THE HOMELAND SECURITY INFORMATION NETWORK: AN UPDATE ON DHS INFORMATION—SHARING EFFORTS

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

SEPTEMBER 13, 2006

Serial No. 109-101

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

35-623 WASHINGTON : 2007

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

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
BENNIE G. THOMPSON, Mississippi
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
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

ROB SIMMONS, Connecticut, *Chairman*

CURT WELDON, Pennsylvania
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
STEVAN PEARCE, New Mexico
BOBBY JINDAL, Louisiana
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
PETER T. KING, NEW YORK *(Ex Officio)*
ZOE LOFGREN, California
LORETTA SANCHEZ, California
JANE HARMAN, California
NITA M. LOWEY, New York
SHEILA JACKSON-LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

THE HOMELAND SECURITY INFORMATION NETWORK: AN UPDATE ON DHS INFORMATION–SHARING EFFORTS

Wednesday, September 13, 2006

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

The subcommittee met, pursuant to call, at 1:00 p.m., in Room 2212, Rayburn House Office Building, Hon. Rob Simmons [chairman of the subcommittee] presiding.

Present: Representatives Simmons, Souder, Gibbons, Lofgren, Harman, and Jackson Lee.

Mr. SIMMONS. [Presiding.] A quorum being present, the Committee on Homeland Security's Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment will come to order.

Today the subcommittee meets to hear testimony on the effectiveness of the Homeland Security Information Network, or HSIN. On our first panel today, we have three witnesses.

First, Mr. Frank Deffer, assistant inspector general at the Department of Homeland Security. Welcome.

Mr. DEFFER. Thank you.

Mr. SIMMONS. Mr. Deffer has been the assistant inspector general for information technology at the Homeland Security since the inception of the office of inspector general in 2003 and has been involved in what I consider to be a very important report on the Homeland Security Information Network.

Second, Mr. Roger Rufe, director of Operations Coordination Directorate at the Department of Homeland Security. The Operations Coordination Directorate has management responsibility for HSIN. Admiral Rufe recently joined DHS, returning to public service after a 34-year career with the United States Coast Guard.

Semper Paratus, Admiral. Good to have you here.

Third, we have Mr. Charlie Allen, chief intelligence officer at the Department of Homeland Security. He is the chief intelligence officer at the department and has become a regular fixture at this subcommittee.

Thank you, Mr. Allen, for your appearance.

Over the last 2 years, this subcommittee has spoken to and received testimony from many different state and local officials, and

almost universally when we ask, "Has information sharing improved?", the answer is yes.

But are we where we want to be? And I would say probably not; we can do better. There have been improvements. We need more improvements.

The inspector general's report has demonstrated that there are particular problems with the HSIN network, and that is the focus of what we are trying to do today.

Information sharing is not culturally what we expect when we consider our intelligence community and when we consider our different departments and agencies in government. And yet, this is absolutely what we have to be able to do.

If we are not successful in our information-sharing efforts, then we are not going to be successful in connecting the dots to protect our people and our nation from the possibility of additional attacks. And so, that is why we continue, as a subcommittee, to focus on this important aspect of our nation's security.

I will request that the remainder of my statement be placed in the record as read, and take this moment to yield to the distinguished ranking member of the committee.

And if I am speaking quickly, it is because I realize that we may be having votes sooner than anticipated this afternoon and I want to make sure we can get started.

And now I recognize the gentlelady from California, the ranking member, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman.

As I reviewed the inspector general's report on the Homeland Security Information Network, it reminded me of the old proverb, "Haste makes waste." And I remember my mother telling me that.

Mr. SIMMONS. She was right.

Ms. LOFGREN. She was right, as well. I think that taxpayers really should be outraged by what has happened here. The program is not only a model of haste and waste, but it is a missed opportunity to do things right.

Now, these comments are true, but they also reflect that we have two people here who are not blame-worthy, really, on this?and I want to state that. I mean, Mr. Allen and Vice Admiral Rufe came in after this was well under way. But it is still a mess that is in their hands.

Creating a secure information-sharing network was essential to partnering with our state, local and tribal law enforcement partners. And given the prominence that this network was played we had been told over the years, it is just astonishing to me that your predecessors didn't give some deliberation and planning into its development.

And so, here we have $50 million, whether it is all down the drain or just partly down the drain, I would like to hear from the department.

As the inspector general has said, the network does not support information sharing effectively, does not meet user needs, and, as a result, is not relied upon regularly by anyone. So we have HSIN but apparently not greater security, and that is a shame.

I want to make it clear that I remain a partner with the department in our efforts to improve the situation. But to say that this is a disappointment is to understate the situation.

And as the chairman has indicated, I will make my full statement a part of the record, understanding that we will have votes called soon and they should go on for 20 minutes or so. I would hope that we have the opening statements of the witnesses that are very helpful. Perhaps they can also be brief and we will get to questions.

And I yield back to the chairman.

Mr. SIMMONS. I thank the lady.

We are honored to have the ranking member of the House Intelligence Committee with us here. Normally, under our rules of procedure, we extend the courtesy of an opening remark to the chairs and the ranking, but I would be happy to hear from the gentlelady from California if she has something she wants to say.

Ms. HARMAN. Well, I thank you, Mr. Chairman. I wasn't expecting this, but I have become a regular at Charlie Allen briefings. I come here to make sure he stays out of trouble.

[Laughter.]

And so far he has performed admirably.

I just would make a comment that it is important to focus on how information sharing can work better. It is not just that DHS needs to be at the table, but it also needs to be an information source. And I think all the witnesses understand that, and I think that is the direction that Charlie is heading.

But, Mr. Chairman, I was in New York on 9/11, and after the wrenching ceremonies at Ground Zero, I had lunch with some of my favorite friends at the NYPD, and we were talking about information sharing. They set up something truly amazing in New York, but they did talk about the challenges still for the federal government to be the kind of player it needs to be.

And they are right. The federal government has to do more. DHS has to do more. Charlie is building something from scratch, but it needs to be able to do more in real-time real soon.

Let me just close with a comment about my visit recently to the Joint Regional Intelligence Center in Los Angeles with Secretary Chertoff and LAPD Chief Bratton and L.A. Sheriff Baca. That is an impressive facility, and it would not be there but for DHS and the efforts of Charlie and others, including the FBI. Forgot to mention them.

But these JRICs are only as good as the material that is in them. So, again, let me just close with my comment that the HSIN needs to do better. And I think the gentlemen at the table are going to make it do better.

Thank you, Mr. Chairman.

Mr. SIMMONS. Thank you very much.

Why don't we begin with you, Mr. Deffer?

STATEMENT OF MR. FRANK W. DEFFER, ASSISTANT INSPECTOR GENERAL, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. DEFFER. Thank you, Mr. Chairman and members of the subcommittee. My testimony today will address the evolution, plan-

ning and development, implementation, and effectiveness of HSIN based on our July 2006 report.

By working together, federal, state and local governments can maximize the benefits of information gathering and analysis to prevent an respond to terrorist attacks. However, prior reports have shown that counterterrorism-related information is not shared routinely or effectively.

To help improve this situation, DHS has expanded access to its secure, unclassified HSIN system, which connects the department's Homeland Security Operations Center, or HSOC, with private industry and federal, state and local organizations responsible for or involved in combating terrorism and supports various community groups, including law enforcement and emergency management.

HSIN began as an extension of the Joint Regional Information Exchange System, or JRIES, a law enforcement intelligence system that proved useful for information sharing during the Northeast blackouts of 2003. After DIA transferring management of the system to DHS in September of 2003, the department expanded the system to meet its crisis planning, communications, and emergency management requirements.

Renamed HSIN, the system was migrated to a series of Web-based portals and ultimately redeployed nationwide as well as to several international partners.

Despite the vital role that HSIN was to play in ensuring intergovernmental connectivity and communications, DHS did not follow several steps essential to effective system planning and development.

Specifically, after assuming ownership of the system in 2003, DHS quickly expanded system access to other user groups. In the heightened counterterrorism environment, the department decided to implement HSIN right away and address operational issues later.

This created an environment that was not conducive to thorough system planning and implementation. For example, the rush to implement resulted in inadequate definition of HSIN's role vis-a-vis related systems; insufficient identification of requirements of the HSIN user community; inadequate technical evaluation of system releases prior to deployment; and a lack of HSIN user guidance, training and reference materials.

Largely due to these planning and implementation issues, users are not fully committed to the HSIN approach. Specifically, users generally like the Web portal technology, but do not fully understand HSIN's role and how the information shared on the system is used. Further, situational awareness information is not readily available through the system.

Some users in the law enforcement community, in particular, told us that they do not trust the system to share sensitive case information. Because HSIN does not fully meet their needs, law enforcement users often use other existing systems such as Law Enforcement Online and the Regional Information Sharing Systems Network, perpetuating the ad hoc, stovepipe information-sharing environment that HSIN was intended to correct.

Similarly, officials at nine of the 11 state and emergency operations centers that we visited stated that they only log on to the

system occasionally. Some emergency operations centers have a very limited number of user accounts, while others are not connected to HSIN at all.

Although the total number of HSIN user accounts has increased since the system was deployed, use of HSIN's law enforcement, emergency management and counterterrorism portals has remained consistently low.

In conclusion, DHS has a critical role to play in ensuring national awareness, preparedness, and coordinated response to potential emergency situations, suspicious activities and terrorist threats. HSIN can assist by supporting timely and relevant counterterrorism-related data exchange across governments.

But overcoming system planning and implementation issues, as well as related challenges, will assist DHS in fulfilling its central coordination role and providing the collaborative capabilities needed to help keep our homeland secure. Toward the end, DHS concurred with our report recommendation and is taking steps that, once implemented, will improve HSIN effectiveness.

Mr. Chairman, this concludes my prepared statement. I appreciate your time and attention and welcome any questions from you or members of the subcommittee.

