencies, as well as state and local governments. In addition, the total cost to develop, operate, and maintain these networks and HSIN in fiscal years 2005 and 2006, as reported by DHS, was $611.8 million. Of this total, the networks accounted for the vast majority of the cost: $579.4 million.

DHS Established HSIN to Provide Information–Sharing Capabilities

DHS considers HSIN to be its primary communication application for transmitting sensitive but unclassified information. According to DHS, this network is an encrypted, unclassified, Web-based communications application that serves as DHS's primary nationwide information-sharing and collaboration tool. It is intended to offer both real-time chat and instant messaging capability, as well as a document library that contains reports from multiple federal, state, and local sources. Available through the application are suspicious incident and pre-incident information and analysis of terrorist threats, tactics, and weapons. The application is managed within DHS's Office of Operations Coordination.

HSIN includes over 35 communities of interest, such as emergency management, law enforcement, counterterrorism, individual states, and private sector communities. Each community of interest has Web pages that are tailored for the community and contain general and community-specific news articles, links, and contact information. The community Web pages also provide access to other resources, such as the following:

- *Document library.* Users can search the entire document library within the communities they have access to.
- *Discussion threads.* HSIN has a discussion thread (or bulletin board) feature that allows users to post information that other users should know about and post requests for information that other users might have. Community administrators can also post and track tasks assigned to users during an incident.
- *Chat tool.* HSIN's chat tool, known as Jabber, is similar to other instant message and chat tools—with the addition of security. Users can customize lists of their coworkers and send messages individually or set up chat rooms for more users. Other features include chat logs (which allow users to review conversations), timestamps, and user profiles.

States and Local Governments Have Also Established Similar Initiatives

State and local governments have similar IT initiatives to carry out their homeland security missions, including sharing information. A key state and local-based initiative is the Regional Information Sharing Systems (RISS) program.

The RISS program helps state and local jurisdictions to, among other things, share information in support of their homeland security missions. This nationwide program, operated and managed by state and local officials, was established in 1974 to address crime that operates across jurisdictional lines. The program consists of

six regional information analysis centers that serve as regional hubs across the country. These centers offer services to RISS members in their regions, including information sharing and research, analytical products, case investigation support, funding, equipment loans, and training. Funding for the RISS program is administered through a grant from the Department of Justice.

As part of its information-sharing efforts, the RISS program operates two key initiatives (among others): the RISS Secure Intranet (RISSNET) and the Automated Trusted Information Exchange[7] (RISS ATIX):

- Created in 1996, RISSNET is intended as a secure network serving member law enforcement agencies throughout the United States and other countries. Through this network, RISS offers services such as secure e-mail, document libraries, intelligence databases, Web pages, bulletin boards, and a chat tool.
- RISS ATIX offers services similar to those offered by RISSNET to agencies beyond the law enforcement community, including executives and officials from governmental and nongovernmental agencies and organizations that have public safety responsibilities. RISS ATIX is partitioned into 39 communities of interest, such as critical infrastructure, emergency management, public health, and government officials. Members of each community of interest contribute information to be made available within each community.

  According to RISS officials, the RISS ATIX application was developed in response to the events of September 11, 2001; it was initiated in 2002 as an application to provide tools for information sharing and collaboration among public safety stakeholders, such as first responders and schools. As of July 2006, RISS ATIX supported 1,922 users beyond the traditional users of RISSNET.

  RISS ATIX uses the technology of RISSNET to offer services through its Web pages. The pages are tailored for each community of interest and contain community-specific news articles, links, and contact information. The pages also provide access to the following features:

- *Document library.* Participants can store and search relevant documents within their community of interest.
- *Bulletin board.* The RISS ATIX bulletin board allows users to post timely threat information in discussion forums and to view and respond to posted information. Users can post documents, images, and information related to terrorism and homeland security, as well as receive DHS information, advisories, and warnings. According to RISS officials, the bulletin boards are monitored by a RISS moderator to relay any information that might be useful for other communities of interest.
- *Chat tool.* ATIXLive is an online, real-time, collaborative communications information-sharing tool for the exchange of information by community members. Through this tool, users can post timely threat information and view and respond to messages posted.
- *Secure e-mail.* RISS ATIX participants have access to e-mail that can be used to provide alerts and related information. According to RISS, this is done in a secure environment.

GAO Has Designated Information Sharing as High Risk

The need to improve information sharing as part of a national effort to improve homeland security and preparedness has been widely recognized, not only to improve our ability to anticipate and respond to threats and emergencies, but to avoid unnecessary expenditure of scarce resources. In January 2005,[8] and more recently in January 2007,[9] we identified establishing appropriate and effective information-sharing mechanisms to improve homeland security as a high-risk area. The Office of Management and Budget (OMB) has also issued guidance that stresses the importance of information sharing and avoiding duplication of effort.[10] Nonetheless, although this area has received increased attention, the federal government faces formidable challenges in sharing information among stakeholders in an appropriate and timely manner.

As we concluded in October 2005, agencies can help address these challenges by adopting and implementing key practices, related to OMB's guidance, to improve collaboration, such as establishing joint strategies and addressing needs by leveraging resources and developing compatible policies, procedures, and other

[7] Formerly called the Anti–Terrorism Information Exchange.
[8] GAO, *High-Risk Series: An Update,* GAO–05–207 (Washington, D.C.: January 2005).
[9] GAO, *High-Risk Series: An Update,* GAO–07–310 (Washington, D.C.: January 2007).
[10] For example, Office of Management and Budget, *Management of Federal Information Resources, Circular* A–130 (Washington, D.C.: Nov. 30, 2000) and *Preparation, Submission, and Execution of the Budget,* Circular A–11 (Washington, D.C.: June 30, 2006).

means to operate across agency boundaries.[11] Based on our research and experience, these practices are also relevant for collaboration between federal agencies and other levels of government (e.g., state, local). Until these coordination and collaboration practices are implemented, agencies face the risk that effective information sharing will not occur.

Congress and the Administration have made several efforts to address the challenges associated with information sharing. In particular, as we reported in March 2006, the President initiated an effort to establish an Information Sharing Environment that is to combine policies, procedures, and networks and other technologies that link people, systems, and information among all appropriate federal, state, local, and tribal entities and the private sector.[12] In November 2006, in response to congressional direction, the Administration issued a plan for implementing this environment and described actions that the federal government intends—in coordination with state, local, tribal, private sector, and foreign partners—to carry out over the next 3 years.

Efforts to Coordinate HSIN with Key State and Local Information–Sharing Initiatives Have Been Limited

DHS did not fully adhere to the previously mentioned key practices in coordinating its efforts on HSIN with key state and local information-sharing initiatives. The department's limited use of these practices is attributable to a number of factors: in particular, after the events of September 11, 2001, the department expedited its schedule to deploy HSIN capabilities, and in doing so, it did not develop an inventory of key state and local information initiatives. Until the department fully implements key coordination and collaboration practices and guidance, it faces, among other things, the risk that effective information sharing is not occurring. DHS has efforts planned and under way to improve coordination and collaboration, including implementing the recommendations in our recent report.[13]

Key Practices Were Not Effectively Implemented

In developing HSIN, DHS did not fully adhere to the practices related to OMB's guidance. First, although DHS officials met with RISS program officials to discuss exchanging terrorism-related documents, joint strategies for meeting mutual needs by leveraging resources have not been fully developed. DHS did not engage the RISS program to determine how resources could be leveraged to meet mutual needs. According to RISS program officials, they met with DHS twice (on September 25, 2003, and January 7, 2004) to demonstrate that their RISS ATIX application could be used by DHS for sharing homeland security information. However, communication from DHS on this topic stopped after these meetings, without explanation. According to DHS officials, they did not remember the meetings, which they attributed to the departure from DHS of the staff who had attended.

In addition, although DHS initially pursued a limited strategy of exchanging selected terrorism-related documents with the RISS program, the strategy was impeded by technical issues and by differences in what each organization considers to be terrorism information. For example, the exchange of documents between HSIN and the RISS program stopped on August 1, 2006, because of technical problems with HSIN's upgrade to a new infrastructure. As of May 3, 2007, the exchange of terrorism-related documents had not yet resumed, according to HSIN's program manager. This official also stated that the program is currently working to fix the issue with the goal of having it resolved by June 2007.

Finally, DHS has yet to fully develop coordination policies, procedures, and other means to operate across agency boundaries with the RISS program. DHS has not fully developed such means to operate with the RISS program and leverage its available technological resources. Although an operating agreement was established to govern the exchange of terrorism-related documents, according to RISS officials, it did not cover the full range of information available through the RISS program.

DHS's Expedited Schedule Was Major Cause for Limited Coordination, Increasing the Risk of Ineffective Information Sharing and Duplication

The extent of DHS's adherence to key practices (and the resulting limited coordination) is attributable to DHS's expedited schedule to deploy an information-sharing application that could be used across the federal government in the wake of the September 11 attacks; in its haste, DHS did not develop a complete inventory of key

[11] GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies,* GAO–06–15 (Washington, D.C.: October 2005).

[12] GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitve but Unclassified Information,* GAO–06–385 (Washington, D.C.: March 2006).

[13] GAO–07–455.

state and local information initiatives. According to DHS officials, they still do not have a complete inventory of key state and local information-sharing initiatives. DHS's Office of Inspector General also reported that DHS developed HSIN in a rapid and ad hoc manner, and among other things, did not adequately identify existing federal, state, and local resources, such as RISSNET, that it could have leveraged.[14]

Further, DHS did not fully understand the RISS program. Specifically, DHS officials did not acknowledge the RISS program as a state and local based program with which to partner, but instead considered it to be one of many vendors providing a tool for information sharing. In addition, DHS officials believed that the RISS program was solely focused on law enforcement information and did not capture the broader terrorism-related or other information of interest to the department.

Because of this limited coordination and collaboration, DHS is at increased risk that effective information sharing is not occurring. The department also faces the risk that it is developing and deploying capabilities on HSIN that duplicate those being established by state and local agencies. There is evidence that this has occurred with respect to the RISS program. Specifically:

- HSIN and RISS ATIX currently target similar user groups. DHS and the RISS program are independently striving to make their applications available to user communities involved in the prevention of, response to, mitigation of, and recovery from terrorism and disasters across the country. For example, HSIN and RISS ATIX are being used and marketed for use at state fusion centers[15] and other state organizations, such as emergency management agencies across the country.
- HSIN and RISS applications have similar approaches for sharing information with their users. For example, on each application, users from a particular community—such as emergency management—have access to a portal or community area tailored to the user's information needs. The community-based portals have similar features focused on user communities. Both applications provide each community with the following features:[16]
- *Web pages.* Tailored for communities of interest (e.g., law enforcement, emergency management, critical infrastructure sectors), these pages contain general and community-specific news articles, links, and contact information.
- *Bulletin boards.* Participants can post and discuss information.
- *Chat tool.* Each community has its own online, real-time, interactive collaboration application.
- *Document library.* Participants can store and search relevant documents.

DHS Has Improvements Planned and Under Way, Including Implementing Our Recent Recommendations

According to DHS officials, including the HSIN program manager, the department has efforts planned and under way to improve coordination. For example, the department is in the process of developing an integration strategy that is to include enhancing HSIN so that other applications and networks can interact with it. This would promote integration by allowing other federal agencies and state and local governments to use their preferred applications and networks—such as RISSNET and RISS ATIX—while allowing DHS to continue to use HSIN.

Other examples of improvements either begun or planned include the following:

- The formation of an HSIN Mission Coordinating Committee, whose roles and responsibilities are to be defined in a management directive. It is expected to ensure that all HSIN users are coordinated in information-sharing relationships of mutual value.
- The recent development of engagement, communications, and feedback strategies for better coordination and communication with HSIN, including, for example, enhancing user awareness of applicable HSIN contact points and changes to the system.
- The reorganization of the HSIN program management office to help the department better meet user needs. According to the program manager, this reor-

[14] Department of Homeland Security Office of Inspector General, Office of Information Technology, *HSIN Could Support Information Sharing More Effectively,* DHS/OIG–06–38 (Washington, D.C.: June 2006).

[15] A fusion center is defined as a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."

[16] Beyond the collaboration tools listed, RISSNET also provides access to other law enforcement resources, such as analytical criminal data-visualization tools and criminal intelligence databases.

ganization has included the use of integrated process teams to better support DHS's operational mission priorities as well as the establishment of a strategic framework and implementation plan for meeting the office's key activities and vision.

• The establishment of a HSIN Advisory Committee to advise the department on how the HSIN program can better meet user needs, examine DHS's processes for deploying HSIN to the states, assess state resources, and determine how HSIN can coordinate with these resources. In addition to these planned improvements, DHS has agreed to implement the recommendations in our recent report. Specifically, we recommended that the department ensure that HSIN is effectively coordinated with key state and local government information-sharing initiatives. We also recommended that this include (1) identifying and inventorying such initiatives to determine whether there are opportunities to improve information sharing and avoid duplication, (2) adopting and institutionalizing key practices related to OMB's guidance on enhancing and sustaining agency coordination and collaboration, and (3) ensuring that the department's coordination efforts are consistent with the Administration's recently issued Information Sharing Environment plan.[17] In response to these recommendations, DHS described actions it was taking to implement them. (The full recommendations and DHS's written response to them are in report.)