[The statement of Mr. Deffer follows:]

PREPARED STATEMENT OF MR. FRANK DEFFER

Thank you for the opportunity to discuss the work of the Office of Inspector General (OIG) relating to DHS' system and approach for sharing counterterrorism, emergency management and intelligence-related information government-wide as well as the recommendations that we made to enhance departmental operations. My testimony today will address the evolution of the Homeland Security Information Network (HSIN); ongoing system planning and development activities; how well the system works to share information; and, major challenges to effective implementation. The information and recommendations that I will provide is contained in our report, Homeland Security Information Network Could Support Information Sharing More Effectively (OIG-06-38).

The Evolution of HSIN

State and local personnel have capabilities not possessed by federal agencies to gather information on suspicious activities and terrorist threats. By working together, government organizations can maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks. But earlier reports from congressional and industry organizations show that information on the threats, methods, and techniques of terrorists has not been shared routinely-and when information is shared it has not been consistently perceived as timely, accurate, or relevant.

HSIN is a secure, unclassified, web-based communications system that provides connectivity between DHS' Homeland Security Operations Center (HSOC)-the national center for real-time threat monitoring, domestic incident management, and information sharing-and the critical private industry as well as the federal, state, and local organizations responsible for or involved in combating terrorism, responding to critical incidents, and managing special events. HSIN offers both real-time chat and instant messaging capability as well as a document library that contains reports from multiple federal, state, and local sources. The system supplies suspicious incident and pre-incident information, mapping and imagery tools, 24/7 situational awareness, and analysis of terrorist threats, tactics, and weapons. HSIN consists of a group of web portals organized along the lines of several community groups including law enforcement, emergency management, fire departments, homeland security, counterterrorism, and the National Guard. To fulfill its responsibility to coordinate the distribution of counterterrorism-related information across the various levels of government, DHS is expanding access to HSIN.

HSIN was created as an extension of the Joint Regional Information Exchange System (JRIES), begun in December 2002 as a grassroots pilot system to connect the California Anti-Terrorism Information Center, the New York Police Department,

and the Defense Intelligence Agency (DIA) to facilitate the exchange of suspicious activity reports, register events potentially related to terrorist activity, and to foster real-time intelligence and law enforcement collaboration in a secure environment across federal, state, and local jurisdictions. JRIES proved useful during the northeast blackout in 2003 when information posted on the system allowed users across the country to quickly learn that the event was not related to terrorism. Although the DIA originally operated and maintained JRIES, DIA transferred program management of the system to DHS in September 2003, due to funding constraints.

After acquiring JRIES, DHS recognized that the system's utility could be expanded beyond its existing counterterrorism intelligence and threat awareness mission to support crisis planning, communications, and emergency management across federal, state, and local agencies. In 2004, the DHS Secretary renamed the system as HSIN in order to reflect its broader scope. DHS subsequently deployed HSIN to all 50 states, 53 major urban areas, five U.S. territories, the District of Columbia, and several international partners-extending HSIN access beyond the law enforcement community to include state homeland security advisors, governors' offices, emergency managers, first responders, the National Guard, and an international component. Because the system could not accommodate a large increase in users, DHS decided to migrate HSIN from the original software, Groove, to a series of web-based portals. DHS also launched an initiative to identify and address requirements of state and local communities of interest, as well as to provide robust training to promote effective use of the system. As of January 2006, eight states had adopted state-specific HSIN portals for use throughout their respective departments and agencies.

HSIN Planning and Development

Despite the vital role that HSIN was to play in ensuring intergovernmental connectivity and communications in a heightened counterterrorism environment, DHS did not follow a number of the steps essential to effective system planning and development. Specifically, DHS:

- rushed the HSIN schedule;
- did not clearly define relationships to existing systems;
- developed and deployed HSIN in an ad hoc manner;
- provided inadequate user guidance; and,
- did not establish performance metrics.

After assuming ownership of the system from DIA in 2003, DHS quickly expanded the system access to other user groups. Due to increased concerns and warnings about potential terrorist threats, the department's HSIN strategy was to implement a tool for nation-wide connectivity immediately and address operational problems and details later.

Such pressures to complete the system, however, created an environment that was not conducive to thorough system planning or implementation. For example, the rush to implement resulted in inadequate definition of HSIN's role with respect to comparable law enforcement systems such as, Law Enforcement Online (LEO) and the Regional Information Sharing System Network (RISSNET); and, a failure to identify potential areas of duplication or opportunities for sharing information. Also, DHS developed the HSIN portals based solely on law enforcement requirements but did not sufficiently identify the needs of other HSIN user communities such as emergency management personnel and state homeland security advisors. Further, because DHS did not evaluate adequately the major HSIN releases prior to their implementation, technical problems that hindered system performance went undetected. Inadequate user guidance, training, and reference materials on what or how information should be shared resulted in some states defining information sharing processes and procedures on their own-activities that increased the potential for duplication of effort and lack of standardization. Additionally, DHS did not develop adequate performance measures. Instead it assessed HSIN performance based on tallies of active user accounts. Such numbers were neither a good indicator of system use nor the quantity of information shared using the system.

Some members of the law enforcement intelligence community raised concerns early on that DHS was expanding HSIN access and capability too quickly. For example, in an April 2004 issue paper, the executive board responsible for the predecessor JRIES stated that DHS was proceeding at a rapid rate in implementing the system and contended that this approach increased the risk of system misuse, security breaches, privacy violations, and user confusion as well as dissatisfaction. The board pointed out that the department's newness and its lack of established relationships hampered its ability to quickly gain the trust and commitment of states and major cities to the HSIN approach.

HSIN Information Sharing Effectiveness

We found that, largely due to the planning and implementation issues discussed, users are not fully committed to the HSIN approach. Specifically, state and local users we interviewed provided mixed feedback regarding HSIN. Although they generally like the web portal technology, they have several suggestions on how to improve the system's technical capabilities to meet their needs. Users do not fully understand HSIN's role and how the information shared on the system is used, either. Last, situational awareness information that could help states and cities determine how to respond to threats when major incidents occur is not readily available. The HSIN-Secret portal, meant to function as a temporary channel to deliver classified information, does not provide valuable terrorism-related content.

Some users in the law enforcement community told us that they do not trust the system to share sensitive case information. This erosion in trust as the system was expanded led to conflicts between the JRIES executive board, comprised primarily of law enforcement officials, and HSIN program management. In May 2005, concerned with the direction that DHS had taken with JRIES/HSIN without soliciting its input, the JRIES executive board voted to discontinue its relationship with the HSOC. The consensus of the board was that the HSOC had federalized what it believed to be a successful, cooperative federal, state, and local project. After their withdrawal, the JRIES executive board continued to promote its initial information-sharing concept as JRIES II, a separate system apart from HSIN, which has confused state law enforcement personnel.

Because HSIN does not fully meet their needs, users do not rely upon the system to share counterterrorism information. For example, law enforcement users said that they often use other existing systems, such as Law Enforcement Online, the Regional Information Sharing System Network, and the Federal Protective Services-Secure Portal System. Private systems, such as the ″NC4″ managed by the National Center for Crisis and Continuity Coordination, provide real-time information to state and local subscribers. The system provides warnings, alerts, and situational awareness on a fee for service basis. In some instances, agencies such as the U.S. Secret Service are creating their own portals for information sharing among a limited user group. Such practices perpetuate the ad hoc, stove-pipe information-sharing environment that HSIN was intended to correct.

Further, state and local law enforcement officials said that they continue to depend upon personal contacts and telephone calls to related organizations to exchange intelligence on potential threats. These users recognize, however, that phone calls are not the most efficient means of obtaining situational awareness information and coordinating incident response activities. For example, users stated that during the 2005 London bombings, they needed timely information, such as whether the attacks were suicide attacks, so that state and local transportation security would know what to look for in their own jurisdictions. However, the information provided on HSIN was no more useful or timely than information available via public news sources. Users were able to get better information faster by calling personal contacts at law enforcement agencies with connections to the London police, than by using the system.

Along with a continued reliance on alternative means to share information, state and local users are making limited use of HSIN. Although law enforcement is a principal HSIN customer, officials at state fusion centers and police counterterrorism units said that they do not use the system regularly to share intelligence information. Officials at nine of the 11 state and city emergency operation centers that we visited stated that they log on to the system only occasionally. Further, some emergency operation centers have a very limited number of user accounts, while others are not connected to HSIN at all.

Data provided by HSIN program management demonstrates that user logons and postings are limited, and that users do not view the system as the nation's primary information sharing and collaboration network as DHS intended. Although the total number of HSIN user accounts has increased since the system was deployed, use of three of the primary HSIN portals-the law enforcement, emergency management, and counterterrorism portals-has remained consistently low.

Major Challenges

In addition to the technical system issues discussed above, DHS faces multiple challenges, often beyond the control of HSIN program management to successfully implementing HSIN to support homeland security information sharing. First, resource limitations have hindered the ability of organizations at all levels of government to effectively share information. This will undoubtedly continue to pose challenges in the future. For example, DHS officials cited a lack of sufficient personnel as a reason for their inability to provide vital support to HSIN users, especially during its initial release. Similarly, state officials expressed concern that they do not

have enough personnel to monitor all of the federal systems available to them. For example, a state emergency management official said that, at one point, a single employee had to monitor 19 different systems. State officials added that a lack of funding limits their ability to sustain operations at state-run facilities, such as intelligence fusion and analysis centers, too.

Second, legislative requirements have created challenges to effective information sharing. Federal legislation over the past several years has established new goals and authorities for information sharing beyond those initially assigned to DHS. The Homeland Security Act of 2002 gave DHS the responsibility to coordinate and share information related to threats of domestic terrorism with other federal agencies, state and local governments and private sector entities. In 2004, however, the Intelligence Reform and Terrorism Prevention Act established the Office of the Director of National Intelligence external to DHS. The act mandated the establishment of an information-sharing environment under the direction of a newly designated program manager to facilitate sharing of terrorism-related data nation-wide. Establishing this new information-sharing environment will involve developing policies, procedures, and technologies to link the resources of federal, state, local, and private sector entities to facilitate communication and collaboration.

State laws, which differ widely, also may conflict with federal collaboration initiatives and, in some cases, prevent effective information sharing. For example, DHS has little authority to require that state and local governments or other user communities use HSIN for information sharing. As such, department officials often find themselves in a consultation mode with the states. Alternatively, state laws, which may be very restrictive, can limit the ability of state and local user communities to share information through HSIN. Law enforcement communities, for example, are governed by laws that prohibit sharing certain types of sensitive information.

Third, privacy considerations cannot be ignored in the context of information sharing. Specifically, maintaining the appropriate balance between the need to share information and the need to respect the privacy and other legal rights of U.S. citizens can be a difficult and time-consuming effort. Due to privacy concerns, civil liberties organizations have challenged information-sharing initiatives in the past and could pose similar challenges for the HSIN program.

In 2003, the American Civil Liberties Union raised concerns about the Multistate Anti-Terrorism Information Exchange (MATRIX) system, an effort to link government and commercial databases to enable federal and state law enforcement to analyze information as a means of identifying potential patterns of suspicious activity by individuals. As a result of the privacy concerns raised, as well as the costs involved, many state law enforcement communities stopped using the Multistate Anti-Terrorism Information Exchange system.

Failure to consider privacy concerns could result in similar abandonment of HSIN before its full potential is realized. As required by the Homeland Security Act, and in an effort to assuage civil liberty concerns, DHS performed a privacy impact assessment of HSIN portals before deploying them. As a result, DHS had to shut down the HSIN document library which contained reports from nation-wide sources, significantly hampering system usefulness. In addition, DHS is creating another database subject to a privacy impact assessment prior to its implementation. This database will provide intelligence analysis capability similar to that of the abandoned Multistate Anti-Terrorism Information Exchange system. Besides the privacy impact assessment, clear standards and effective controls will be needed to demonstrate to concerned consumer groups that the information gathered through HSIN does not violate the rights of American citizens.

Fourth, a culture that is not receptive to knowledge sharing is one of the foremost hurdles to widespread adoption of the HSIN collaboration software. HSIN users comprise diverse communities, including state and local government officials, emergency managers, law enforcers, intelligence analysts, and other emergency responders. Each has different missions, needs, processes, and cultures. Because of these differences, often the various user groups are reluctant to share information beyond the bounds of their respective communities. Traditionally, for example, law enforcement has operated in a culture where protecting information is of paramount concern. Shifting from this ″need to know″ culture to a ″need to share″ culture has proven difficult. DHS officials anticipated when they first released HSIN that culture might become an issue, but they did not have the time or resources to build the trusted relationships necessary to overcome this issue.

Identifying and understanding such user community goals and requirements are a first step to understanding cultural differences and building collaborative relationships. Frequent communication, guidance on how shared information will be used and protected, effective feedback, and mechanisms for resolving issues in a timely manner can also serve to overcome differences and instill trust and understanding.

Conclusions and Recommendations

DHS has a critical role to play in ensuring national awareness, preparedness, and coordinated response to potential emergency situations, suspicious activities, and terrorist threats. HSIN can assist by supporting timely and relevant information exchange among the federal, state, local, and private organizations that need to share counterterrorism-related data to carry out their respective missions. However, the many system planning and implementation issues, as well as other related challenges, that I have outlined have hindered DHS' ability to fulfill its central coordination role and to provide the communications and IT infrastructure needed to keep our homeland secure.

To ensure the effectiveness of the HSIN system and information sharing approach, we recommended in our report that the Director, Office of Operations Coordination, Department of Homeland Security:

1. Clarify and communicate HSIN's mission and vision to users, its relation to other systems, and its integration with related federal systems.
2. Define the intelligence data flow model for HSIN and provide clear guidance to system users on what information is needed, what DHS does with the information, and what information DHS will provide.
3. Provide detailed, stakeholder-specific standard operating procedures, user manuals, and training based on the business processes needed to support homeland security information sharing.
4. Ensure cross-cutting representation and participation among the various stakeholder communities in determining business and system requirements; and, encourage community of interest advisory board and working group participation.
5. Identify baseline and performance metrics for HSIN, and begin to measure effectiveness of information sharing using the performance data compiled.

The Acting Director, Office of Operations Coordination, concurred with our recommendations in their entirety. Further, the Acting Director noted that the recommendations are solid, and when implemented, will improve the HSIN system and information sharing effectiveness.

Mr. Chairman, this concludes my prepared statement. I appreciate your time and attention and welcome any questions from you or Members of the Subcommittee.

Mr. SIMMONS. I thank you very much for that excellent testimony.

We will go now to Mr. Allen. We will do all three witnesses and then do questions.

Mr. Allen?

STATEMENT OF MR. CHARLES E. ALLEN, CHIEF INTELLIGENCE OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. ALLEN. Thank you, Chairman Simmons, Ranking Member Lofgren. Thank you, Congresswoman Harman, for your kind comments.

I would like to submit a very brief opening statement but request that my written statement be entered into the record.

Mr. SIMMONS. Without objection.

Mr. ALLEN. It is a pleasure to appear alongside Vice Admiral Roger Rufe. As indicated, he has just joined the department a couple of months ago. He is going to bring a lot of experience to the department.

I also would like to recognize behind me Dr. Carter Morris, who is a detailee from the Central Intelligence Agency, who is helping me with information management and information architecture. And without him, I could not have achieved what we have done in the time that I have been at Homeland Security.

To prevent and counter potential threats to the homeland, first responders and front-line law enforcement officers must be armed with the information needed to recognize and defeat threats. Similarly, the Department of Homeland Security must gain the insights

of local law enforcement and emergency personnel as they collect data that are crucial to identifying threats to the homeland.

To this end, under the state and local fusion center implementation plan that I have developed and am in the stage of implementing, my office continues to embed intelligence officers into fusion centers to facilitate the flow of intelligence-related information downward and all-hazards information that is threat-relevant upward to the federal level. Having officers, for example, in New York City as well as out in Los Angeles is making a major difference.

We have been working very closely with Ambassador Ted McNamara, who is the presidentially appointed program manager for information sharing, as well as the Department of Justice, to develop a common framework for the sharing of terrorism and other threat-related information among executive departments and agencies and state and local authorities.

This framework ultimately will strengthen and codify relationships and permit effective interface between intelligence community agencies and the emerging network of fusion centers. The framework will establish a process that ensures the federal government speaks with consistency to state and local partners. I emphasize the term "consistency."

Moreover, we are developing, in coordination with the component agencies and the chief intelligence officer of DHS, an intelligence information architecture that will transform the decentralized and uncoordinated as-is state of the department's intelligence sharing.

Homeland Sharing Information Network, HSIN, is one system we use to fulfill these information-sharing responsibilities with state and local governments and the private sector. Because the DHS Operations Directorate is HSIN's institutional home, I will let Vice Admiral Rufe speak to the overall efforts to strengthen this network.

I intend to share with you, however, specific initiatives to support information sharing using HSIN that I have undertaken. I have initiated all of these projects since becoming the department's chief intelligence officer.

Early in my tenure, we conducted a study on how we could improve the flow of sensitive-but-unclassified intelligence information to state and local authorities. Based on this study and a user-requirement study, we developed and implemented a pilot project to share unclassified intelligence information among the states using the existing HSIN platform.

This project, known as HSIN–Intel, involves six states: Arizona, California, Florida, Illinois, New York and Virginia. We use HSIN–Intel primarily to disseminate current homeland security intelligence information and integrated intelligence assessments, derived both from DHS and the intelligence community's sources.

Let me cite just one example. The day after the 11 July, 2006, attack on the transit system in Bombay, India, my office transmitted relevant intelligence reporting, held a quick-look teleconference with all HSIN–Intel members, and provided valuable information that was not widely available to the public.

In the first 5 months of the pilot operation, my office has posted more than 500 documents on HSIN–Intel, and the states have posted an additional several hundred. Additionally, HSIN–Intel per-

mits us to receive and properly respond to state and local requests for assistance and information.

We are taking steps in partnership with the Operations Directorate to continue to develop this HSIN–Intel pilot program. The pilot runs through the end of this month, in line with the approach that the Office of the Inspector General advocated in the June 2006 report. In fact, launching HSIN–Intel in its pilot form has given the department to road-test business processes to strengthen HSIN–Intel for its rollout.

Whereas HSIN–Intel has emerged as a robust capability for sharing and exchanging valuable and sensitive information, my office also provides intelligence products up to the collateral Secret classification level to our state and local partners through what is known as the HSIN–Secret network.

I assumed management of this program in December 2005. Much like the unclassified HSIN enterprise, the HSIN–Secret system was a troubled, dysfunctional system developed within the department to enhance rapid classified information sharing with the state emergency operations centers, homeland security advisers, state and local fusion centers, and major urban-area police departments.

HSIN–Secret is now available, I am pleased to say, to all state emergency operations centers and a good number of fusion centers. We are, moreover, able to post directly both unclassified and classified threat products, such as Homeland Security assessments, on this new capability. Since August 2005, my office has posted more than 150 products on HSIN–Secret.

But that is not enough; we must do more. Secure connectivity to the states is essential for our collaboration. But HSIN–Secret's inherent limitations constrain us. As an independent network that is not directly connected to the commonly used federal system, the Secret Internet Protocol Network, or SIPRNET, this prevents us from going where we need to be.

In recognition of this, we are aggressively moving to transition from the HSIN–Secret to a truly robust, Secret-level, classified communications network system, the Homeland Security Data Network, HSDN, which is analogous to the Department of Defense's SIPRNET.

With HSDN, government agencies are able to share information and collaborate in order to detect, deter and mitigate threats to the homeland at the Secret level. This new capability will enable our external state and local government and private-sector partners with a Secret clearance to have information-sharing collaboration capacity at that level and allow them to be directly connected with federal users.