In closing, DHS has not effectively coordinated its primary information-sharing system with two key state and local initiatives. Largely because of the department's hasty approach to delivering needed information-sharing capabilities, it did not follow key coordination and collaboration practices and guidance or invest the time to inventory and fully understand how it could leverage state and local approaches. Consequently, the department faces the risk that effective information sharing is not occurring and that its HSIN application may be duplicating existing state and local capabilities. This also raises the issue of whether similar coordination and duplication issues exist with the other federal homeland security networks and associated systems and applications under the department's purview.

DHS recognizes these risks and has improvements planned and under way to address them, including stated plans to implement our recommendations. These are positive steps and should help address shortfalls in the department's coordination practices on HSIN. However, these actions have either just begun or are planned, with milestones for implementation yet to be defined. Until all the key coordination and collaboration practices are fully implemented and institutionalized, DHS will continue to be at risk that the effectiveness of its information sharing is not where it needs to be to adequately protect the homeland and that its efforts are unnecessarily duplicating state and local initiatives.

Madame Chair, this concludes my testimony today. I would be happy to answer any questions you or other members of the subcommittee may have.

Ms. HARMAN. I thank you, Mr. Powner, for powerful testimony delivered in precisely 5 minutes.

Mr. Kennedy, no pressure.

[Laughter.]

STATEMENT OF DONALD KENNEDY, EXECUTIVE DIRECTOR, NEW ENGLAND STATE POLICE INFORMATION NETWORK, (RISS)

Mr. KENNEDY. Good morning. Chairman Harman and members of the subcommittee, I sincerely appreciate the opportunity to appear before you today to discuss efforts in the exchange of homeland security information and initiatives currently under way to leverage existing systems available to criminal justice agencies throughout our country.

As stated by the chairman, I am currently the executive director of the New England State Police Information Network, one of the six regional information-sharing system centers in the United States, otherwise known as RISS.

[17] As mentioned earlier, this plan is aimed at establishing, in 3 years, the networks and other technologies that link people, systems, and information among all appropriate federal state, local, and tribal entities and the private sector.

Having been a part of law enforcement for the past 33 years, first serving 24 years as a member of the Rhode Island State Police and now serving as a member of the RISS program for the last 9 years, I have come to understand first-hand the importance of information sharing across all levels of government.

Decades before terrorism moved into the forefront, RISS was established to combat crime and enhance public safety. The RISS program is a congressionally funded nationwide program supporting state, local, federal and tribal law enforcement, and prosecution efforts, with membership in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England.

The RISS program operates on a national basis, but provides support regionally through its six intelligence centers, which support and serve the unique needs of their individual regions. One of RISS's strengths is that each RISS center is governed by a policy board consisting of executives representing state, local and tribal law enforcement.

RISS currently provides services to 75,000 access offices representing hundreds of thousands of law enforcement officers from all government levels. Some of those services that RISS provides includes analysis, training, confidential funds, equipment loans, and a telecommunications systems we call RISSNET.

RISSNET was developed in 1997 and is a national system that was designed by and for state and local law enforcement. RISSNET provides its users with a variety of online resources, which include websites, bulleting boards, and intelligence databases that are managed and populated by the law enforcement community we serve.

At RISS, we have always be cognizant of the need for communication interoperability between existing law enforcement systems, so much so that in the pat 10 years, RISS has partnered and linked our system to numerous other state, local and federal databases, as well as recently providing node connectivity to state fusion centers and intelligence centers throughout the U.S. so that data can be shared securely, using the RISS backbone, fusion center to fusion center.

RISS has worked closely with DEA to develop the national virtual pointer system, which is a national database for narcotics traffickers, along with the Alcohol, Tobacco and Firearms to share their GangNet database; and the U.S. Secret Service, who share their dignitary protection database with our users, using our node connection to RISSNET.

Continuing with this effort, soon after 9/11, RISS partnered with the FBI's law enforcement online system in an attempt to share data between the two systems. This partnership was referenced in the global national criminal intelligence sharing plan as systems that law enforcement should utilize in their information intelligence sharing using the Internet.

After 9/11, RISS also approached the Department of Homeland Security to partner with their then-JRIES—Joint Regional Intelligence Exchange System. Several meetings were held, and several presentations were provided in the hopes that DHS would adopt the RISSNET system, or at least utilize some of the law enforcement or first responder resources we provide. For whatever reason,

that did not come to fruition, and soon after JRIES became the Homeland Security Information Network.

Recently, RISS again approached DHS and HSIN in an effort to better share law enforcement first responder documents. This dialogue ahs been quite successful as of late, and thanks to the hard work of folks like Theresa Phillips of Homeland Security in the HSIN program, we believe that we are closer to completing that particular RSS feed from Homeland's information network to the RISS environment.

But we need to do more. We need to continue the dialogue between systems like RISS, LEO, HSIN and other systems that have a public safety mission or nexus. We need to discuss not only the sharing of documents, but the need for bidirectional communication and the interoperability of these systems so that we can technically accomplish what I call a single log-on capability where if I, as a HSIN user, would like to get to a RISS or a LEO resource, that I can do that without having to log-off from that system and log-on to one of those other two systems.

The time is right for this technical solution to occur. RISS has been working very hard and has developed a way in which this will work and work successfully. RISS stands ready to meet and discuss and work with the policymakers and technical staffs of both DHS and DOJ to make this goal a reality. But first we need buy-in by the senior leadership of both DOJ and DHS.

Madam Chairman, I thank you and your colleagues for giving me this opportunity to speak with you today. I hope that my comments have been of use to you.

[The statement of Mr. Kennedy follows:]

PREPARED STATEMENT OF DONALD F. KENNEDY

Chairman Thompson, Ranking Member King, Chairwoman Harman, and Members of the Subcommittee, I sincerely appreciate the opportunity to appear before you today to discuss efforts in the exchange of homeland security information and initiatives currently under way to leverage existing systems available to criminal justice agencies in our country.

I currently serve as the Executive Director of the New England State Police Information Network (NESPIN), one of the six Regional Information Sharing Systems (RISS) centers. Prior to being named Executive Director, I served as NESPIN's Deputy Director of Field Services after retiring as a captain from the Rhode Island State Police, having served in all bureaus and divisions within the state police for 24 years. In my career, I have been afforded the opportunity to actively participate in many aspects of law enforcement, from patrol to policymaker. In those roles, I have come to understand firsthand the importance of information sharing across all levels of government.

Decades before terrorism moved to the forefront, RISS was established to combat crime and enhance public safety. The RISS Program is a congressionally funded, nationwide program supporting local, state, federal, and tribal law enforcement and prosecution efforts, with membership in the 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England. The RISS Program operates on a national basis but provides support regionally through its six regional intelligence centers, which support and serve the unique needs of their individual regions. The six RISS centers and the areas which they serve are:

- **Middle Atlantic–Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN):** *Delaware, District of Columbia, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, and Pennsylvania, as well as Australia, Canada, and England.*
- **Mid-States Organized Crime Information Center (MOCIC):** *Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin, as well as Canada.*

• **New England State Police Information Network (NESPIN):** *Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont, as well as Canada.*
• **Regional Organized Crime Information Center (ROCIC):** *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.*
• **Rocky Mountain Information Network (RMIN):** *Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming, as well as Canada.*
• **Western States Information Network (WSIN):** *Alaska, California, Hawaii, Oregon, and Washington, as well as Canada and Guam.*

Each RISS center is governed by a policy board or executive committee, composed of representatives from member agencies in the center's multistate region. The RISS National Policy Group is composed of the six Directors of the RISS centers and the chair of each center's policy board. The RISS National Policy Group is responsible for strategic planning, resolution of operational issues, advancement of information sharing, and decision making affecting the six RISS centers, the national organization, service delivery, member agencies, and related partner organizations.

The RISS Program strives to enhance the ability of criminal justice agencies to identify, target, and remove criminal conspiracies and activities spanning multijurisdictional, multistate and, sometimes, international boundaries. RISS facilitates rapid exchange and sharing of information among the agencies pertaining to known suspected criminals or criminal activity and enhances coordination and communication among agencies that are in pursuit of criminal conspiracies determined to be interjurisdictional in nature.

RISS is a force multiplier in fighting increased violent criminal activity by terrorists, drug traffickers, sophisticated cybercriminals, gangs, and emerging criminal groups that require a cooperative effort by local, state, federal, and tribal law enforcement. There is an increasing communications sophistication by the criminal networks, including terrorists, and a rising presence of organized and mobile narcotics crime. Interagency cooperation in sharing information has proven to be the best method to combat this increasing criminal activity. The RISS centers are filling law enforcement's need for rapid, but controlled, sharing of information and intelligence pertaining to known or suspected terrorists and other criminals. Congress funded the RISS Program to address this need, as evidenced by its authorization in the Omnibus Crime Control and Safe Streets Act, Part M.

RISS provides diverse and valuable services and tools directly to detectives and investigative units within local, state, regional, federal, and tribal criminal justice entities, making RISS a comprehensive and universal program. These services and tools include investigative and intelligence analysis, secure national information sharing and communications capabilities, specialized investigative equipment, investigative funds support, criminal activity bulletins and publications, training, and other investigative support and technical services *(Attachment A)*.

The Bureau of Justice Assistance (BJA) administers the RISS Program and has established guidelines for provision of services to member agencies. The RISS centers are subject to oversight, monitoring, and auditing by the U.S. Congress; the U.S. Government Accountability Office, a federally funded program evaluation office; the U.S. Department of Justice (DOJ), BJA; and local and state governmental units. BJA also monitors the RISS centers for 28 Code of Federal Regulations (CFR) Part 23 compliance. 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 its 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 adopted a RISS Privacy Policy to further strengthen their commitment and support of 28 CFR Part 23 and protection of individual privacy rights.

RISS has served as a pioneer, forging the way for today's information sharing age. In 1997, through funding from Congress, RISS implemented and continues to operate the secure Web-based nationwide law enforcement network known as RISSNET. RISSNET offers state-of-the-art technology to address and support law enforcement demands for rapid communication and sharing of information. RISSNET provides the communications backbone and infrastructure for sharing investigative and intelligence information, offers secure sensitive but unclassified electronic communications, and provides controlled access to a variety of sensitive information resources.

Currently, RISS serves over 7,700 law enforcement and criminal justice agencies from all levels of government. Over 75,000 access officers, representing hundreds of

thousands of law enforcement officers from all government levels, are able to access the databases of six regional RISS centers and other intelligence systems from a single query—member agencies have bidirectional access to a number of state, regional, federal, and specialized criminal intelligence systems electronically connected to RISSNET. Examples of agencies connected to RISSNET include the Clandestine Laboratory Seizure System at the El Paso Intelligence Center (EPIC); the National Drug Pointer Index (NDPIX); the Law Enforcement Intelligence Unit (LEIU) Database; the National White Collar Crime Center (NW3C); Nlets—The International Justice and Public Safety Information Sharing Network; the California Department of Justice, Bureau of Investigation, Intelligence Database; the Criminal Information Sharing Alliance network (CISAnet); the Oregon State Intelligence Network; the Utah Law Enforcement Information Network; the Wyoming Criminal Justice Information Network; and the Colorado Law Enforcement Intelligence Network. The Executive Office for United States Attorneys has also connected staff to RISSNET, as well as all of the 93 U.S. Attorneys' Offices Anti-Terrorism Task Forces throughout the United States. In addition, staff at DOJ, Criminal Division, have connected to RISSNET.

In this world of rapidly changing technology and with the increased need to provide timely, accurate, and complete information to law enforcement and public safety professionals, the ability to connect critical systems and streamline the ability to house, share, inquire, and disseminate information and intelligence is paramount. Through RISS's trusted system, the ability for law enforcement to target, investigate, and prosecute crime continuously improves. RISS also provides valuable collaboration with others who have experienced similar crime problems or who are investigating the same or similar crime.

RISS has also entered into a partnership with the High Intensity Drug Trafficking Areas (HIDTA) to electronically connect all of the HIDTAs to RISSNET for communications and information sharing. Currently, 18 HIDTAs are electronically connected as nodes to RISSNET. RISS is working to complete the connection of the remaining HIDTAs. RISS has partnered with the HIDTAs and Nlets to create the National Virtual Pointer System (NVPS). The NVPS, which became operational in June 2004, is an automated system that connects existing deconfliction pointer databases into one virtual pointer system. RISS has also developed an officer safety deconfliction system, RISSafe, to be accessible by member agencies for the purpose of identifying potential conflict in operational cases.

RISS has emerged as one of the nation's most important law enforcement intelligence sharing networks and continues to support efforts to expand and improve information sharing. The partnerships RISS has formed with fellow criminal justice and public safety agencies has allowed for this unprecedented level of information and intelligence to be exchanged through RISSNET. As a result, it is critical to ensure that the information is secure and available only to those with authorized access. RISSNET protects information through use of encryption, smart cards, Internet protocol security standards, and firewalls to prevent unauthorized access. The criminal intelligence information accessed through RISSNET is controlled by its local, state, federal, and tribal law enforcement member agency owners. 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. RISSNET supports secure e-mail and is easily accessible using the Internet. This type system and architecture is referenced and recommended in the *General Counterdrug Intelligence Plan* (GCIP) and is endorsed by the *National Criminal Intelligence Sharing Plan* (NCISP).