We are rolling out HSDN to all state and local fusion centers. I intend to have HSDN installed everywhere I have officers assigned to a fusion center by the first quarter of fiscal year 2007. Yesterday we installed it in the New York City intelligence division at Chelsea. Today we are installing another terminal over at the counterterrorism division in Brooklyn.

In the initial phases of its deployment, only DHS officers will have access, but we plan to expand this to cleared state and local personnel.

In closing, DHS intelligence, like our colleagues in Admiral Rufe's Operations Directorate and the rest of the department, takes seriously its overarching obligation to partner with state, local and tribal authorities and the private sector to share the information needed to protect our homeland.

I believe that in the brief time that Dr. Morris and I have had to take on the issue of establishing a vigorous capability to communicate and share intelligence information with our state, local, tribal and private sectors, we have enhanced significantly our ability to get critical information to these partners. We have put in place an aggressive program that will, over the next year, provide the systems, the networks and processes that will integrate my organization into a fully collaborate environment with the state and local partners.

Thank you, Mr. Chairman.

[The statement of Mr. Allen follows:]

PREPARED STATEMENT OF CHARLES E. ALLEN

Chairman Simmons, Ranking Member Lofgren, Members of the Subcommittee, I am pleased to appear today alongside Vice Admiral (Ret.) Roger Rufe, the Department's new Operations Director, whose 34 years of experience with the United States Coast Guard will prove invaluable in his new mission.

Thank you for inviting me to update you on the progress that the Department has made in strengthening intelligence and information sharing with state, local, and tribal authorities and the private sector through the Homeland Security Information Network (HSIN).

As the DHS Inspector General noted in his June 2006 report on HSIN, ″State and local personnel have opportunities and capabilities not possessed by federal agencies to gather information on suspicious activities and terrorist threats. By working together, the various levels of government can maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks.″ The Homeland Security Act of 2002 gives the Secretary-broad responsibilities to access, receive, and integrate intelligence, law enforcement, and other information from state, local, and tribal government agencies and the private sector; and to disseminate to them, as appropriate, analysis to assist in the deterrence, prevention, and preemption of, or response to terrorist attacks against the United States. The Secretary has delegated these responsibilities to me as Assistant Secretary for Intelligence and Analysis and Chief Intelligence Officer.

DHS has a federal responsibility to develop and disseminate threat alerts, notifications, warnings, and threat-based risk assessments. The audience includes, but is by no means limited to, state and local officials, and other public safety entities; emergency fire and rescue services personnel; public health officials; transportation and coastal maritime security officials; and local government agencies supporting federal efforts to interdict illegal narcotics, alien, and other transnational trafficking activities. This is an important mission that I and the Department are firmly committed to fulfilling.

As vital as HSIN is to the fulfillment of this critical information sharing mission, I should remind you that HSIN is just one of the Department's ongoing efforts to enhance information sharing with our non-federal partners. The Office of Intelligence and Analysis has embraced a comprehensive series of initiatives to improve information sharing with our state, local, tribal, and private sector partners. For example, I have previously addressed before this Subcommittee one of this Department's most important initiatives, the State and Local Fusion Center (SLFC) Implementation Plan. Under this plan, which Secretary Chertoff approved on 7 June of this year, DHS ultimately will embed intelligence and operational personnel in SLFCs to facilitate the flow of timely, actionable, ″all-hazard″ information between and among state and local governments and the national intelligence and law enforcement communities, in support of the President's Guidelines for the Information Sharing Environment. These deployed professionals will form the basis of a nationwide homeland security information network for collaboration and information sharing. My Office is the executive agent for this Department-wide effort. Already we have placed intelligence personnel in fusion centers in Los Angeles, New York City,

Maryland, Georgia, and Louisiana; we are pursuing an aggressive schedule to staff additional fusion centers across the country in accordance with their needs.

Additionally, in accordance with the December 2005 Presidential Guidelines and Requirements in Support of the Information Sharing Environment, we have been working closely both with the Office of the Program Manager for the Information Sharing Environment and the Department of Justice to develop a common framework for the sharing of terrorism and other threat-related information among executive departments and agencies and state and local entities, including law enforcement agencies. This framework ultimately will strengthen and codify relationships and permit the effective interface between the Intelligence Community and the emerging network of fusion centers. Most importantly, this framework will establish a process to ensure that the federal government speaks with ″one voice″ to state and local partners. Consistent with its authorities and mandate, the Department will coordinate with the Department of Justice, NCTC and the FBI to ensure that all ″federally coordinated″ terrorism products are created for, and disseminated to, these partners.

Moreover, under my leadership as the Department's Chief Intelligence Officer, we are developing, in coordination with the component agencies and the Chief Information Officer, an intelligence information architecture. This architecture will transform the decentralized and uncoordinated ″as-is″ state of the Department's intelligence sharing infrastructure by identifying gaps in Department-wide capabilities and other areas where the management of information across the Department, and with our external partners, demands improvement. Through this architecture we will achieve a fully integrated intelligence information sharing enterprise. To implement this plan, we have formed a number of working groups to undertake specific tasks in analyzing requirements, conducting prototyping and piloting of emerging technologies, and initiating the acquisition of necessary capabilities. This effort represents a central thrust of our initiative to improve and optimize information flow both within the DHS intelligence enterprise and between this enterprise and our state and local partners.

Leveraging these additional information sharing efforts with a robust HSIN platform will optimize the ability of the Department to communicate critical information clearly, efficiently, and effectively both within DHS and among its many external partners. That said, the DHS Operations Directorate is HSIN's institutional home, and I will let Vice Admiral Rufe speak to the overall efforts to strengthen and perfect HSIN. However, I want to share with you my Office's initiatives to support information sharing using HSIN and other capabilities.

As I have stated, HSIN plays a major role within my Office's intelligence information sharing program. My analysts, in coordination with the Department's Office of State and Local Government Coordination, each of the Department's operational components, other Federal agencies with homeland security functions, and the National Counterterrorism Center (NCTC), routinely post products to HSIN's law enforcement, emergency management, international, and state and local intelligence communities.

The Department filled a vital near-term requirement and mandate by moving rapidly to establish network connectivity to all 50 States, many major cities, and five U.S. territories by December of 2004. However, significant time constraints encountered in meeting the ambitious roll-out plan did not permit DHS to do all that it would have ideally wanted to do before launching the system. Nevertheless, as the system has and continues to mature, the Department remains committed to improve its usefulness and accessibility.

Shortly after becoming Chief Intelligence Officer of DHS, my Office conducted a study on how we could improve the flow of Sensitive but Unclassified (SBU) intelligence information to the State and local environment. In November and December 2005, my staff also conducted a user requirements study, including a survey of state and local fusion centers, and used the results to develop a concept of operations and an interim governance structure for more effectively moving information between my Office and our state, local and private sector partners. Based on this we have implemented a pilot project to share unclassified intelligence information with and among the states using the existing HSIN platform-this project is known as HSIN-Intel.

The HSIN-Intel pilot project involves six states: Arizona, California, Florida, Illinois, New York, and Virginia. The participants include senior representatives from the intelligence offices supporting the Homeland Security Advisors, leadership and senior analysts of state and local fusion centers, and senior major urban area law enforcement executives from each of the respective states. The pilot governance structure is managed through a steering group of the participants, ensuring direct input from the participants into the development of the system. DHS Intelligence

uses HSIN-Intel primarily to disseminate current homeland security intelligence information and integrated intelligence assessments derived both from DHS and Intelligence Community sources. DHS Intelligence personnel also are able to access, receive, and analyze law enforcement and intelligence information provided by the state and local partners; fuse this information with national intelligence and other information; and report threat information back to the State and local participants for action. Finally, through HSIN-Intel, DHS Intelligence personnel are able to receive and promptly respond to state and local requests for assistance and information that are passed via the HSIN-Intel portal.

In addition to the ″finished″ intelligence products-that is, products which contain analytic assessments and which have been fully vetted-DHS Intelligence also provides through HSIN-Intel unevaluated, or ″raw,″ homeland security-related reporting, such as Homeland Intelligence Reports. In the first five months of the pilot operation, my Office has posted more than 500 documents on HSIN-Intel and the states have posted an additional several hundred.

We are taking steps in partnership with the Operations Directorate to continue to develop this pilot program in line with the approach that the Office of the Inspector General advocates in its June 2006 report. In fact, launching HSIN-Intel in its pilot form has given the Department the opportunity to ″road-test″ business processes and functional capabilities that could be used to further strengthen the larger HSIN enterprise. To that end, we have taken steps to ensure that any law enforcement or other sensitive homeland security related information shared throughout the HSIN-Intel portal is appropriately handled and that all parties understand and apply the rules in order to achieve the appropriate protections to their data.

Among its more immediate benefits, HSIN-Intel users have greater situational awareness of worldwide terrorism events. For instance, the day after the 11 July 2006, attacks on the transit system of Bombay, India, my Office transmitted relevant intelligence reporting, held a ″quick-look″ teleconference with all HSIN-Intel members, and was able to provide valuable information that was not already widely available to the public. We are looking forward to transitioning this program to full operational capability in the near term, and will continue to work directly in that regard with the customer based steering group and the Operations Directorate.

Whereas HSIN-Intel will continue to develop a robust capability for sharing and exchanging valuable and sensitive unclassified information, my Office also provides intelligence products up to the collateral SECRET classification level to our State and local partners through what is known as the HSIN-Secret network, or HSIN-S. Much like the unclassified HSIN enterprise, HSIN-S also was developed within the Department to enhance rapid classified information sharing with State Homeland Security Advisors, emergency operations centers, state and local fusion centers, and major urban area police departments. Through HSIN-S, we are able to post directly both unclassified and classified threat products, such as Homeland Security Assessments, on systems accessible by many of our state and local partners. Since August 2005, my Office has posted more than 150 products on HSIN-S.

Secure connectivity to the states is essential for our collaboration, but HSIN-S's inherent limitations prevent us from going where we need to be in this regard. In recognition of this, we are aggressively moving to transition from HSIN-S to a more robust Secret-level classified communications network system-the Homeland Security Data Network (HSDN). HSDN is analogous to the Department of Defense's Secret Internet Protocol Network, or SIPRNET. With HSDN, government agencies are able to share information and collaborate in order to detect, deter and mitigate threats to the homeland at the Secret level. This new capability will enable our external state and local government and private sector partner with a Secret clearance to have information sharing collaboration capacity at that level. We have already begun to roll out HSDN to all state and local fusion centers. I intend to have HSDN installed everywhere I have officers assigned to a fusion center by the first quarter of Fiscal Year 2007. In the initial phases of its deployment, only DHS officers will have access, but we plan to expand access to appropriately cleared state and local personnel.

In conclusion, DHS Intelligence, like our colleagues in Admiral Rufe's Operations Directorate and the rest of the Department, takes seriously its obligation to partner with state, local, and tribal authorities and the private sector to share the information needed to protect our homeland. As a member of the Intelligence Community, my Office also is working closely with the Office of the Director of National Intelligence, the Office of the Program Manager for the Information Sharing Environment, the National Counterterrorism Center, the Department of Justice, the FBI, and others, to create efficiencies and interoperability among the existing intelligence information systems to enhance our collaborative efforts.

To prevent and counter potential terrorist attacks, first responders and front-line law enforcement officers must be armed with the information to recognize and defeat the threat. Similarly, the Department of Homeland Security must gain the insights of local law enforcement and emergency personnel as they identify trends and patterns involving potential threats to our Homeland. The networks we implement must serve this flow of information. I look forward to answering your questions.

Mr. SIMMONS. Thank you.

Admiral Rufe?

STATEMENT OF VICE ADMIRAL ROGER T. RUFE, JR. (RETIRED), DIRECTOR, OPERATIONS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Admiral RUFE. Good morning, Mr. Chairman, Ranking Member Lofgren, members of the subcommittee. I am Roger Rufe, director of the Department of Homeland Security's Operations Directorate.

I am pleased to appear today alongside the department's assistant inspector general, Frank Deffer, and the department's chief intelligence officer, Charlie Allen. Thank you for the opportunity to update you on the Homeland Security Information Network.

While I have already had the pleasure of meeting with a few of you, I welcome the opportunity to meet with each of you personally and listen to your thoughts as we move forward on our important work together.

I was appointed director by Secretary Chertoff in July of this year. I am a 34-year career veteran of the United States Coast Guard, with experience commanding five Coast Guard cutters, as well as being commander of both the Atlantic area and the Pacific area of the Coast Guard. I know first-hand the importance of effective information sharing in coordinating and responding to emergency situations.

In my written statement, I describe some recent steps the Office of Operations Coordination has taken to improve the effectiveness of the Homeland Security Information Network.

I accept the major findings of the inspector general. Our customers found HSIN difficult to use, and, rather than struggle with the system, they quickly resorted to pre-existing means of acquiring and sharing information through phone calls and e-mail. These are all valid complaints, and we are focused on fixing them.

We are going to use the I.G. report as a catalyst for change. We are moving forward to implement needed program oversight and management, and we have engaged our federal, state, local and tribal partners to better understand how we can design the system to address their requirements and ensure that HSIN becomes a user-friendly and useful network that will enhance information sharing with state and local officials.

In my view, the most critical shortfall in the HSIN program has been its lack of programmatic discipline. I don't think we can be too harsh on those who saw the need to rush out the system, however. We need only recall the holiday threat stream in December 2003/January 2004 to remember the pressure to develop an information-sharing network.

However, we are now moving forward in a more calculated, measured way to a program management that will ensure the long-term viability of the program. Critical to the improvement and suc-

cess of HSIN will be hiring a well-qualified program manager who possessed the skills and experience to guide this effort.

To receive formal input from our various customers, DHS is moving to establish the Homeland Security Information Network Advisory Committee. This advisory committee will initially include 14 representatives from federal, state and local governments and the private sector, including homeland security advisers, law enforcement, fire services, public health, emergency managers, and the private sector.

This group will provide organizationally independent advice and recommendation to me and other DHS leadership on the requirements of the various end users. A notice on the establishment of this advisory committee should be published in the Federal Register early next month.

Another key point in the I.G. report was that HSIN's mission and vision and its relationship to other systems were not adequately defined. The inability to identify what HSIN is and how it is used is at the root of the disconnect between our customer base and DHS.

Since April 2006, early this year, we have been hard at work in developing the common operating picture, or the COP, a situational awareness tool that displays key information and data that will enhance decision-making. The COP is still in the development stage, but it is operational for sharing information related to hurricane response and recovery. The Homeland Security Information Network is the means by which the department's common operating picture is shared with other partners.

In mid–August, the National Operations Center and the HSIN team, in conjunction with the department's Preparedness Directorate, executed a major information-flow exercise. Using a hurricane exercise, we instituted an information flow that tested and evaluated the information-flow reporting processes during a simulated national incident using HSIN and its common operating picture/common operating database.

This successful exercise included participation from the National Infrastructure Coordinating Center, the National Response Coordination Center, and the Baton Rouge, Louisiana, Joint Field Office.

The chief goal of the exercise was to establish the effectiveness, efficiency and operational value of this system's information-sharing processes for all levels of the government. Our goals included identifying gaps with the existing information-sharing procedures and protocols for the National Operations Center and addressing each of the DHS components' core mission competencies.

Lessons learned from this exercise were documented, and many changes deemed critical were implemented prior to Tropical Storm Ernesto's arrival shortly thereafter. The information flow improvements were evident and were further refined during the real-world tropical storm?that is Ernesto.

In the course of rolling out the COP to state emergency operations centers, FEMA operations centers, and other locations, we have found a renewed interest in HSIN. Some of our improvements to make the system more user-friendly, such as single-user sign-on and more useful desktop features, have garnered some positive comments from the field.

We will continue to make improvements in HSIN technology, but I recognize that the more difficult improvements will require the development of policy; articulating a clear vision; a sound and proven information-sharing processes; and a business model that supports the Homeland Security Information Network.

I realize?and the I.G. report bears this out?that all of these efforts need to be coordinated closely with our federal, state, local and tribal partners.

Finally, Mr. Chairman, I would like to invite you, other members of the subcommittee, and your staffs to visit us at the National Operations Center to see how we use the Homeland Security Information Network and the common operating pictures.

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

[The statement of Vice Admiral Rufe follows:]

PREPARED STATEMENT OF VICE ADMIRAL ROGER T. RUFE, JR., (RETIRED)

Good morning, Mr. Chairman, Ranking Member Lofgren, and Members of the Subcommittee. I am Roger Rufe, Jr., Director of the Office of Operations Coordination at the U.S. Department of Homeland Security (DHS). I am pleased to appear today alongside DHS's Chief Intelligence Office, Charlie Allen. Thank you for inviting me to update you and your subcommittee on the status of the Department's Homeland Security Information Network (HSIN).

While I have already had the pleasure of meeting with a few of you, I welcome the opportunity to meet with each of you personally and listen to your thoughts as we begin this important work together on a vision for many successful future endeavors.

I was appointed Director by Secretary Chertoff in July of this year. I am a 34-year career veteran of the United States Coast Guard with experience commanding five Coast Guard cutters in the Pacific and Atlantic regions in addition to being commander for both the Atlantic and Pacific areas. As a result, I know firsthand the importance of skilled operations in coordinating and responding to emergency situations.

Overview

As you are aware, HSIN is the primary, secure nationwide network through which DHS receives and shares critical information, including alerts and warnings, with its components and its public- and private-sector partners, including Federal, State, local, and tribal officials and the owners and operators of critical infrastructures. HSIN allows these parties to communicate on suspicious activities, threats, and infrastructure vulnerabilities; prepare for and mitigate natural or manmade disasters; and collaborate on restoration and recovery efforts following a serious incident. This is a system that has the potential to improve vertical and horizontal homeland security information sharing.

DHS agrees with the five recommendations in the DHS Inspector General's June report on the HSIN program. Since this report focuses on interactions with State and local governments, I will restrict my comments to those communities of interest.

From the Office of Operations Coordination perspective, HSIN has not realized its full potential because it lacks many aspects of a typical Federal government program. As noted in the report, the urgency to roll out HSIN meant that several critical elements of the program-such as a requirements definition, program goals, milestones (metrics), and an evaluation of user needs-were not thoroughly addressed.

Lacking the benefits from a more detailed planning process, HSIN suffered from inadequate program oversight and management. To address this, Operations Coordination is creating an HSIN Program Management Office, headed by an experienced GS-15 to manage all aspects of the program.

But even before the final IG report, DHS had identified several shortcomings and had developed initiatives to aggressively address those shortcomings. As can be seen in our response to the IG's recommendations, we implemented a series of these initiatives to support the long-term success of HSIN. Significant, measurable progress is being made in these areas.

We believe that the IG's report is a catalyst to improve HSIN.

We also believe that input from our Congressional partners, and especially this Subcommittee, will be invaluable in defining the systems and processes for our

homeland security. Toward that end, let me reassure you that the Office of Operations Coordination will continue to work closely with Congressional partners; our DHS partners such as Assistant Secretary of Intelligence and Analysis Charlie Allen, Assistant Secretary of Infrastructure Protection Robert Stephan; and other partners to identify areas for improvement. Together we will work to ensure HSIN becomes a better homeland security information sharing tool.

Recent HSIN Accomplishments

In addition to and in conjunction with the IG report recommendations, there are two areas of recent attention that deserve highlighting because they are critical to the success of HSIN: efforts with our users and system enhancements.

Being Responsive to the User Community

It is always important to listen to the needs of the users. To that end, DHS is moving to establish the Homeland Security Information Network Advisory Committee. This advisory committee will initially include 14 representatives from Federal, State and local governments and the private sector including: homeland security advisors, law enforcement, fire services, public health, emergency managers and the private sector. This group will provide organizationally independent advice and recommendations to me and other DHS leadership on the requirements of the various end users. A notice on the establishment of this advisory committee should be published in The Federal Register in early to mid-October.