The NCISP represents law enforcement's commitment to ensure that the "dots are connected," be it in crime or terrorism. The Plan supports collaboration and fosters an environment in which all levels of law enforcement can work together to improve the safety of the nation. The Plan is the outcome of an unprecedented effort by local, state, federal, and tribal law enforcement officials at all levels, with the strong support of DOJ, to strengthen the nation's security through better intelligence analysis and sharing.

The NCISP provides in Recommendation 21 that RISS and the Federal Bureau of Investigation (FBI) Law Enforcement Online (LEO) systems, which interconnected September 1, 2002, as a virtual single system, shall provide the initial sensitive but unclassified secure communications backbone for implementation of a nationwide criminal intelligence sharing capability. In addition to providing secure communications, the RISS Program has embraced and integrated many of the recommendations contained in the NCISP. For example, RISS is developing 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. This project, known as the

Trusted Credential Project, will promote interoperable connectivity among information sharing systems, allow bidirectional sharing, and enhance critical information exchange.

RISS is also embarking on an initiative to streamline the process for RISS users to access RISSNET resources. Known as the RISSNET Portal, it will provide users with one entry point for RISSNET, allowing them to instantly view and access all RISSNET resources from one location. In addition, RISS is moving to an industry standards-based SSL authentication technology. SSL technology is a mature technology for the transmission of encrypted information and is supported by all major Internet browsers. These three initiatives—the Trusted Credential Project, RISSNET Portal, and SSL—will work in unison and represent the natural next steps for enhancing RISS technology and service to its members.

In the aftermath of 9/11, RISS recognized the critical need for timely exchange of national security and terrorist threat information, not only among law enforcement officials but to all first responders and officials involved in homeland security. As a result, RISS created the Automated Trusted Information Exchange (ATIX). ATIX is a communication system that allows first responders, critical infrastructure personnel, and other public safety personnel—including firefighters and public utility and school personnel and local, state, and federal law enforcement—to share terrorism and homeland security information in a secure, real-time environment. Through ATIX, users access the RISS ATIX Web pages and library, the ATIX bulletin board, ATIXLive, and secure e-mail.

In its first year of connectivity, ATIX was selected as the official system for secure communication and information sharing for the G8 Summit in 2004 by the team in charge of security and communications, 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. In 2005, the ability for ATIX to be successfully utilized in the aftermath of a disaster was demonstrated when it served as a communication tool following Hurricane Katrina. RISS provided logistical support to law enforcement in the damaged areas to receive water, clothing, food, medical supplies, information, and equipment. In addition, RISS prepared intelligence assessments on gang and criminal activity, which aided law enforcement response following the hurricane. In 2006, ATIX demonstrated its communications power during a plane crash incident in Delaware, when a C–5 cargo plane, laden with supplies for U.S. troops in Iraq, crashed after takeoff from Dover Air Force Base. The Delaware Information Analysis Center (DIAC), through its use of ATIX, communicated the incident to appropriate officials and personnel ten minutes prior to media reports of the incident. This allowed law enforcement and first responders to coordinate efforts, assess the situation, and secure the scene. And today, some state homeland security offices, such as DIAC, use ATIX to communicate critical information on a daily basis. In Delaware, more than 100 users across 21 discipline communities involved in their multijurisdictional, multiagency response to all crimes and all hazards utilize ATIX as a primary tool to communicate on a daily basis.

In the months following the creation and deployment of ATIX, RISS reached out to the U.S. Department of Homeland Security (DHS) and other federal agencies to offer the infrastructure support and services available through RISSNET. It was also during this time that DHS was transitioning from the Joint Regional Information Exchange System (JRIES) to the Homeland Security Information Network (HSIN) as a means of expanding to include more communities. In July 2005, at the culmination of numerous briefings and meetings, an executive meeting was held to discuss interoperability and interconnection of the JRIES/HSIN, RISS, and LEO. At that time, a joint decision was made by policymakers from RISS, DOJ, DHS, and FBI to demonstrate interoperability of the systems within a short time frame of 60 days. The parties collaborated to produce a technical white paper describing the information sharing project and a memorandum of understanding. The ultimate goal of this project was to quickly demonstrate the capability to create a seamless connection between systems, permitting users of the individual systems to access unique tools, resources, and capabilities of all the systems through the current access method.

Although not all the aspects of this initiative came to fruition, RISS and DHS still created an information sharing partnership. During the past two years, RISS has continued to work with DOJ and DHS on what has evolved into the Counterterrorism Collaboration Interoperability Project (CCIP). CCIP is a partnership among RISS, HSIN, LEO, and CISAnet that allows the participating partner systems to publish documents for access by authorized users of the other participating partners? systems via the use of Really Simple Syndication (RSS) feeds. This project has been recognized as a model for all agencies that will share information, as required

by Presidential Executive Order 13388, *Strengthening the Sharing of Terrorism Information to Protect Americans.*

While significant strides have been made in the implementation of the CCIP, much work still remains. For example, a disruption in the RSS feeds from HSIN to RISSNET has resulted in a daily search effort by RISS technical staff to access documents posted on the HSIN Law Enforcement and HSIN Emergency Management sites. Through the limited access that RISS has been granted to HSIN, a concerted effort is made to identify and retrieve information available on HSIN, which could be provided automatically through RSS feeds, and post this information on ATIX for access by thousands of users.

In addition to the CCIP, RISS is also involved in other critical initiatives with federal agencies to assist in their efforts to facilitate the exchange of criminal intelligence with local and state law enforcement. As the only nonfederal agency or organization involved in the Law Enforcement Information Sharing Program (LEISP), RISS has the unique opportunity to participate in the this critical initiative with DHS and DOJ to demonstrate applicability of federated identity management as a tool to enhance information sharing. In addition, RISS has been invited to participate in a Secure But Unclassified (SBU) Networks/Systems Collaboration Effort initiative from the Information Sharing Council, tasked to the Program Manager—Information Sharing Environment. This effort is focused on sharing SBU terrorism information and identifying capabilities necessary for a SBU Network/System to be included in the Information Sharing Environment. RISS is pleased to receive these invitations, have the opportunity to assist in the development of national strategies for information sharing, and be recognized for its significant role in advocating for local and state agencies who depend on RISSNET as a system of systems for information sharing.

Local and state law enforcement, which depend on the RISS centers, must be leveraged and included in an information sharing plan. The more than 800,000 law enforcement officers and over 19,000 police agencies in this country are part of the frontline defense in domestic security. Important intelligence/information that may forewarn of a future attack is collected by local and state government personnel through their routine activities. The critical importance of intelligence for frontline police officers cannot be overstated. And without the benefit of intelligence, local and state law enforcement cannot be expected to be active partners in protecting our communities from terrorism. The RISS Program aims to represent these frontline officers in the quest for increased terrorism information sharing in our nation and strives to provide a platform for all areas of homeland security to work together to detect, deter, and prevent terrorist activities and to improve the safety of our nation. As demand from citizens continues to increase for the country to be ready and prepared and funds continue to tighten, it will be critical to leverage available resources and expertise.

The ultimate goal of RISS is to develop and enhance bidirectional systems access and provide secure real-time information, enabling all participants to share information to enhance the investigative process, in furtherance of recommendations in the *National Criminal Intelligence Sharing Plan.* Having a trusted sharing environment for communicating information and intelligence is a priority issue. There are a number of national systems and networks that local, state, and tribal law enforcement agencies utilize for information sharing efforts, including RISS, LEO, and HSIN. Each of these systems offers unique resources and provides essential information to its primary users. However, the power of these systems linked is exemplary of the whole being greater than the sum of its parts. A true success would be the creation of a "system of systems" that is accessible by hundreds of thousands of criminal justice and homeland security officials, as well as first responders and private sector partners who aid our country in the battle against terrorism.

Currently, users must sign on to multiple systems in order to access information. Rather than develop new systems, it is recommended that the existing networks and systems be modified and augmented based on continuing information needs. The federal government should provide the funding needed to leverage existing information sharing systems and expand intelligence sharing by executing interoperability between operating systems at the local, state, regional, federal, and tribal levels using a federated identification methodology. Local, state, and tribal users should be able to access all pertinent information from disparate systems with a single sign-on, based on the user's classification level and need to know.

In order to succeed, we must bridge the remaining gaps between local, state, and federal intelligence agencies and homeland security information consumers. If we are to continue to successfully deter and prevent attacks, we must work as one united force to combat all crimes.

Over the last few years, RISS has seen increased interest by individuals, agencies, and organizations to use RISSNET as their primary communications system and to partner with RISS on a variety of critical projects and initiatives. RISS is eager to meet this demand and continually partners with law enforcement and criminal justice agencies to fully develop an efficient and effective information sharing environment. However, this demand is draining RISS's resources, and additional funds are needed to ensure that law enforcement and the criminal justice community continue to improve both their information sharing and investigative capabilities in order to most effectively protect public safety.

In Fiscal Year (FY) 2007, RISS was appropriated $39.719 million, the same level appropriated in fiscal year 2006. For fiscal year 2008, the President's Budget includes $38.5 million, $1.219 million less than the fiscal year 2007 appropriation. Based on the needs of local and state law enforcement throughout the country, as well as the demand for increased safeguarding against terrorism, gangs, violent crimes, and other critical crime problems, RISS has requested $53.7 million.

To combat crime, there must be continued funding support to programs like RISS, which have demonstrated decades of success in fighting crime, advancing technology, and enhancing officer safety. Through this strategy, we can maximize available funding, eliminate duplication, and accomplish more with less.

Mr. Chairman, I thank you and your colleagues for giving me the opportunity to speak to you today, and I hope my comments have been of some use to you in your deliberations.

ATTACHMENT A: The Regional Information Sharing Systems

Each RISS center offers basic services to member agencies. Traditional services include information sharing, analysis, telecommunications, equipment loans, confidential funds, training, and technical assistance.

- **Information Sharing**—The operation of RISSNET and its various applications enhances information sharing and communications among RISS members by providing various secure databases and investigative tools. Each RISS center develops and provides access to specialized information sharing systems for use by its member agencies.
- **Analysis**—RISS center personnel create analytical products for investigative and prosecutorial use. RISS develops flowcharts, link-analysis charts, crime scene diagrams, telephone toll analysis reports, and financial analysis reports and provides computer forensics analysis. Staff also provide video and audio enhancement services.
- **Investigative Support**—Each center maintains a staff of intelligence technicians that support member agencies with a variety of investigative assistance. Staff conduct database searches, utilize all RISS applications, and process batch uploads. Intelligence technicians respond to thousands of requests and questions.
- **Field Operations**—Centers maintain field service coordinators who dedicate their time visiting and liaising with RISS member agencies to coordinate delivery of RISS services. This personal interaction with member agencies significantly improves information sharing and ensures that member agencies are provided quality and timely service.
- **Telecommunications**—RISSNET is the communications backbone that supports electronic access and exchange of information by RISS users. The network provides a secure platform for communications, as well as access to various state and federal intelligence systems across the country. RISSNET provides member agencies with a secure, rapid means to access RISS resources. In addition to RISSNET, several RISS centers operate long-distance telecommunications, or WATS services, to facilitate toll-free contact between RISS member agencies working jointly on investigations.
- **Equipment Loans**—Pools of specialized and surveillance equipment are available for loan to member agencies for use in support of multijurisdictional investigations.
- **Confidential Funds**—Member agencies can use funds to purchase information, contraband, stolen property, and other items of an evidentiary nature or to provide for other investigative expenses related to multijurisdictional investigations. The availability and use of confidential funds are strictly controlled by federal guidelines, and internal policies and procedures are developed by each center.
- **Training and Publications**—RISS centers sponsor or cosponsor meetings and conferences that build investigative expertise for member agency personnel. Subject areas include anti-terrorism, crime-specific investigative and surveillance techniques, specialized equipment, officer safety, and analytical tech-

niques. In addition, each center researches, develops, and distributes numerous publications, such as bulletins, flyers, and criminal intelligence publications. Centers also offer additional services based on regional and member agency needs.

Ms. HARMAN. I thank the witness.

We will now hear from our final witness, Mr. Parent.

Let me say that votes are expected soon. Hopefully, we will get through all the testimony. If there is more time before the votes are called, it is my intention—and I hope all the members will agree with this—to ask the godfather of this hearing, Mr. Langevin, to ask the first questions.

Mr. Parent, you are recognized for 5 minutes.

STATEMENT OF WAYNE PARENT, DEPUTY DIRECTOR, OFFICE OF OPERATIONS COORDINATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. PARENT. Good morning, Madam Chairman, members of the subcommittee. I am Wayne Parent, the deputy director of the Office of Operations Coordination at the Department of Homeland Security. I am pleased to appear before this subcommittee. Thank you for the opportunity to discuss the Homeland Security Information Network and to provide an update on the department's continuing efforts to improve information sharing with HSIN.

Before I begin my testimony, I would like to thank Congresswoman Harman for all of her efforts on information sharing. I know that you have been active in this arena for years, working to ensure efficient and timely vertical and horizontal information sharing. I look forward to working with you and the members of the subcommittee on a path forward for HSIN.

The DHS mission requires a robust information-sharing environment. Assorted efforts have been under way to connect the department with our stakeholders, the state, local, and tribal entities, the private sector and other federal partners. One of the most important tools DHS has to facilitate information sharing in the sensitive-but-unclassified environment is HSIN.

Although various issues have at times hampered the effectiveness and the use of HSIN, it remains an important tool in the fulfillment of the department's mission. Previously released GAO and DHS inspector general reports have called attention to many shortcomings, and action has been taken by the Office of Operations Coordination to address many of these recommendations. I have included specifics on those actions in my written testimony, but I would like to address just a few of the improvements that have been made to HSIN over the past year.

In response to concerns expressed by the DHS IG, the GAO and this subcommittee, we have instituted a strategy for the management of HSIN, as well as a requirements evaluation process. These are key elements of any program, but previously missing in HSIN.

Many of the previous criticisms of HSIN have centered on poor communication with stakeholders. We have established the HSIN Mission Coordination Council, or HMCC, to work HSIN issues within DHS. For stakeholders outside of DHS, just this week we released a solicitation for members to the HSIN Advisory Council, which will be a key body for collecting state, local and private-sec-

tor issues and recommendations. The first meeting of the HSIN Advisory Council will be held in August of this year.

Within the last month, we have hired a person to engage full-time on issues pertaining to the information-sharing environment. This will ensure that HSIN stays aligned with the efforts and recommendations of the ISE. In addition, this person will spearhead an effort to measure content quality within the key communities of HSIN.

The National Operations Center carries the DHS common operating picture on HSIN. This common operating picture, or COP, which was fielded last year in response to Hurricane Katrina lessons learned, is a key element of national incident management and provides critical situational awareness for stakeholders and DHS leadership during an incident. It includes pre-incident, obviously.

The COP has recently been upgraded to include the integrated common analytic viewer, or iCAV, a state-of-the-art GIS mapping package that has been strongly desired by our stakeholders going back several years in the state, local and private sectors. It is a good system. Within incident management, HSIN is the information-sharing tool that brings all of the DHS components and external partners together to maximize situational awareness and support decisionmaking.

Finally, we know that a system must be user-friendly, and HSIN has not enjoyed that evaluation. We have worked to improve customer service by establishing a single sign-on mechanism within HSIN, and also increasing the loading capability to prevent slowdowns on system time, and in also developing a more focused stakeholder outreach program.

This program also includes the addition of an automated feedback process, or feedback button, on the user portals which never existed previously. This system will be operational in August 2007.

I think it is important for me to state that DHS is committed to integrating HSIN with other interagency information-sharing systems. Our intent is for HSIN to leverage existing platforms designed to share information in order to increase information-sharing efficiency among our partner organizations and their existing systems. Our HSIN strategy is not to duplicate capability that already exists, but to leverage existing capability.

With the HSIN Joint Program Management Office and our new program manager, we are pushing ahead to ensure the ability and capability of HSIN to get relevant information to and from our stakeholders in a more increasing manner. As we look to the future, we will continue the pattern of recent program enhancements and outreach efforts. We recognize that work must continue to ensure increasing connectivity and interoperability with all of our DHS partners. We are committed.

Thank you for this opportunity to testify today, and I look forward to answering your questions.

[The statement of Mr. Parent follows:]

PREPARED STATEMENT OF WAYNE PARENT

Good morning, Madam Chairman, Ranking Member Reichert, and Members of the Subcommittee. I am Wayne Parent, Deputy Director of the Office of Operations Coordination at the U.S. Department of Homeland Security (DHS). I am pleased to ap-

pear today before this Subcommittee. Thank you for inviting me today to discuss the Homeland Security Information Network (HSIN) and to provide an update on the Department's continuing efforts to improve information sharing and HSIN.

The DHS mission demands a robust information sharing environment. Key to addressing information sharing requirements is the ability to share information both vertically and horizontally. Assorted efforts are underway to connect the Department with our stakeholders: state, local, and tribal entities, the private sector and other federal partners. One of the most important tools DHS has to maximize information sharing in the sensitive but unclassified environment is HSIN.

Background

As you are aware, HSIN is a set of commercially secure web-based portals through which DHS provides real-time operation information and decision support, shares documents, supplies situational awareness and collaboration opportunities, and provides alerts, warnings and notifications. HSIN operates at the Sensitive–But–Unclassified (SBU) level from which threat and incident management information is collected and shared between all levels of government.

Although complex issues have, at times, hampered the effectiveness and use of HSIN, it remains an important tool in the fulfillment of the Department's mission. Previously released GAO and DHS Inspector General Reports have called attention to certain shortcomings, and action has been taken by the Office of Operations Coordination to address their various recommendations. Specifically, in response to these shortcomings, Operations has, among other efforts:

• *Improved Management*

In November 2006, our office hired the first Program Manager (PM) for HSIN and stood up a Joint Program Management Office (JPMO). Since starting, the PM has created integrated project teams to establish programmatic discipline and to systematically address the network's development and use. The PM has initiated formal assessments of the system's vulnerabilities, redundancy, survivability and training. Additionally, the PM has identified key performance measures to gain a better understanding of the network's operation and use and guide future improvements. Of note, the PM initiated and completed an extensive review of HSIN, which I will discuss in more detail today. The review resulted in the creation of a HSIN Strategic Framework Implementation Plan.

• *Assessed the Policy and Strategy Framework for HSIN*

In October of 2006, the Office of Operations Coordination stood up the HSIN Working Group which conducted an internal review of HSIN and issued a final report that provided recommendations to DHS leadership on the required actions or decisions to make HSIN a more effective and efficient program. The working group was comprised of representatives from various DHS components. Key recommendations were:

(1) Establish clearly defined requirements processes;
(2) Develop HSIN into a capable information sharing, communication, and collaboration solution;
(3) Identify the user and technical requirements of HSIN; and
(4) Develop metrics to periodically assess the program

These recommendations formed the basis of the HSIN Strategic Framework Implementation Plan that was finalized in December 2006.

• *Created the framework for the HSIN Mission Coordinating Committee (HMCC)*

The HMCC consists of DHS mission component representatives who plan to or are currently utilizing HSIN to support their operation mission requirements. The goal of the HMCC is to identify and validate operational enhancements to HSIN that are critical to the successful accomplishment of the mission of DHS components and the external partners they represent. Through these efforts, we can plan for a prioritized delivery of solutions that meet mission-operational needs.

• *Create the HSIN Advisory Committee (HSINAC)*

A Federal Advisory Committee Act (FACA) compliant advisory committee is being formed to provide independent advice and recommendations to DHS leadership, particularly the Office of Operations Coordination Director, on HSIN requirements of end users within State, Local, Federal and Tribal governments and the Private Sector.

The advisory committee efforts will initially focus on: operational requirements necessary for effective information sharing and incident management; compatibility and interoperability between HSIN and other relevant information networks, databases, and resources of State, Local, Federal, Tribal, and Private

Sector entities; and the security, integrity, and safety of HSIN resources and contents.

The *Federal Register* notice announcing the formation of the HSINAC was posted on October 20, 2006. The *Federal Register* notice soliciting members for the committee was published earlier this week. Our goal is to have our first meeting of the advisory committee this summer.

Interagency Integration

The Office of Operations Coordination is committed to integrating HSIN with other interagency information sharing systems. The intent is for HSIN to leverage existing platforms designed to share information so as to increase information sharing efficiency among partnership organizations and their existing systems. As such, we are working to establish a technical means to seamlessly utilize information resident on other platforms. This enables HSIN to both serve the internal needs of DHS missions, while also addressing the convergence of DHS missions with those of other agencies.

Some of our current initiatives focused on interagency integration include:

Reestablish Connection between HSIN and RISS

The initiative to reconnect the technological bridge between the HSIN and the Regional Information Sharing System (RISS) is nearing completion. In June 2006, when HSIN completed a technology refresher that moved HSIN from the old JRIES technology platform to its current platform, the bridge was inadvertently severed and not reconnected. Reconnecting this bridge will allow pre-defined information to automatically flow back and forth between the two systems.

Additionally, the original agreement between HSIN and RISS only allowed for very narrowly defined information to be passed between the systems. This definition mandated that the content be specifically identified as terrorism information. We are working to incorporate a more liberal, flexible definition such as suspicious activity that may later be deemed terrorist related. The expansion of content will enhance information delivery over a single platform; maximizing the usefulness of both systems.

Intelink-U

HSIN will provide a link to Intelink-Unclassified, affording access to the content and contacts available on this online compendium of resources. Intelink-U is well-used content repository. This enhancement will provide a broad range of relevant information to HSIN users who may not have another way to access this valuable resource.

Federated Identity Management

The JPMO is actively involved in an Office of the Program Manager-Information Sharing Environment (PM–ISE)-sponsored, Department of Justice-led pilot project for Federated Identity Management. Federated identity management is a systematic effort to create a single sign-on for multiple secure websites. Our office understands the long-term possibilities and benefits of this pilot and is committed to the effort.

Federated identity management will allow authorized HSIN users to seamlessly traverse other participating programs' systems, gaining access to content and tools that are not available on HSIN. It will also permit other authorized system members to gain access to the tools and content on HSIN. This is a significant step in the direction of eliminating duplication and maximizing existing systems across the entire landscape of the ISE. HSIN, Law Enforcement Online (LEO), and RISS are all participants in this groundbreaking pilot. Once identity management has been federated—including federation to the state fusion centers and critical infrastructure Sector Coordinating Councils—it will provide a basis for such advanced capabilities as fine-grained dissemination control based on the recipient's identity, role, and organizations/communities to which the recipient belongs.

Data Exchange Hub

The Office of Operations Coordination is working towards an initial operating capability between HSIN and a Data Exchange Hub (DEH) that connects the National Capital Region's emergency management systems. The DEH will enable a two-way transfer of information between multiple reporting systems within the NCR (to include WebEOC) with HSIN. The success of this initiative is expected to result in a repeatable process that can be used throughout the nation to connect HSIN to emergency operation centers that use different communication platforms.

HSIN Utilization

Over the past nine months, numerous improvements and enhancements to HSIN have been made and I believe it has the potential become the information sharing and situational awareness tool it was envisioned to be. For instance, DHS National Operations Center (NOC) notifications, which alert leadership and key stakeholders when incidents occur, are posted on HSIN through the COP. Additionally, HSIN supports the National Incident Management System (NIMS) by becoming the primary national hub for communications and information during major domestic incidents.

An increased number of DHS components are now using HSIN extensively in the execution of their mission. The Federal Emergency Management Agency (FEMA) has integrated the tool in all emergency management coordination and has conducted extensive training across the nation. The United States Coast Guard has begun to use the tool as its primary coordination tool for exercises and missions that require large-scale, real-time collaboration. In addition, Customs and Border Protection (CBP) has constructed collaboration space for each of its 27 border patrol sectors to enhance seamless information flow and situational awareness. Data currently shows that CBP is making daily use of this tool.

HSIN is also an important tool for information sharing between state, local, tribal, and private sector communities. The network is also actively embraced by state and local fusion centers across the country, many of which have created their own customized portals. For example, in the State of Tennessee, the Director of the Office of Homeland Security has cited HSIN as the backbone of its new state fusion center and recommended that all states adopt the network for information sharing and situational awareness. As I believe you will hear from additional testimony today, The State of Florida is also an active user of the system.

One of the most valuable tools on HSIN is the Common Operating Picture. HSIN and COP will be increasingly relied upon as the Department continues with a number of important initiatives, in particular, interagency planning and exercises. The COP is a real-time, web-based situational awareness tool that ties together key homeland security partners primarily at the federal, state, and Joint Federal Official (JFO) levels. It is designed to:

- Provide a common view of critical information during a crisis in order to enhance situational awareness;
- Support sound, timely, risk mitigated and informed decision making by providing a shared understanding of the situation;
- Provide the inter-agency with the capability to share critical information;
- Provide information integrity for reporting requirements; and
- Support a geospatial mapping feature known as iCAV—the infrastructure critical asset viewer—that can overlay events such as hurricanes onto critical infrastructure assets.

The COP was initially deployed during Hurricane Season 2006. As such, the focus of the early iterations of the COP was on natural disaster information. Currently, as part of our incremental approach, we are advancing the COP capabilities from natural disasters to all hazards and all threats. These steps will advance the COP capabilities from unclassified, hurricanes/natural disasters to classified, terrorist threats and incidents. The current focus is to develop a COP template for the "worse case" scenario for nuclear/radiological incidents and will use national exercises such as Ardent Sentry and real world events to validate and continue this development.

While initially focused on integrating natural disaster information, DHS activated the COP for several non-natural disaster incidents, including the liquid explosive airline plot in the UK and the private airplane crash in New York City.