Under this year's HSIN State Expansion Initiative, the HSIN Team has redoubled its efforts to address the specific technological and training needs of today's and tomorrow's State user communities. During a typical deployment to a State, the team conducts a series of meetings with the appropriate officials to explain HSIN's tools and capabilities and to develop a State site to meet officials' needs. This year, the team has constructed 24 sites for the States. It is important to note that the HSIN capability is provided at no cost to the State.

As an example, the HSIN Team fulfilled the Commonwealth of Massachusetts' requirement for a cost-efficient and secure system to exchange information. The team worked with the Massachusetts Commonwealth Fusion Center to integrate the Commonwealth's existing tools into the HSIN website.

Since October 2005, the team has completed 10 training sessions in Massachusetts and now HSIN serves over 2,200 users in all counties of the Commonwealth. Users of the Commonwealth's website include: Commonwealth, county and municipality police; the Commonwealth Homeland Security Advisor's Office; Commonwealth emergency management officials; Commonwealth critical infrastructure personnel; Commonwealth fire services personnel; Commonwealth emergency operations center personnel; and others. As we all know, priorities can change and the HSIN Team can easily modify the State site to reflect those changes upon request.

Offering special support to State governments for hurricane preparedness efforts in light of the Hurricane Katrina aftermath, DHS has deployed the HSIN Team to 17 States throughout the Gulf Coast and East Coast. The team provides HSIN training to State Emergency Operations Center (EOC) principals and staff members to ensure they are prepared to utilize the system during emergencies.

More specifically, team members train EOC employees on HSIN's tools, which include geospatial mapping, a search engine which queries the HSIN portal, Request For Information (RFI) and FYI options, and document management functions. In early August 2006, the HSIN Team provided technical support and HSIN Common Operating Picture (COP) training at the Principal Federal Official exercise, conducted at the Emergency Management Institute in Emmitsburg, Maryland.

In mid-August, the National Operations Center (NOC) and the HSIN Team, in conjunction with the Preparedness Directorate, executed a major information flow exercise. The Hurricane Ennis Information Flow Functional Exercise tested and evaluated the information flow reporting processes during a simulated national incident using HSIN and its COP/Common Operating Database (COD). This successful exercise included participation from the National Infrastructure Coordinating Center (NICC), the National Response Coordination Center (NRCC) and the Baton Rouge, LA Joint Field Office (JFO). The chief goal of this exercise was to establish the effectiveness, efficiency and operational value of this systems information sharing processes from all levels of the government. Other goals included identifying any gaps with the existing information sharing procedures and protocols for the NOC and addressing each of the DHS components' core mission competencies. Lessons learned from the ″Hurricane Ennis″ exercise were documented and many changes deemed critical were implemented prior to Tropical Storm Ernesto's arrival. The information flow improvements were evident and had positive effects during this real world Tropical Storm.

A functional exercise like this enabled DHS to apply real-time emergency communications in a simulated environment. HSIN's capabilities functioned as they were

meant to-and ensure that during crises, each State EOC has the means to communicate and collaborate through site posting, threaded discussion, secure chat conference rooms, or instant messaging with the Joint Field Office (JFO), FEMA's Regional Response Coordination Center (RRCC) and National Response Coordination Center (NRCC), and DHS's National Operations Center (NOC). Also, it is important to note that these capabilities allow for inter and intra-state collaboration during crises.

Just as important as having functional, efficient communications during Federal hurricane response efforts, is having staff that can easily use HSIN. To ensure that, specialized DHS teams have trained personnel in HSIN use at the NRCC, the RRCCs, JFOs, Federal Departments and Agencies with Emergency Support Function (ESF) roles, NORTHCOM, various Federal operations centers including the Department of Energy, the Department of Health and Human Services, the National Guard Bureau and the White House Situation Room.

Better Communicating with the User Community

In an effort to better communicate with the State user community, we have taken a number of steps including holding educational conferences and updating reference materials. For example, we held a User's Working Group meeting in February 2006 at the Pennsylvania Emergency Management Agency facility in Harrisburg. This two-day meeting was attended by multiple representatives from the initial eight pilot States.

We are also scheduled to brief and demonstrate HSIN at the Fusing the Fusion Centers conferences in September and October. The conferences will be held on a regional basis, ensuring that officials from the same regions meet, network, and discuss issues impacting their area. Input and recommendations received at the conferences will be compiled and shared with fusion center leaders and related Federal agencies.

To further augment support materials available on the website, the HSIN Team has updated the HSIN frequently asked questions document, the fact sheet detailing the most recent changes in the program, and is publishing monthly bulletins. These bulletins contain up-to-date information on program activities and articles describing how HSIN is being used to support day-to-day and special operations. These and other materials will help ensure that users better understand the HSIN mission and have the most current materials at their fingertips.

In addition to the conferences, three meetings have been held with HSIN State and local community representatives and HSIN briefings have been provided to the Major Cities Chiefs, the International Association of Police Chiefs, and the National Sheriffs' Association.

Upgrading the System

HSIN is currently introducing a series of infrastructure upgrades that will improve the system's speed, reliability and capability. These upgrades will increase user capacity and operational ease as well as the system's responsiveness. For example, the user interface has been improved to permit single sign on to all communities of interest on all national and state websites. All communities of interest sites have been given a common look and feel, and the nomination and validation of new users have been simplified and made expedient. Additionally, to ensure system availability, DHS has implemented a survivable infrastructure, using two geographically dispersed systems. Hopefully this configuration change will be fully implemented by first quarter FY 07.

The newest capability on HSIN is the National Operations Center's Common Operating Picture (COP). Eventually, the COP will provide all HSIN users nationwide with the capability to view and share critical information from a common operating database for crises and significant events. This means that officials in various parts of the Federal government and across the country can share situational understanding and make informed decisions on such topics as asset deployment and evacuation, in addition to just monitoring a situation.

The COP development is an incremental build that was initially focused on this hurricane season. Thus, current access to the COP has been prioritized at the Federal level while ongoing training efforts have reached into FEMA's Regional Response Coordination Centers and the Joint Field Office in Louisiana. The intent is to provide COP access and training to all partners at the Federal, State, local, tribal, and private sector nationwide. HSIN/COP was recently fully accredited--meaning adequate security controls are in place.

Though these upgrades are vital, the underpinning for system improvement is the hiring of a HSIN Program Manager. As related in our response to the IG report and earlier here, the importance of the programmatic responsibility of HSIN will be elevated. The Program Manager, working with end users, will ensure that performance

metrics are established and instituted. The Program Manager will engage all HSIN stakeholder groups to assess deficiencies in training materials and SOPs and ensure that adequate training materials and support are available to optimize the effective operation of this system. This person will ensure that HSIN development becomes a fully collaborative process among other Federal, State, local and tribal partners and is consistent with the Information Sharing Environment required by the Intelligence Reform and Terrorism Prevention Act. The efforts of the HSIN Program Manager will include:

- Aligning DHS and National Operation Center (NOC) missions
- Coordinating the approach to Federal, State, and local stakeholders and partners centering on increased engagement
- Providing stakeholder-specific SOPs, CONOPs and educational information to HSIN users
- Coordinating the HSIN Advisory Committee to obtain increased stakeholder advice
- Using earned value management (EVM) measurements to determine the effectiveness and use of HSIN information sharing and collaboration.
- Having daily interaction with other DHS and Federal agencies to share leads to ensure the unified delivery and exchange of information among our partners.

Conclusion

Mr. Chairman, be assured that DHS is committed to ensuring that all viable recommendations on system improvement are elevated and acted upon and that the needs of the end user are met. We will continue to work together with all partners to ensure we have the best system possible.

The IG's report has been helpful in identifying areas of needed improvement and, as noted earlier, efforts are underway to address the issues raised.

I would hope that you continue to have a desire to learn more about HSIN and DHS's other information sharing efforts. If your time allows, we would enjoy the opportunity to host a visit by this Subcommittee and staff to the NOC to learn more about HSIN in a ″hands on″ manner.

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

Mr. SIMMONS. Thank you for that testimony.

And the noise that you have heard is the call for votes. So I would like to at least get one or two questions in?maybe we can get several more?before we have to break.

I would like to take the liberty of referring to a subsequent testimony of the second panel by Mr. Hay.

Is he here today, by any chance? Yes, thank you.

He makes the comment, "Can the public sector truly engage all the resources available by the private sector before, during and after a disaster?" And then he says, "The short answer is an emphatic no. The public sector has approximately 750,000 personnel. The private sector has over 2 million private security professionals," et cetera, et cetera. And then he says, "The government?DHS, FBI, DNI?are still not yet aware of the enormous potential for intelligence and information sharing via the private sector."

I make those references in advance to going back to your testimony, Mr. Allen, where, on page 7, you talk about secure connectivity being essential and moving aggressively toward a more robust, Secret-level classified communications network system. And then you refer also to extending Secret clearances to those within the system.

And what I am looking at here, and my questions is, that we have this fundamental problem. We have a Homeland Security Information Network that needs to be improved. It seems to me, Mr. Allen, that part and parcel of your improvements go to the issue of making it more secure and getting more clearances for people in

the system. And we know how difficult that is, since the clearance process is bogged down by almost a year.

In contrast to that is testimony from one of our other witnesses saying, "Hey, there is a whole world of folks out there, eyes in the field, boots on the ground, ears in the community, that aren't going to have those Secret clearances, that are not connected into this system."

And so, my question to all three of you is, you know, which model are we following here? And which model is going to work best over the long term?

You know I am an advocate of open-source intelligence. You know I am an advocate for that sort of approach to these issues. But it does seem to me that we have got a fundamental disconnect here that is worth exploring.

Mr. ALLEN. Mr. Chairman, I think you asked, as usual, very tough and candid questions.