Additionally, the National Infrastructure Coordination Center (NICC) utilizes the HSIN-Critical Sectors (HSIN–CS) portal to share information about the nation's infrastructure with private sector stakeholders. DHS has designated HSIN–CS to be its primary information-sharing platform between the Critical Infrastructure/Key Resource sectors. HSIN–CS enables DHS and the critical sector stakeholders to communicate, coordinate, and share information. Through HSIN–CS, users are able to:

- Receive, submit, and discuss timely, actionable, and accurate information;
- Communicate information pertaining to threats, vulnerabilities, security, response and recovery activities affecting sector and cross sector operations; and
- Maintain a direct, trusted channel with DHS and other vetted sector stakeholders

The primary objectives of HSIN–CS are to generate effective risk management decisions, and to encourage collaboration and coordination on plans, strategies, protective measures, and response/recovery efforts between government, operators, and owners.

HSIN's Way Ahead

Building on HSIN successes, lessons learned, and various recommendations from outside review, the Joint Program Management Office is pushing ahead to ensure that we get relevant information to more of our stakeholders more of the time. As we look to the future, we will continue the recent program enhancements and outreach efforts. Additionally, system enhancement will continue by examining and taking action on additional measures. The JPMO will:

- Assess, and act upon, results from metrics designed to measure a number of aspects of the overall program regarding the effectiveness of information sharing across HSIN. Some areas to be assessed include: the number of users, timeliness of information posted, response times for requests for information, numbers of outstanding and closed action items, and comments posted through the system feedback mechanism.
- Ensure DHS components become more involved in the development of HSIN capabilities, articulate their mission needs as well as the needs of the external partners they sponsor, create a governance structure within their mission areas with regard to HSIN use, and become active participants in shaping the future of the program;
- Evaluate advanced information technologies for incorporation into HSIN such as tools for multi-party real-time collaboration/co-authoring and fine-grained dissemination and user access control to sensitive information products.
- Work with the PM–ISE and the Information Sharing Council to improve business processes and contribute to an Information Sharing Environment that eliminates current "stove-pipes" between programs;

T3Conclusion

HSIN plays an important role in the information sharing mission of DHS. Additionally, it is critical that all agencies and components are able to monitor HSIN/COP for up-to-date event/threat information when notified via NOC Notification.

HSIN is the information sharing tool that brings together all DHS components and external partners to maximize situational awareness.

Without HSIN, the ability of the Department to share information would be degraded.

Work needs to continue to ensure there is robust connectivity and interoperability with all DHS partners. This is an obtainable goal that will be achieved through methodical, thoughtful collaboration and planning.

HSIN, in conjunction with the COP, is becoming the Department's solution to address the ever-growing need to gather, assess, and share information critical to the Department's overall mission.

Finally, as we improve the HSIN technology and core functionality, we will focus on customer involvement and user satisfaction. Our goal is to improve overall collaboration and situational awareness among Federal, State, Local, and private industry partners.

HSIN is playing a critical role in the Ardent Sentry and Pinnacle exercises that are currently underway. In these instances, HSIN and the COP are being utilized for situational awareness and information sharing.

Thank you for this opportunity to testify today and I look forward to answering your questions.

Ms. HARMAN. I thank the witness. He is in a tough position on this panel. I do appreciate the fact that you see this as a collaboration. We do want to be your partners in fixing the problem. That is our goal.

I now recognize our colleague, Mr. Langevin, for 5 minutes of questions.

Mr. LANGEVIN. Thank you, Madam Chair.

I want to thank the panel for being here.

Before I begin with my questions, I just want to thank you, Madam Chair, for holding this hearing and for focusing on this issue, which is of great importance.

It is worth noting that the chair until just recently served for a number of years on the House Permanent Select Committee on Intelligence, and served for most of that time as ranking member of

the Intelligence Committee. There is not a person in the Congress who understands the importance of good intelligence more than Congresswoman Harman.

On that, you and I are in lock-step. Again, I thank you. It is no surprise that you would be holding this hearing so early as chair of this subcommittee. It is a great service to the country, and I appreciate it.

I also, again, want to thank the panel.

Ms. HARMAN. We won't take that out of your time.

Mr. LANGEVIN. Thank you very much, Madam Chair.

[Laughter.]

I want to thank the panel for being here.

Mr. Powner, thank you for issuing and conducting this very important report. GAO is to be commended. You are focusing on issues that I have tried to raise now for a number of years. In particular, Don Kennedy and I have had the opportunity to speak on several occasions, going back over a number of years.

Again, I thank you all for being here.

I know that the focus of the hearing is moving past the missteps, but I think a certain amount of history is necessary here for context. In March of 2002, when I was first briefed by Mr. Kennedy and his team, about the RISS program, and actually went to RISS in Massachusetts and saw it first-hand for myself. I was certainly impressed with its information-sharing capabilities. I thought it could be the backbone for a national information-sharing network for the homeland security of the nation.

In September of that year, I met with Tom Ridge, then secretary, or actually director of homeland security—later to be secretary—to recommend that RISS be used as a tool for the federal government to disseminate information for first responders and law enforcement. He seemed receptive and said he would look into it.

Later in July of 2003 at a Homeland Security Intelligence Subcommittee hearing, I informed Bill Parrish, DHS's acting assistant secretary for information analysis, about my meeting with Secretary Ridge, and asked for an update of how DHS was working with RISS. In the 4 years since then, I have discussed RISS numerous times with DHS officials, so its existence and capabilities should not be a surprise at all to DHS.

Given that history, I was extremely frustrated to read Mr. Powner's report, and learn not only that HSIN and RISSNET are not fully interoperable, but also that they are in many cases duplicative. It is certainly not a surprise to me. We have spent tens of millions of taxpayer dollars to create HSIN, yet it falls far short of what it should accomplish.

Now, I know that Mr. Parent cannot speak to some of the mistakes that were made before his tenure, but I have to ask why DHS did not make it a priority from day one to ensure that HSIN would be fully compatible with RISSNET and other information sharing networks.

My second question for Mr. Kennedy, RISS has been in existence since 1974, and reaches more than 7,500 law enforcement and criminal justice agencies. I would like to just have you take a few minutes to describe how and why RISS has been such a success.

So with that, Mr. Parent?

Mr. PARENT. Yes, sir. What I can give you is the history of the relationship between RISS and HSIN, as I know it, and I am very certain it is correct. There was a relationship that resulted in a technological connection between RISS and HSIN that occurred sometime within the dates that you talked about and last June 2006. Last June 2006, which is about the time that my involvement with RISS and HSIN, and my involvement with HSIN goes back a little bit further, that connection was severed when HSIN went through an upgrade process in 2006. So that is the first point that the present group of people had to look at that issue.

We are now re-fixing that technological connection between RISS and HSIN that Mr. Kennedy talked about, but I would also like to emphasize what he said which is that is only the first step. That is, in essence, a gateway that will allow documents to flow back and forth between the two systems. But I think we both have a bigger expectation of what this is going to go than just documents going back and forth.

We have identified that the previous technological connection was very restrictive in terms of what documents went back and forth between the two systems. Our goal at this time is to open that conduit up substantially. But I think this is the beginning of a new relationship, or certainly a much better relationship. That is what I know about the history.

Mr. LANGEVIN. Thank you.

Mr. KENNEDY. Thank you, Congressman Langevin.

To answer your question, I believe that the success of RISS lies in the fact that we are run by state and local and tribal law enforcement. We are funded through the federal government, but our executive policy boards are the colonels and the chiefs of police that we serve throughout the United States.

I also believe that it is that regionality that we have, that actually we work with our users and we are user-driven. So if we have a system, we don't just give them a system; we sit our members down in a group and ask them for their input as to what they would like in a system, and then that is how we developed RISSNET.

Whatever program that we do or whatever service we provide, whether it be camera equipment or to develop a database for them, it is for the users, and they are the ones that usually come to us, and we try to provide them with that service.

But I think the most important thing is that we are not in competition with any agency, whether it be state, local or federal. I am sorry. We are not in competition with any agency or system. We are like Switzerland. We want to get along with everyone. We believe that if our members have a need for information, wherever it resides, that we at RISS have to find a way through interoperability with systems like HSIN and LEO to get that information to our members, because it is bi-directional.

Mr. LANGEVIN. Thank you. My time has expired.

I thank the chair for her indulgence, and thank you for your testimony.

Ms. HARMAN. Thank you, Mr. Langevin.

We will now move to Mr. Perlmutter. We are sort of recognizing people in the order of arrival, and then Mr. Carney.

VerDate Nov 24 2008 10:59 Jun 24, 2009 Jkt 000000 PO 00000 Frm 00032 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-34\48909.TXT HSEC PsN: DIANE

There will be a long recess for about six votes or so. It is coming up shortly. Hopefully, all three of you can ask your questions before we do that recess. And then what I think I might do, if it works out that way, is forego my own questions. I think you have all heard from me. And we will move to our next panel after the recess.

Mr. Perlmutter, 5 minutes.

Mr. PERLMUTTER. Thanks, Madam Chair.

Just thinking about this over the last few days, there are different kinds of approaches here, if I understand it correctly. The HSIN system is a centralized system where there is somebody at the top. The RISS system is a decentralized system where you have a board of law enforcement for a particular region—the Rocky Mountain West or the Northeast.

And so, to you, Mr. Kennedy, and to you, Mr. Parent, and then Mr. Powner if you want to jump in, how do we best get information? We talked about it. The ultimate goal here is the safety and security of the citizens of the United States of America within the bounds of the Constitution. The next level up is law enforcement. How do we best provide them information that makes me and my neighbors secure in Golden, Colorado?

Mr. Parent? Am I wrong in describing one as a centralized kind of system and the other as a decentralized system?

Mr. PARENT. It is very hard to put HSIN into any normal category like that. What you said is correct, sir. It is central in that DHS is at the center of it, but HSIN is basically a series of communities. The communities include some law enforcement members, but they also include a large contingent of emergency management people, an international community, the private-sector people in the critical sector connections, and a few others that kind of represent this family.

I agree with your goal completely, and I think all of us recognize the fact that we inherited or we have a series of what we can call "communities," but they are enclaves out there, and the enclaves all need to be connected. They need to be connected in any way of communication that is presently being utilized to share information, whether that is chat, email, whether that is documents going back and forth.

And that is our goal right now, is to, one, acknowledge that we at least have the communities. We have the people who have stepped up to the plate to participate in this grand information-sharing endeavor. It is our job to connect all of them.

Mr. PERLMUTTER. Mr. Kennedy?

Mr. KENNEDY. Thank you.

I wouldn't say that RISS is decentralized. We work individually in the regions with our network, but it is a national network. We have one IT. We call it the Office of Internet Technology that oversees all of the RISS programs as it relates to RISSNET. We also have all, like I said, state, local, federal and tribal systems that are online with us. We interconnect with many of the systems that I have actually briefed in my nine-page brief that is before you.

But to answer your question, I think that what we need to do to continue this dialogue is we need to probably set up some type of an executive steering committee made up of the policymakers

and the leadership of Homeland, DOJ, and RISS and others, and then maybe have someone that is the chairman of that particular steering committee—maybe the program manager from ISE or someone from Global—so that we can ensure that these meetings will continue so that the information that law enforcement and first responders need, you know, that comes from these systems that work independently of one another, can work together to try and make sure that that information doesn't slip through those cracks, and then incidents like that that happened in New Jersey don't fall by the wayside.

Mr. PERLMUTTER. And I guess I can see some instances where we have to take information from the top and push it down, and then others where there is information from the bottom and push it up to the top—to do it as quickly as possible to minimize whatever the damage might be on some kind of bad guy out there who wants to do harm to Golden, Colorado.

So for $300 million per year, what is it that I am actually getting out of HSIN?

Mr. PARENT. HSIN is not a $300-million-a-year program. In the entire life of HIS, we have spent $71 million, sir, and right now it is budgeted at about $20 million or $21 million per year. The $300 million is a number that I think includes a number of other DHS systems that are not part of HSIN or connected with this directly.

Mr. PERLMUTTER. Thank you.

Ms. HARMAN. The time of the gentleman has expired.

We will now hear from Mr. Carney for 5 minutes for questions. Following that, this panel will be adjourned. I am intending to come back during votes, during the motion to recommit, to convene the second panel. Unfortunately, this is a crazy day, so that we can get their testimony on the record.

If some of you can come back, that will be great.

Mr. Carney?

Mr. CARNEY. Thank you, Madam Chairman. Once again, thank you for your leadership.

And my good colleague, Mr. Langevin, thank you so much. It is absolutely critical to get through this and get this fixed.

Mr. Parent, DHS had an opportunity to comment on the GAO's report. The GAO obviously said that there is a lot of duplication going on. Do you agree with that?

Mr. PARENT. I agree with it, and Mr. Powner and I have talked, as well as our staffs have worked on this report together from the time the first draft came out in January. There is some truth in there. There are some functions that take place within the HSIN system that are very, very similar, dealing with the same kind of people and the same kind of information.

But it is not and either/or-type situation. If you today said, "Stop HSIN; pull the plug; save the $20 million; everybody use RISS," that couldn't work. RISS does not have a common operating picture. It doesn't have the information flow templates and process that we put into place for incident management. It also doesn't have all the same people. So there is a little bit of apples and oranges there, but it is true to say that at some point there are groups of the same type of people getting onto two different systems that are doing similar things.

Mr. CARNEY. What percentage of HSIN do you think is unique, compared to what else is out there? Compared to RISS or LEO?

Mr. PARENT. I think the incident management piece is completely unique. I think the private-sector piece is completely unique. The law enforcement piece is the one where there are obviously other systems that are frequently compared as the GAO did, RISS and LEO being the two biggest systems. But some of the states have systems that they have put together that are obviously just state-centric that are also very similar.

Mr. CARNEY. But on a percentage basis, could you give me a rough estimate?

Mr. PARENT. I think the law enforcement piece on HSIN, and let me use the number of authorized users. We have about 17,500 authorized active users today on HSIN. About 4,000 are law enforcement members of HSIN–LE.

Mr. CARNEY. Okay. Nothing further. We should go vote.

Thank you.

Ms. HARMAN. Thank you, Mr. Carney.

That was the 10-minute bell, so I do think we need to move.

I would just say to Mr. Powner—in fact, I will stay around for another minute or so, and I haven't asked questions—I would like to ask you to comment on the answers to prior questions, including the answer to the budget question.

How much money, in GAO's opinion, has been spent on these different systems? And going forward, if we were able to rationalize this more efficiently, how much money would it cost and how much money would we save?

Mr. POWNER. Collectively, when you look at roughly 10 homeland security information networks and applications at DHS, the annual amount spent is around $300 million. If you look at HSIN in particular, between 2004 and 2007, we have spent about $75 million.

Now, in terms of going forward—and we had this discussion about in terms of what is duplicative and what is not duplicative—I wouldn't use the word that it is completely unique, because I think even in some of those areas that Mr. Parent referred to, there still is some duplication that occurs in some of those areas.

The important thing moving forward is because we have some users now tied to HSIN—they like HSIN better than RISS, and some folks like RISS better than HSIN—the important thing moving forward is how do we integrate these applications and leverage them. But a couple of things to reinforce: One, we need to start with requirements. What are the users' needs?

There are committees set up. It is very important that these committees actually identify the key users. No matter what the community is we are focused on, we need to make sure we get the right user needs and we proceed forward with that. We need to built out the content so that users are more inclined to use this. The key is linking these applications and perhaps others so that we leverage and we don't duplicate going forward.

The program management of HSIN clearly needs improvement, according to OMB. I think Mr. Parent and I have discussed that. There are many efforts to do that. And then we talked a lot about the technical integration that needs to occur. Coupled with the technical integration, you probably want policies and strategies, be-

cause I think what you heard here is executive governance that would help, where we actually have some policies in place so that we know what the ground rules and game plans are. That can be done through MOAs and MOUs and those types of things.

Ms. HARMAN. Thank you, Mr. Powner. I think you have the last word.

This panel is dismissed. I should say for the record that your testimony will be included in the record in full. Without objection, so ordered.

I would like to thank our colleagues and again commend Mr. Langevin—he wasn't here when I said this—for asking a question in 2002 that we are finally getting the answers to in 2007. It took a while. I thank you for your patience.

And I say to our panelists, we have a lot of work to do together. In real-time, we could be attacked at any moment. It is absolutely critical that information be shared efficiently, and that those who are protecting our hometowns get what they need and can communicate what they need, so that we can prevent, hopefully, or disrupt the plans of those who would harm us.

I will be back shortly during this series of votes to convene the second panel. Hopefully, other members can return as well.

Thank you very much.

[Recess.]

Ms. HARMAN. Hello, everybody. I would like to call up our second panel of witnesses. Thank you.

Welcome to all of you, and apologies for this crazy schedule, but that is what we have today.

I did talk to the ranking member, Mr. Reichert, and he will try to make it briefly. We are in between votes, which I think you all understand, so the goal here will be to convene this panel, to get your testimony in the most abbreviated form, to see whether we can proceed with questions. If that is possible, we will do it, but we are all trying to do all the things that are required this morning.

So I welcome the second panel of witnesses.

Our first witness is Captain William Harris, a 26-year veteran of the Delaware State Police. Captain Harris presently serves as the officer in charge of his agency's criminal intelligence section. His command includes the Delaware State Police electronics surveillance unit, the high-tech crime unit, intelligence investigations, and the Delaware Information and Analysis Center, the DIAC, the Delaware Fusion Center that has been operational since December of 2005.

I am going to skip over some other aspects of your bio to get us going.

Our second witness is First Sergeant Lee Miller, a 13-year veteran of the Virginia State Police, who manages the day-to-day operations of the Virginia Fusion Center. First Sergeant Miller is intimately familiar with that center, having been involved in the working group that led to its creation and the policies and procedures that govern it.

I want to thank you, sir, for the work that you did during the horrible massacre at Virginia Tech. We have heard from others

that that work was widely shared and was very critical in giving needed information to other fusion centers around the country.

The third witness is Inspector Barry Lindquist. Inspector Lindquist has a law enforcement career that exceeds 37 years. This career includes 28 years with the Pompano Beach Police Department, with 22 years as a supervisor, including 12 years as a command-level officer. Inspector Lindquist has worked with the Florida Department of Law Enforcement since his retirement from Pompano Beach in 1998 as a police captain.

Our fourth witness is Major Brian K. Tomblin. Major Tomblin, Tennessee Army National Guard, is the military liaison to the Tennessee Office of Homeland Security. Major Tomblin coordinates military resources and response for the Tennessee National Guard in support of the Tennessee Office of Homeland Security and local authorities. As the program manager for HSIN–Tennessee, Major Tomblin manages the portals and coordinates training of Tennessee users.

I think we will start our testimony right now with Captain Harris. If you can summarize in less than 5 minutes, your nation would be grateful.

Let me just add that, in all cases, your written testimony will be included in the record in full.

STATEMENT OF CAPT WILLIAM HARRIS, DELAWARE STATE POLICE

Captain Harris. Okay. Good morning. First of all, thank you for having me. I am very humbled that you would ask us as a group, and particularly me, for our opinion on such important matters.

My name is Captain Bill Harris. I am with the Delaware State Police. I am in charge of the criminal intelligence section and the Delaware Information Analysis Center, Delaware's state fusion center. I have been asked to give you state law enforcement's perspective on the information sharing culture as it pertains to our counterterrorism efforts.

I will specifically speak about the duplication of efforts in federal agencies that not only hamper our efforts at effective information sharing, but also hamper our efforts to secure our state and our nation from future terrorist activity and attack.

I would first like to preface my comments that I have had positive experience with professionals from both the Department of Homeland Security and many with the Department of Justice, particularly with the Bureau of Justice Assistance. As the commander of our state's fusion center, I am thoroughly familiar with the Department of Justice, the Department of Homeland Security's unclassified-but-sensitive information sharing systems.

I would particularly like to speak about the duplication of efforts between the Homeland Security Information Network, RISS, the regional information-sharing system, and LEO, to include INFRAGARD.

The RISS network was established in 1974 and has been a staple of federal, state and local law enforcement information sharing for over 30 years. In 2002, RISS launched new assets with the Automated Trusted Information Exchange. This new asset was to enhance the information-sharing environment with those non-law en-

forcement, homeland security stakeholders, within their own discipline, cross discipline, and their local, state and federal law enforcement partners.

Each of the previously mentioned systems offer similar capabilities, such as an electronic bulletin board, document library, a chat tool, and encrypted email. As a law enforcement agency participating in the information-sharing environment, we are forced to choose between information-sharing systems with separate logons and passwords, and the monitoring of those systems. Because of this bureaucracy of multiple systems, our personnel have had to monitor all of these systems at once in an attempt to stay current on the sharing of counterterrorism information and homeland security information.

This has also forced law enforcement agencies such as mine to look at the bes6t information-sharing resources available. This has been by far the regional information sharing system, or RISS. This system is both robust, user-friendly, contains more relevant, reliable and timely law enforcement and homeland security information that is actionable for the line-level law enforcement personnel, that will most likely identify the link to disrupting pre-operational planning of a domestic or international terrorist.

Ms. HARMAN. Captain Harris, I hate to interrupt you. It has been 3 minutes, and it is not that we didn't tell you 5 minutes, but I want to give everyone a chance. You have a made a point that I think is enormously important for our record.

Is there one more sentence you would like to tell us?

Captain Harris. Yes. The difference in the systems, ma'am, particularly with the private sector and other stakeholders. RISS or ATIX has no portals. They share cross-sector information across discipline information. Where HSIN, separate from the law enforcement side, has different portals. It doesn't allow for that information sharing that might be important to public health, and may also be important to agriculture.

[The statement of Captain Harris follows:]

PREPARED STATEMENT OF CAPT WILLIAM HARRIS

I am commander of the Delaware State Police's, Criminal Intelligence Section and the Delaware Information and Analysis Center (DIAC), Delawares state fusion center. I have been asked to give you state law enforcement's perspective on the information sharing culture, as it pertains to our counter-terrorism efforts.

I will specifically speak about the duplication of efforts by federal agencies that not only hamper our efforts to effective information sharing, but also hamper our efforts to secure our state and nation from future terrorist activity and attack.

I would like to preface my comments that I have had positive experiences with professionals from both the Department of Homeland Security, and many with the Department of Justice, particularly the Bureau of Justice Assistance.

As the commander of our state's fusion center, I am thoroughly familiar with the Department of Justice and Department of Homeland Security's unclassified, but sensitive information sharing systems. I would particularly like to speak about the duplication of efforts between the Homeland Security Information Network (HSIN), the Regional Information Sharing System (RISS), and Law Enforcement on Line (LEO), to include INFRAGARD.

The RISS network was established in 1974 and has been a staple of federal, state, and local law enforcement information sharing for over 30 years. In 2002, RISS launched new assets with the Automated Trusted Information Exchange. This new asset was to enhance the information sharing environment with those non-law enforcement, homeland security stakeholders, within their own discipline, cross discipline, and their local, state, and federal law enforcement partners.

Each of the previously mentioned systems offer similar capabilities such as an electronic bulletin board, document library, a chat tool, and encrypted Email. As a law enforcement agency participating in the information sharing environment, we forced to choose between information sharing systems with separate logons and passwords, and the monitoring of those systems. Because of this bureaucracy of multiple systems, our personnel have had to monitor all of these systems in an attempt to stay current on the sharing of counter-terrorism and homeland security information.

This has also forced law enforcement agencies, such as mine to look at the best information sharing resource available. This has been by far the Regional Information Sharing System (RISS). This system is both robust, user friendly, and contains more relevant, reliable, and timely law enforcement and homeland security information that is actionable for the line level law enforcement personnel, that will most likely be the identified link to disrupting pre-operational planning of a domestic or international terrorist.

The RISS network gives access to an electronic bulletin board (RISS Leads) used by multiple law enforcement agencies, to include a national criminal intelligence database (RISS Intel) to include gangs (RISS Gang). In addition to this RISS has connectivity to assets such as the High Intensity Drug Trafficking (HIDA) Centers (19 databases), the National White Collar Crime Center, the U.S. Secret Service's Targeted Violence Information Sharing System (TAVIS database), the Law Enforcement Intelligence Unit (LEIU database), the El Passo Intelligence Center, (EPIC database), the National Drug Pointer Index (NDPIX database), to name just a few. These features are the force multiplier that law enforcement agencies and fusion centers are searching for to assist in identifying anomalies and those common crimes and networks that are part of pre-operational planning by both domestic and international terrorist.

Duplication of systems within the information sharing environment with the public and private sectors are just as confusing and bureaucratic. HSIN has several portals for this purpose, the FBI is promoting INFRAGARD as a communication tool, and RISS has the Automated Trusted Information Exchange (ATIX). The concept of including the public and private sector are part of the Information Sharing Environment Implementation Plan, and makes good business sense to include these disciplines. However, when working with our critical infrastructure stakeholders in the private sector, they are presented with three systems that are supposed to accomplish the same goal.

Once again, state and local law enforcement, which have responsibility for protecting our critical infrastructure, are forced to choose the best information sharing resource available. This has been by far the RISS ATIX system, for many of the same reasons law enforcement likes the features of the RISS law enforcement network. The information, contacts, and features available on the ATIX system make it more robust and user friendly. Additionally, like HSIN, users have the ability to go into their identified "communities" or disciplines, however unlike HSIN and INFRAGARD; users have the ability to gather information and contacts from users outside of their discipline, giving them relevant, reliable, and timely information sharing relationships of mutual value. This was most evident recently in February 2006, when DHS released the "lessons learned" from "Cyber Storm," a cyber security preparedness exercise. One of the key lessons learned, was to no one's surprise, that interagency coordination and cross-sector information sharing enhanced overall coordination, communication, and response.

RISS ATIX gives our law enforcement personnel and key stakeholders within our state and region this type of effective information sharing capability that no other system does.

Ms. HARMAN. Let me thank you for that.

We are moving right now to Sergeant Miller.

We are going to continue to call on all of you, because we want this whole reform effort to start with you, not end with you. You should have been incorporated in the first place. If the RISSNET turns out to be much more user-friendly and helpful, I don't want to imagine what our final conclusion will be, but you should bet on the fact that we want to be useful and helpful to you.

Sergeant Miller?

STATEMENT OF 1stSgt LEE MILLER, VIRGINIA STATE POLICE

Sergeant Miller. Good morning, Madam Chairman.