First, on the outreach?and we will get to the open source as a second part?but on the outreach at the classified level to both state and local governments, we are actually getting a lot of clearances.

My own office has taken on significant responsibility to clear people in police departments, fusion centers. We are doing it on a regular basis. I cleared 50 officers alone for New York City, which is a phenomenal increase, an exponential increase. We are doing it around the country: Las Vegas, California.

We are also working very closely with the infrastructure protection side of DHS, with George Foresman's side of the organization. And we find, and not surprisingly given your experience in intelligence, that many of the people in the private sector not only have Secret clearances, they have Top–Secret SCI clearances.

And as a result, many of the people with whom we deal and interact at the sector level, they not only receive our Secret-level products and read them, but they are briefed regularly. We bring the sector leaders in. So we are working very hard to ensure that the information flows out.

We are also trying to get sensitive communications out to certain sectors on a very select basis, where we know that secure communications with leaders in the private sector will benefit the security of the country. This is something I don't advertise, but I am doing it. And it is unique; it has not been done previously. But we are giving some of these secure communications to key people in the private sector who have huge responsibilities. And I would prefer not to mention them in an open session. I would be happy to talk to you offline.

On the second question, getting the information from the local level?and open source is clearly an area where we must do better. And I developed and will be presenting to you later this year our open-source approach to this.

But at the same time, by putting our officers down into each of the state and local government fusion centers?38 of them, by the end of fiscal year 2008?there is going to be a lot of culling and sending of information at that local level and getting it to the federal level. Because we want to get all that information that is a suspicious nature. Some of it seems suspicious and is not, but we

need to cull and filter and bring that information back to the state level.

A lot of information already flows in through the HSIN network from the state and local government, as well.

Mr. SIMMONS. Thank you. This is an issue that I think we will pursue in subsequent questioning.

Ms. Lofgren?

Ms. LOFGREN. Mr. Deffer, earlier this summer we learned that the Secure Flight Program, which we were told cost $120 million, was, due to planning and I would say mismanagement, grounded or, in the words they said, rebaselined.

And last year we learned that the Homeland Secure Data Network, a $337 million program, was rushed and "that the speeded-up schedule prevented the department from completing critical system development requirements."

Now we find that this $50 million computer network basically is junk.

What is going on over there, in terms of planning and development of these information systems?

Mr. DEFFER. Well, part of it is?and we talk about this in our report?there was a rush to get something done. So when that happens?

Ms. LOFGREN. But this isn't the first time. I mean?

Mr. DEFFER. It is not the first time, and it is, you know?I have been looking at this for 22 years. I was at GAO, and I looked at the systems over and over again. And it gets repeated, and for some reason sometimes in government they just don't get it, and they try to rush things through and don't follow the disciplined processes that?you know, laws were established for you to follow certain ways to get things done: identify requirements, develop an architecture, and bring it together into a system that works.

And in some cases they do it well; in some cases they don't. I think, in this case, they?

Ms. LOFGREN. Well, we haven't learned about a case where they have done it well yet, although we would like to.

Mr. DEFFER. I can't think of one off the top of my head.

[Laughter.]

But it is a constant problem in the federal government. And the answer, it comes from OMB and the Hill to force the agencies to follow these disciplined processes and to get it done.

Ms. LOFGREN. On the JRIES system, about a year ago we were told that the JRIES executive board had just broken off discussions with DHS, and they really terminated the effort to assimilate JRIES into the Homeland Security Information Network.

Now, I understand?I would like to know if you know whether this is true?that the JRIES executive board wanted to limit who would have access to HSIN because they had concerns about non-law enforcement access, possible misuse of HSIN, possibility of security breaches, privacy violations, as well as user confusion, and that the department really wanted broad use.

And that, in reaction, the JRIES executive board is now, I guess, marketing, if that is the right word, a JRIES–2 concept for virtual intelligence analytical unit that only trusted law enforcement officers would have.

Isn't that kind of a major blow to what DHS has been trying to do? Where does this put our efforts?

Mr. DEFFER. It is. You are right, there is a dustup between the JRIES executive board and operations coordination. And the executive board pulled out of it because they were concerned about expanding it too quickly to law enforcement and not putting security controls in place.

And I have heard about this JRIES–2. I am not exactly sure where it is going. But it is troubling, because, again, it establishes another system out there for someone else to use. And I think the whole idea of HSIN is to have a one-stop shopping, one place where people can go to get the information they need to do their mission in homeland security. So it is troublesome.

Ms. LOFGREN. I wonder if Mr. Allen and Mr. Rufe could comment on that, if you are able.

Mr. ALLEN. I would like to comment, but Admiral Rufe should comment first.

Ms. LOFGREN. Okay.

Admiral RUFE. Okay. Thank you. Yes, we were disappointed that it didn't work out with JRIES, as well, but it was for a variety of reasons.

We proposed an MOU with JRIES, and there were some statutory requirements that we were obligated to fulfill, including the Anti–Deficiency Act, Homeland Security Act, and they were unwilling to accept those limitations that we had statutorily.

I should point out, as well, that JRIES is a good system, but it is a single-use system; it is a law enforcement system. And it is relatively limited in terms of the users that it can take on. Now, maybe the second level will allow them to take on more users.

But we were obligated to put together a system that was nationwide in nature; was open to a wide variety of users; and could also accommodate not just law enforcement but emergency management, carrying of other types of information. It is a much broader and substantial system than JRIES was able to accommodate.

Mr. ALLEN. Yes, Congresswoman, I want to strongly support?and I think Admiral Rufe has truly answered your question. It is a much broader capability.

I believe the way this was handled was not at all effective, the way the JRIES–HSIN dispute grew up. And I think that has occurred; should have been handled much better.

I do believe that for getting information down and building a strong system for intelligence sharing at the sensitive-but-unclassified level, which will meet some of the law enforcement officials' capabilities, will be this experiment I am running with HSIN–Intel. This intel portal directly off of HSIN I think will prove to be a great success.

Ms. LOFGREN. If I could just do a quick follow-up, Mr. Chairman, and I know then we have to go vote, but the concern I have and what we have been advised is that law enforcement officials that have been interviewed by the I.G. just don't trust the system. They don't think that the system is secure and that their sources will be protected, privacy data will be secured.

And if that is the case, what I see is not one?I mean, if you can't give that level of security, you end up with what the I.G. is report-

ing now not being used?that will be used and the inability to actually fuse, as is your vision.

So what is the answer to that, Mr. Deffer?

Mr. DEFFER. Well, first of all, the technology is there to make this work. This is not an issue of, "Do we have the system? Do we have the software?" This is Web-based, and you can secure that. And so, that has to be pointed out to the JRIES executive board.

And down the road, I think they need to be brought back into the fold. It is people and process. You have people involved; they have didn't views of how to do this. And then you have processes that are not real clear about how to share information.

You have got to, sort of, get them all on the same sheet of music, as to what HSIN is for and explain that it is going to be more than law enforcement, but that law enforcement case information will be protected. And that can be done with current technology.

Mr. ALLEN. Let me just add to that. Admiral Rufe and I and Secretary Chertoff recently met with six of the major city police chiefs. We are rolling out a new agreement with those police chiefs by the 1st of October, and a great deal of the emphasis was just on the point you made: the need for a trusted relationship between Homeland Security and the chiefs of police and for good, strong, secure, sensitive-but-unclassified networks that will protect law enforcement information. We are very sensitive to this.

Mr. SIMMONS. We are about out of time to go vote.

Ms. LOFGREN. Yes.

Mr. SIMMONS. I would ask the ranking member if she wishes to address additional questions to the panel on our return.

Ms. LOFGREN. I think, in view of the time and the fact that we want them to be working on this, we should go to the second panel and submit whatever questions further we have in writing.

Mr. SIMMONS. That being the case, we release the panel. We go on about a 20-minute recess. If folks want to get a cup of coffee or whatever, feel free. And we should be back here by 2:10.

The subcommittee stands in recess.

[Recess.]

Mr. SIMMONS. The subcommittee will come to order.

We are now pleased to have the second panel.

And we have with us here today Captain Charles Rapp, director of the Maryland Coordination and Analysis Center, or MCAC if you like the acronyms. He achieved the rank of captain in 1998, was assigned to command the Towson precinct, which houses the county seat and many government buildings. He was detailed in March of 2006 as the director of the MCAC, where he now oversees the fusion center and its components.

Good to have you hear, Captain.

We also have Mr. Ian Hay, president of the Southeast Emergency Response Network Interim Governance. He was elected by his private-sector constituents to his current position. The Southeast Emergency Response Network is the southeastern component of the joint DHS–FBI Homeland Security Information Network–Critical Infrastructure Program. It is headquartered in Atlanta, and the network covers one of the largest FEMA regions, with a population of approximately 51 million people.

Additionally, we have Ms. Maureen Baginski, director, BearingPoint Intelligence Sector. She has 27 years of service in the United States intelligence community and served from 2003 to 2005 as the FBI's executive assistant director for intelligence, where she was responsible for establishing and managing the FBI's first ever intelligence program, including technology acquisition and workforce development.

She is the recipient of two Presidential Rank Awards; two director of CIA national achievement medals; the director of military intelligence leadership award; the National Security Agency's exceptional civilian service award; and the first ever recipient of the National Security Agency's outstanding leadership award, an award voted on and bestowed by the NSA workforce. Very impressive.

Why don't we start with you, Captain Rapp?

STATEMENT OF CAPTAIN CHARLES W. RAPP, DIRECTOR, MARYLAND COORDINATION AND ANALYSIS CENTER

Mr. RAPP. Thank you, Chairman Simmons.

Chairman Simmons, members of the subcommittee?

Mr. SIMMONS. And I should mention that we will have a timer, so if?we have your statement; if you want to summarize, we can get into questions.

Mr. RAPP. I thank you for inviting me here today. I am Captain Charles Rapp, currently serving as the director of the Maryland Coordination and Analysis Center, as you referred to as MCAC.