The primary mission of the Virginia Fusion Center is to fuse together key resources from local, state and federal agencies, as well as private industry, to facilitate information collection, analysis and sharing in order to prevent and deter a terrorist attack and all other forms of criminal activity.

After the September 11, 2001, terrorist attacks, law enforcement agencies were forced to meet the information demands created by the increased focus on terrorism. As a result, the resources needed to provide proactive intelligence operations have increased exponentially, thus compelling law enforcement agencies to consider the concept of a fusion center.

In order to meet our mission, the Virginia Fusion Center utilizes a vast array of networks and databases to assist in the fusion process. These separate systems provide information and intelligence relevant to situational awareness, as well as providing the ability to identify trends, patterns, and targets that enhances the ability of law enforcement to be proactive instead of reactive.

Some of the networks that the Virginia Fusion Center monitors during our day-to-day operations are HSIN, of course, LEO, FPS Portal, HSDN, RISSNET, JRIES, and systems developed by the Commonwealth of Virginia. As stated in previous reports, the number of systems that are available causes duplication and does not promote an effective business process.

These systems also provide the Virginia Fusion Center an avenue for disseminating information and intelligence to our different partners. In order to reach all of our partners, our information must be submitted to multiple networks and systems, thus creating another area of duplication and operational ineffectiveness.

On March 24, 2006, the Department of Homeland Security's Office of Intelligence and Analysis initiated the homeland security information network, HSIN–Intel. This was a 3-month pilot effort of multi-directional sharing assessments between state and local intelligence professionals and the Department of Homeland Security's Office of Intelligence and Analysis, of timely, accurate, actionable information at the unclassified, for-official-use-only level.

This pilot gave local and state officials the opportunity to provide input into the business process, as well as the functionality of the system, and a steering group comprised of local and state officials wrote and approved the charter. This pilot was extended for a second 3 months, and then the steering group recommended turning this into an operational community of interest.

This collaborative effort between state and local created a true community of interest that encompassed a usable network of intelligence professionals, analyst-to-analyst collaboration, and a continuing partnership between local, state and federal intelligence communities. This community has created trust relationships that ultimately is a more powerful tool than any network or portal, and these relationships will remove the resistance to sharing information that has plagued government response in the past, thereby pooling together information form all pertinent intelligence sources to effect a decisive response.

This community of interest now has 14 member states, and it is expected to double by the end of this fiscal year, and is a perfect example of local, state and federal agencies working together in an effort to meet the needs of all those involved.

Recommendations. In order to be a true intelligence-led policing model, local, state and federal analysts must be able to see all information and intelligence. If analysts are provided only a couple of pieces of the puzzle, we will never be able to see the overall picture. Local, state, tribal and federal agencies, as well as private industry, have individual pieces, and we must have an IT mechanism, as well as trusted relationships, to put these pieces together.

Currently, state and local analysts are provided access to a wide range of unclassified systems, to include some of the ones that I spoke of before, but we have limited access to classified systems such as the homeland secure data network. Local, state and federal unclassified initiatives must be incorporated to meet the needs of everyone involved in homeland security and to improve operational effectiveness. Local and state intelligence professionals must also be given the same opportunity as their federal counterparts regarding the access to classified systems.

[The statement of Sergeant Miller follows:]

PREPARED STATEMENT OF 1STSGT LEE MILLER

Good morning Mr. Chairman and distinguished members of the Subcommittee.

My name is Lee Miller and I am a 15-year member of the Virginia State Police. I currently coordinate the day-to-day operations of the Virginia Fusion Center. Thank you for the opportunity to testify today regarding the Homeland Security Information Network. There have been several reports written regarding the numerous federal networks that are available to promote information sharing among local, state, and federal agencies and private industry. These reports discussed practices that were not utilized in the implementation of the Homeland Security Information Network and recommendations to improve coordination between the Department of Homeland Security and local and state initiatives. In my testimony, I will discuss some of these issues, but I will concentrate on collaborative efforts that will enhance information sharing as well as Department of Homeland Security initiatives that have produced positive results in order to move towards a better information sharing platform.

The Primary Mission of the Virginia Fusion Center is to fuse together key resources from local, state, and federal agencies and private industries to facilitate information collection, analysis, and sharing in order to prevent and deter terrorist attacks and all other forms of criminal activity. The secondary mission of the Virginia Fusion Center is to support the Virginia Emergency Operations Center by centralizing information and resources to provide a coordinated and effective response in the event of an attack or natural disaster. After September 11, 2001 terrorist attacks, law enforcement agencies were forced to meet the informational demands created by the increased focus on terrorism. As a result, the resources needed to provide proactive intelligence operations have increased exponentially, thus compelling law enforcement agencies to consider the concept of a Fusion Center.

In order to meet our mission, the Virginia Fusion Center utilizes a vast array of networks and databases to assist in the fusion process. These separate systems provide information and intelligence relevant to situational awareness as well as providing the ability to identify trends, patterns and targets that enhances the ability of law enforcement to be pro-active instead of re-active. Some of the networks that the Virginia Fusion Center monitors during our day-to-day operations are the Homeland Security Information Network (HSIN), Department of Justice's Law Enforcement Online (LEO), Federal Protective Services Law Enforcement portal, Homeland Secure Data Network (HSDN), Regional Information Sharing System Network (RISSNET), Joint Regional Information Exchange System (JRIES) as well as systems developed by the Commonwealth of Virginia. As stated in previous reports, the number of systems that are available causes duplication and does not promote an effective business process. These systems also provide the Virginia Fusion Center an avenue for disseminating information and intelligence to our different

partners. In order to reach all of our partners, our information must be submitted to multiple networks and systems thus creating another area of duplication and operational ineffectiveness.

Moving Forward

On March 24, 2006, the Department of Homeland Security's Office of Intelligence and Analysis (I&A) initiated the Homeland Security Information Network State and Local Intelligence (HSIN-Intel) Community of Interest (COI). This was a three month pilot effort for the multi-directional sharing assessments between state and local intelligence professionals and Department of Homeland Security's Office of Intelligence and Analysis (DHS/I&A) of timely, accurate, actionable information at the unclassified, For Official Use Only level. This pilot gave local and state officials the opportunity to provide input into the business process and functionality of the system, and a Steering Group comprised of local and state officials wrote and approved the charter. This pilot was extended for a second three months, and then the Steering Group recommended turning this into an operational Community of Interest. This collaborative effort created a true Community of Interest that encompassed a useable network of intelligence professionals, analyst to analyst collaboration and a continuing partnership between local, state and federal intelligence communities. This community has created trusted relationships that ultimately is a more powerful tool than any network or portal and these relationships will remove the resistance to sharing information that has plagued government response in the past, thereby pooling together information from all pertinent intelligence sources to effect a decisive response. This Community of Interest now has fourteen member states, and it is expected to double by the end of this fiscal year, and is a perfect example of local, state and federal agencies working together in an effort to meet the needs of all those involved.

Recommendations

In order to be a true Intelligence led policing model, local, state and federal analysts must be able to see all information and intelligence. If analysts are provided only a couple pieces of the puzzle, we will never be able to see the overall picture. Local, state, tribal and federal agencies as well as private industry have individual pieces, and we must have an IT mechanism as well as trusted relationships to put these pieces together. Currently, state and local analysts are provided access to a wide range of unclassified systems, to include the Homeland Security Information Network, but have limited access to classified systems such as the Homeland Secure Data Network (HSDN). Local, state and federal unclassified initiatives must be incorporated to meet the needs of everyone involved in homeland security and to improve operational effectiveness. Local and state intelligence professionals must also be given the same opportunity as their federal counterparts regarding the access to classified systems. In the past, analysts from the federal intelligence community primarily focused on information contained in classified systems, while local and state analysts focused on information contained in unclassified systems. Using this system, how will we ever be able to see the overall picture?

Conclusion

Virginia and other state and local agencies understand the importance of protecting classified information to include sources and methods that are contained in these reports. The problem that still exists is the over classification of information and intelligence and the lack of tear lines that could be provided to local and state law enforcement in addition to other agencies and private Industry with a homeland security role. These tear lines could provide valuable tactical and strategic information that could assist in the overall mission of these entities. The ability of local and state law enforcement agencies to mitigate potential threats in their communities is hampered because of the lack of actionable information and intelligence. In all likelihood, a police officer in one of our communities will encounter a potential terrorist during their normal tour of duty, and without the information needed to perform their duties; they will not be able to identify the possible threat. The Federal Intelligence community needs to understand the importance of either providing local and state law enforcement agencies with a valid "right and need" access to some of these networks or the ability to provide tear lines through a standard business process and network. The Homeland Security Information Network would be a perfect network to disseminate these tear lines in "real time" so that local and state law enforcement agencies could have the ability to receive tactical and strategic information and intelligence to assist them in their homeland security role.

Ms. HARMAN. Sergeant, I am going to cut you off there. Point well-taken, and you should know that this subcommittee is work-

ing on both reforming our classification and our pseudo-classification systems, and making certain that you get the information you need.

I just want to get through this testimony, and we will see where we are with votes, and give you more time.

Inspector Lindquist?

STATEMENT OF BARRY S. LINDQUIST, INSPECTOR, OFFICE OF STATEWIDE INTELLIGENCE, FLORIDA DEPARTMENT OF LAW ENFORCEMENT

Mr. LINDQUIST. Good morning, and thank you for the opportunity to speak.

One poster doesn't fit all.

I am departing—for the sake of brevity.

Florida has been deeply committed to HSIN as HSIN–Florida. We have developed with the cooperation and support of DHS. Yes, there has been a bumpy road, but we have a mechanism of sharing for multiple disciplines from our domestic security task force. It includes law enforcement and critical infrastructure, fire, public information and health.

Recently, our state Department of Health has made a decision to vacate a site that they had been using to share response plans for health, and put it on HSIN-Florida. A HSIN-Florida is working. It would be very detrimental for us for any reduction in services or change in the program. If we all the help desk, the help desk is there.

We have asked for improvements. We have received those. The common operating picture, that has been great. I want to mirror what Lee has said about intelligence and analysis, and HSIN-Intel. It has started. It is a collaboration, and it is working extremely well. I think it is the direction that the committee like to see.

We have been guarding that deployment to those intelligence professionals around the state that are important.

[The statement of Mr. Lindquist follows:]

PREPARED STATEMENT OF BARRY S. LINDQUEST

Good morning Madam Chair and distinguished members of the Subcommittee.

My name is Barry Lindquist and I am a member of the Florida Department of Law Enforcement (FDLE). I am an Inspector assigned to Domestic Security matters in the FDLE Office of Statewide Intelligence and the Florida Fusion Center. In this position, I have been the primary point of contact for the Department of Homeland Security for matters relating to HSIN.

Introduction

Florida was one of the first states to pilot the Homeland Security Information Network (HSIN) and since implementation in early 2005, HSIN-Florida has become a cornerstone in our information sharing strategy. Additionally, the HSIN State and Local Intelligence Community of Interest (HSIN-Intel COI) is currently becoming our primary method of sharing information with the Department of Homeland Security, office of Intelligence and Analysis.

Homeland Security in Florida is called Domestic Security and is structured around our multi-disciplinary Domestic Security Task Force (DSTF). The DSTF structure is further subdivided into seven Regional DSTF components (RDSTF) with an FDLE Special Agent in Charge and a regional Sheriff or Police Chief as Co–Chairs of their RDSTF.

Florida RDSTF Regions

Each RDSTF had components that include the following workgroups;

- Law Enforcement,
- Fire,
- Emergency Management,
- Health and Medical,
- Schools and Education,
- Communications Critical Infrastructure, and
- Public Information.

HSIN–Florida

When the Department of Homeland Security first approached Florida in early 2005 with the opportunity to pilot HSIN, we already had a statewide anti-terrorism intelligence database named InSite and an Internet website named ThreatCom that was used to share information and alert our task force members about events and potential threats. Both of these systems were created in 2002 and were well integrated into our Domestic Security information sharing strategy. The challenge that HSIN presented was determining how it could be effectively integrated with our existing systems without confusing our partners.

Florida worked with the Department of Homeland Security to simplify and tailor the system to meet our needs, HSIN-Florida has four main components;

- **Home Page**
  - Announcements
  - Recently uploaded products
  - Calendar
- **Situational Awareness—**a discussion thread
- **DHS Documents—**Recently uploaded documents contained in the government.hsin.gov site
- **Document Library—**that has a statewide document library and libraries for each of our seven regions.

Using this basic structure, HSIN–Florida allows every user to view and upload the documents. Every user has the ability to decide what they believe is important and share their information with other users. In support of our RDSTF structure, Regional HSIN–Florida Administrators have the ability to edit and delete content, and also nominate and validate new users into the system.

Every HSIN-Florida user is asked to complete an application for access to the system. Our Regional Administrators ensure a background is conducted before user access is granted. The Regional Administrators are also responsible for ensuring that

users are removed from the system when their position changes and no longer justifies access.

Since HSIN-Florida was deployed, significant enhancements have been made in the Common Operating Picture (COP) that is deployed in many of the national HSIN sites. Florida did not include COP in HSIN-Florida because of our strong partnership with the Department of Emergency Management which has its own system for managing events in Florida. In its new and improved form, Florida has a pending request to include COP in HSIN-Florida to better inform our task force members about national incidents managed by DHS.

HSIN—State and Local Intelligence

Florida also participated in the HSIN-State and Local Intelligence (HSIN-Intel) pilot initiated by the DHS Office of Intelligence and Analysis (I&A). Our goal in this pilot was to establish a known and trusted community of intelligence professionals that could collaborate together and work with I&A on common Homeland Security matters.

The goal of HSIN-Intel is to provide DHS and selected State and local participants with a trusted and centralized information sharing mechanism for the exchange of controlled, unclassified intelligence and threat related information. In Florida, HSIN-Intel is being deployed in the Florida Fusion Center and with our other fusion centers around the state.

Other HSIN National Communities of Interest

Florida has not widely deployed other HSIN national communities of interest. The Florida information sharing strategy focuses on collecting and analyzing information received from our DSTF regions and ensuring the accuracy and validity of this information as it flows from Florida to our national partners.

National communities of interest such as Emergency Management have been deployed to the Florida Department of Emergency Management. The Law Enforcement community of interest has been made available to some of our state and local Fusion centers and Intelligence partners.

Ms. HARMAN. Thank you for that testimony.

Captain Tomblin?

STATEMENT OF CAPT BRIAN TOMBLIN, MILITARY LIAISON, OFFICE OF HOMELAND SECURITY, TENNESSEE ARMY NATIONAL GUARD

Captain Tomblin. Thank you, ma'am.

I am going to follow along with Barry and depart from written comments, and just state that, like Florida, Tennessee has adopted HSIN, and has followed the DHS lead and invested its information sharing solely on HSIN.

The HSIN-Tennessee system is very robust. We have five separate portals, an emergency management portal, a critical infrastructure portal, and then the law enforcement portal. There is a portal for training exercises and for running operations that you all want out there on the live portal.

So what I would say to you is that HSIN-Tennessee is a standalone system that works for us. It is an information-sharing tool. We took it from DHS as they presented it. We modified it to meet our needs. I am confident in the current leadership, especially Theresa Phillips. She is very aggressive, very open. We have looked to her to reestablish the state working groups, and that is one of the big recommendations.

Everything that we have issue-wise revolves around communications. Reestablishing those state working groups, listening to the states and what their needs are, will just further this system. We are very happy with it at the state level. My commissioner has only one fear, and that fear is that it would go away, and he has invested everything in it.

So I would leave you with that, and I thank you for this opportunity.

[The statement of Captain Tomblin follows:]

PREPARED STATEMENT OF MAJ BRIAN K. TOMBLIN

I. Introduction

Chairwoman Harman, Ranking Member Reichert, and members of the Subcommittee, thank you for the opportunity to appear before you today and discuss the performance of the Homeland Security Information Network in the state of Tennessee.

The State's ability to share information quickly and accurately over a secure network, among various communities of interests, is crucial in order to prevent, protect, deter and respond to potential criminal and terrorist acts. The state of Tennessee has followed the Department of Homeland Security's lead and invested its information sharing holdings and strategies on the Homeland Security Information Network (HSIN) platform. The Homeland Security Information Network—Tennessee (HSIN–TN) provides connectivity for public service disciplines to receive and share information throughout Tennessee. Through a successful partnership with the Department of Homeland Security, HSIN—TN is the secure information sharing network for the state and provides users the ability to interface with the state all crimes intelligence and information fusion center.

II. HSIN—TN Portal Development

In February 2005, TN was selected to participate in the pilot phase of HSIN development at the state level. Recognizing the state did not have the ability to gather, review and disseminate information via a common system, the TN Office of Homeland Security (OHS) developed information sharing goals for the state and an aggressive timeline for the deployment of the HSIN—TN across Tennessee. Working directly with the IT contractor, Mantech–IST, the initial TN portals where developed. A HSIN-TN pre-pilot was conducted in August 2005 and a pilot phase was conducted in September to allow TN OHS users to become familiar with the system. Consequently, HSIN became a viable tool for communication with Louisiana during Hurricane Katrina. Communicating via the HSIN portals, Tennessee was able to provide the Louisiana State Police with logistical support and the Tennessee Office of Homeland Security was able to route an assistance call received from a relative in Knoxville to the Louisiana State Police which resulted in the successful rescue of a family trapped in a flooded attic.

The initial HSIN—TN training of law enforcement occurred in November, 2005. A fusion center initiative conference was held in December 2005. During this conference, HSIN—TN was briefed to the state and local law enforcement leadership as the information sharing platform for the TN fusion center.

III. HSIN—TN Training

In January 2006, I was named the HSIN–TN program manager and tasked with developing a HSIN training program for the state. Based on Tennessee geography and the established 11 TN Homeland Security Districts; a regional, east to west fielding plan was derived. Training requirements were submitted to the primary HSIN training contractor, MTCI, and training began in east TN at Johnson City in March 2006 and concluded in Memphis in August 2006. This initial fielding plan resulted in the training of over 783 individual users, representing over 330 agencies.

The initial training strategy was to train local, state and federal law enforcement officers in order to develop a user base that would share critical information with each other and provide the fusion center with all source criminal data. While reviewing the initial east TN training, a training gap was identified. We determined the state was missing an opportunity to get various public service disciplines together for training which would further promote interaction and information sharing between law enforcement and non-law enforcement partners. Training throughout the remaining homeland security districts was then offered to additional communities of interest (COI) such as emergency management, fire and rescue and selected critical infrastructure partners.

IV. HSIN—TN Portals

In June 2006, DHS recognized the HSIN—TN portals as operational and the portals where considered live and no longer a training environment. TN currently manages five HSIN state portals; Home, Law Enforcement, Critical Infrastructure, Training and OHS. All portals are now monitored by the TN Fusion Center, a joint partnership between the TN OHS and the Tennessee Bureau of Investigations (TBI). The portals allow all communities of interest users to share information at

the Sensitive But Unclassified (SBU) level based on their occupational discipline and provides secure instant messaging via the JABBER collaboration tool. HSIN—TN users can contribute products to the appropriate portal, request information or operational support from the fusion center, research or contribute to the document library and access additional DHS portals via hotlinks. Since becoming operational, we have increased our user base to more than 1000 trained users representing over 500 agencies. HSIN training continues on a weekly basis as the state strives to make HSIN ? TN the focal point for information sharing in Tennessee.

V. Current Challenges

While HSIN—TN provides the state with an excellent ability and resource, frustration is still experienced on managing and maintaining the system at the state level. As the HSIN—TN program manager, I have administration and community of interests rights but these are limited to only the ability to nominate and validate new users and to remove information from the portals. I cannot effectively manage the user data base. There is no capability to monitor use of the portal, review the user data base or to delete users when they no longer require access to the portals. Once the user is validated into the system, I loose the ability monitor and maintain the state user accounts. However, I have been briefed that a new account management tool is reportedly near fielding.

The line of communication between the state and a viable DHS HSIN representative is convoluted. Tennessee has a Stakeholder Relationship Manager assigned through Sim–G Technologies but when request for support or changes to the portals are requested they often go unresolved or unanswered. When HSIN was first deployed at the State level it included a GIS mapping product. Shortly after our state portals where considered functional and after a third of the state had been trained, a decision was made to upgrade the HSIN system. The concept was to standardized portal configuration in order to facilitate faster deployment to new state partners. While this was understandable, the changes to the portal where made without input from the pilot states and included changes that were not discussed with the pilot states. One of those critical changes was the decision to drop the GIS mapping product. A reliable mapping tool is crucial to the success of the portal and provides the smaller departments and agencies a capability they normally could not afford. I have been briefed that a replacement mapping tool will be available on the state portals in the future.

When the pilot states were identified, an HSIN state working group was developed to allow pilot states to meet together quarterly and discuss operational and technical issues with each other and the DHS HSIN staff and contract support. These meetings were very beneficial and allowed the states to adopt best practices and identify common issues and problems with the system. After only two meetings, the working group was dissolved without explanation and changes to the portals where implemented without input from the states. Information technology (IT) support is now handled through the Change Request Registration and Tracking System (CHaRTS). This automated system for requesting changes to the portals works but it is hard to explain complex technical issues through written communication. As the portals are operational, the State cannot afford to submit changes through and automated system, problems need to be rapidly worked in real time. In the past, by talking directly to the IT contract support, simple changes could be made over the phone and reviewed by the state in a matter of minutes, not days or weeks.

VI. Recommendations

The problems and frustrations currently experienced with HSIN are all directly related to a lack of communication and clear guidance between DHS and state partners. Re-establishing the state and local working groups will greatly enhance the states ability to communicate common issues and develop working solutions for implementation. Working together as a team to develop policy and procedures, lessons learned and best practices, and to review, test and implement new technical advances and solutions is critical to the continued success between DHS and its state partners.

VII. Conclusion

The Homeland Security Information Network is a critical component of the information sharing system of Tennessee. Tennessee has taken this information sharing tool and forged it into the secure information sharing network for the state. Continued cooperation and interaction between DHS and its state partners are crucial to the continued success of this system. Re-establishing the state working groups, implementing account management tools and streamlining the IT support will help to ensure the stability and viability of HSIN for years to come.

Ms. HARMAN. Thank you, Captain. I appreciate your testimony.

You can see the votes have been called again, but I am try to get in a couple of questions.

Obviously, two of you think this is more suitable for your needs, and two of you think that you have been able to use the HSIN network, at least in your states, in a way that is satisfactory. I am not sitting up here to referee this. Let me ask a question and just if any of you disagrees with this statement, please say so.

Do you all agree that your needs are what these systems need to satisfy? Yes or no? That the set of criteria that need to be met have to originate from you, because you are the folks who have to take the information and make it operational in your areas. Do you agree with that?

Okay. I think it was Inspector Lindquist who said one size does not fit all. Does everyone agree with that proposition? Or do you think one size should fit all?

Nobody disagrees with that?

Everyone was here when the GAO issued its report in our prior panel. Does anyone want to comment in a sentence on the findings of the GAO report, which was fairly harsh, at least in terms of duplication? Does anyone disagree with the thrust of those findings?

Nobody disagrees? Mr. Lindquist?

Mr. LINDQUIST. No, I don't.

Ms. HARMAN. No. Okay. So the goal here, I hope, is to start at your end, figure out if there is commonality of need, and I don't mean one size fits all, but how best to figure this out. And then try to move forward, eliminating duplication, waste, inefficiencies, with products that suit your needs.

Does anyone disagree with that? No.

We had conversation in the last panel about mechanisms to do that. You all heard those conversations. Does anyone have a specific suggestion about how the consultation should work?

Captain Harris. Madam Chairman, I have just a suggestion on that, not how the mechanism should work, but it is very important to have a single sign-on for those systems because those systems are all important, but a single sign-on feature is very relevant.

Ms. HARMAN. Thank you.

Does anyone disagree with that? No.

Okay, the technologically challenged—that would be me—I would say "hurray," because obviously the goal is to get everything you need quickly. Correct? And make sure that you are not missing anything. Right?

Sergeant Miller. A perfect world for us is a one-stop-one-shop place.

Ms. HARMAN. Right. That would meet your problem, would it not, Inspector Lindquist, because if you could log-on through the system you are comfortable with and get the rest of the information, you would be happy about that. Right?

Mr. LINDQUIST. I think a single log-on is a good idea, but it is not the only solution. I think part of what we need to do is define how the information is going to flow within a state, because the states want to be able to vet and verify the information as it flows from the state to the national community, and to its partners, so that we don't end up erroneously tracing down old information that occurred last week.

Ms. HARMAN. Hear, hear. I agree with that as well. Nobody disagrees with that, right? But accurate, actionable and timely information is what you need. Everyone agrees, and everyone agrees we have some work to do to get that for all jurisdictions in a form that is useful. Correct?

All right. I am going to leave this panel there. I am very sorry about this, but you can hear all the bells and whistles.

Unfortunately, other members could not get back, but if you can stay for a few more minutes, staff is here and if there are additional questions we have, they will be asked informally, because we don't have a mechanism in this committee to do staff questioning of witnesses. I would hope that could occur.

You are all enlisted in this war against those who would harm us in America. Let me just add this one sentence. I have been saying for some time, and it was before the most recent Fort Dix issue, that they are here. There are people in our country who are trained, somewhat loosely coordinated, and intending to attack us. We need our best people on the case. In most cases, they are you, and the people who work with you.

These attacks could occur anywhere at any time, and if you don't have the training and information you need to know what to look for and what to do, we will not prevent and disrupt them. So our goal on this subcommittee is to get you that training and information ASAP.

Obviously, we need you as part of the group that fixes systems that are not working properly, because these products have to suit your needs. That is the absolute priority, and I give you my promise that on a bipartisan basis here, everyone is intent on getting this right, and with your help, we will.

Thank you very much.

The hearing is adjourned.

[Whereupon, at 11:55 p.m., the subcommittee was adjourned.]

VerDate Nov 24 2008 10:59 Jun 24, 2009 Jkt 000000 PO 00000 Frm 00049 Fmt 6633 Sfmt 6011 H:\DOCS\110-HRGS\110-34\48909.TXT HSEC PsN: DIANE