MCAC is an intelligence fusion center that merges federal, state and local resources from 16 different agencies. The center serves a dual function in gathering information through a 24-hour Watch Section and analyzing that information in our Strategic Analytic Section to produce actionable intelligence.

The Watch Section takes tips from a toll-free number and logs those tips in one of several databases depending on the nature of the information. They might also contact the Joint Terrorism Task Force directly if they need to have the tip acted upon immediately.

They also act as Maryland's liaison with the Counterterrorism Watch and the National Operations Center, as well as other fusion centers. In addition, they monitor federal and state databases and public news sources to identify emerging issues that may affect Maryland.

The Strategic Analytic Section staff is from a variety of federal, state and local agencies, as well. They are responsible for analyzing data, interacting with analysts in other fusion centers, and producing comprehensive and reliable intelligence bulletins and threat assessments.

Two of the analysts in the section are tasked with coordinating and analyzing data regarding the national capital region, which keeps us connected to this Urban Area Security Initiative.

Maryland has developed the MCAC to be the conduit through which all critical intelligence information passes to public safety agencies in the state. To consolidate functions, we have centralized the location that agencies can contact to gather information from multiple sources. This allows law-enforcement officers to receive information from multiple databases with one call while remaining focused on their safety and eliminating multiple requests.

It can provide fire services and other agencies information before arriving on a scene so they are better prepared for an event, minimizing the intrusion into personal contacts while safeguarding individual rights.

The Department of Homeland Security has participated in our center, providing the protective security adviser who has been invaluable in navigating some of the intricacies of the DHS system. This position has helped us develop pathways for information flow for many of our critical infrastructure segments. The private sector has many key elements that must be included in any plans to safeguard communities.

Secondarily, assigning a DHS part-time analyst to our center has added depth to our operation and availed our center of information and training that has proved beneficial.

Information sharing on the federal level has improved dramatically over the past several years. There has been a noticeable surge in the volume and quality of intelligence exchanged. The joint collaboration of federal, state and local resources in the fusion center has led to the unprecedented sharing of information.

Fusion centers have fostered the human factors that play a crucial function in information sharing. Knowing the appropriate people to contact and having an established relationship with that person is still one of the most effective ways to share information.

This concept has also created some challenges for us. Federal agencies have also begun to centralize their core information functions into consolidated points. From a state fusion center standpoint, this has created problems in contacting multiple centers and monitoring their databases for information. In some cases, the information reported is redundant, appearing multiple times in several databases. Often it is not accompanied by analysis and frequently is not timely.

Another challenge has been the classification issue. As I am sure you are aware, classified information is often difficult to sanitize and still remain useful. Information that has been sanitized to the point that it can be shared has often lost its ability to be actionable. In addition, it appears that, many times, information is unnecessarily classified with no clear reason.

Another significant challenge is the lack of a universal handling system. Handling caveats are interpreted differently by many agencies. This is another value of the fusion process, which minimizes the number of handlers of information and allows the fusion centers to interpret caveats and then distribute information to those who have a need to know.

Fusion centers should become the focal point in each location for the sharing of information and disseminating it to their community. Currently the director of the Governor's Office of Homeland Security receives most of the critical alerts from DHS. While it is important that they have the information, the fusion centers should also be notified by DHS concurrently.

Secondarily, federal agencies need to recognize that fusion centers have valuable information that could benefit the overall knowledge base. Information developed at the local level can be analyzed and vetted best by those who are familiar with the communities where the information originates.

The Homeland Security Information Network provides good intelligence products for research. However, it does not seem to be populated with current information that would be of benefit to a fusion center.

DHS has recently contacted our center about installing a new network referred to as HSDN. This could provide better information and I hope will be a portal to other fusion centers. One of the most important features of a network would be to let fusion centers talk to each other in times of crisis in a secure network.

A final challenge will be to develop training for fusion centers. For analysts, this training would focus on the intelligence cycle and the difference between typical crime analysis and intelligence gathering and analysis. This is critical to bring the mix of analysts assigned to fusion centers and intelligence units to a common understanding of function. This will enhance their abilities to communicate and develop usable products that translate into actionable intelligence.

In the future, I would look for other intelligence agencies to streamline intelligence and share it by using the least number of networks possible. Ideally one network would channel all intelligence information from the federal agencies to the state fusion centers.

We need to develop a universal lexicon for handling caveats. In addition, we should make every effort to classify information at the lowest level possible to maximize its value and share it with a wider community. We also need to increase the number of state and local leaders that have obtained clearances. This would provide more informed leaders the ability to make better decisions.

Finally, the sustainability of fusion centers needs to be addressed at the federal and state levels. Relying on grant funds is not a beneficial method of operating these valuable centers. Long-term planning then becomes problematic.

I would like to conclude by noting that each of the fusion centers I am familiar with have a unique structure tailored to meet their state's needs. While they may be structured differently, they need to be supported by all levels of our government, because their functionality and value are critical to our national security.

Thank you for allowing me to address you, and I welcome any questions you have.

[The statement of Captain Rapp follows:]

PREPARED STATEMENT OF CAPTAIN CHARLES W. RAPP

The Maryland Coordination and Analysis Center was launched in November 2003. The Anti-Terrorism Advisory Council Executive Board (ATAC) acts as the policy oversight body for the center. The center involves the resources of federal, state and local entities. With the policy oversight and leadership of the ATAC Executive Board, the center was designed to have a structured organization that was not controlled by any one agency. That is why I sit before you as a detailee from a local police agency, currently serving as the Director of Maryland's Intelligence fusion center. The center serves a dual function in gathering information as well as analyzing that information to produce actionable intelligence.

In Maryland this function is carried out as follows.Our center is divided into two sections. The Watch Section is a 24 hour, seven -day- a- week function where tips and other information are tracked. This section is commanded by a Lieutenant from the Maryland State Police and consists of 21 personnel from 16 different agencies. The center operates two toll-free lines designed to solicit reports of any suspicious activity which may involve a terrorist or criminal threat. The Watch Section logs

the tips, and attempts to determine if they are valid. Information and tips are entered into databases for follow up by the Joint Terrorism Task Force (JTTF) or by the appropriate agency. Information involving possible links to terrorism that require immediate investigation are sent to the JTTF, by contacting a supervisor who will then assign a task force member for immediate response and investigation. MCAC also may communicate directly with the Terrorist Screening Center and pass information to officers on the street. This allows the street officers to focus on their safety while we research the issue they contacted us about.

A second function of the Watch Section is to monitor information networks and public sources in order to track events that may be occurring. When the events may possibly have an impact on Maryland or its infrastructure, the Watch Section personnel notify management of the center and senior leaders on the ATAC. This allows us to begin planning for the events impact on Maryland and alerting resources to mobilize for the event if necessary. Examples of some of the information networks monitored are Joint Regional Information Exchange System (JRIES), Homeland Security Information Network (HSIN), Regional Information Sharing System (RISS), public news sources and other sites that may be prudent to the nature of the event(s) that are occurring.

The second section of the center is the Strategic Analytic Section (SAS). This section is commanded by a SSA assigned to the FBI. The SSA has responsibility for the analysts in this section as well as the analysts in the Field Intelligence Group (FIG) for the FBI. The SAS section is staffed by analysts from the FBI, State, Local and National Guard agencies. In addition, two of the analysts funded by the Urban Area Security Initiative (UASI) are assigned to coordinate data regarding the National Capital Region. The analysts review many products and information sources and interact with analysts in other fusion centers to provide comprehensive and reliable intelligence bulletins and threat assessments. These products are then formatted for the appropriate audience. As one innovation they have developed products that have been abridged for time-restricted briefings such as law enforcement roll calls.

Maryland has developed the fusion center to be the conduit through which all critical intelligence information passes to public safety agencies in the state. To consolidate functions, we have developed as a central location that agencies can contact to gather information from multiple sources with one contact. This allows public safety officers to develop information from numerous databases while they remain focused on their safety without having to make multiple requests. It can provide the fire service and other agencies information before arriving on a scene so they are better prepared for the event. And it minimizes the intrusion into personal contacts while safeguarding rights.

The joint collaboration of federal, state and local resources in the fusion center has led to the unprecedented sharing of information. The development of the fusion centers model is an ideal organization for the collection and dissemination of intelligence. In an effort to expand this model on a national scale, many agencies have centralized their core information functions into a consolidated point. This centralized center collects and distributes this information to its partners for their use. From a state-wide fusion center standpoint, our problem is monitoring all of these national centers and their intelligence dissemination. In some cases the information is redundant, reported multiple times by different networks. In many cases the information is not accompanied by analysis. In other instances the information is not timely and its value is diminished proportionately.

Another problem with the sharing of information has been the classification issue. As I am sure you are aware, classified information is often difficult to cleanse and still remain useful and be disseminated to those who need it. It appears that many times information is unnecessarily classified with no clear reason. However, information classified at any level is useless if it cannot be shared with those who have a need to know and can take action based on it's contents. Information that has been cleansed to the point that it can be shared has often lost its ability to be actionable.

Another significant problem is the lack of a universal classification system for information not classified by statute. When dealing with agencies at every level it is not uncommon to find that different classification terms have different meanings to different agencies. The classification terms need to be standardized for clarity and efficiency.Clearly, this is one value of a fusion center to interpret the meaning of these classifications and properly disseminate the information to those who have a need to know.

Information sharing on the federal level has developed dramatically over the past several years. There has been a noticeable surge in the volume and quality of intelligence exchanged. The Department of Homeland Security's Homeland Security In-

formation Network (HSIN) posts information that can be used by analysts and provides other links to obtain more in depth information from sources. It is an information network that could also service a number of communities when a critical event is occurring. Currently, the system does not seem to be populated with information on a timely basis. Most of the information obtained from HSIN is historical and usually is posted too late to be of benefit to a fusion center. Homeland Security also uses the HSIN-S system which my center does not have access too at this time. This system contains information that may be developed and used at the secret level. My understanding is that these systems are currently being combined into one system that will provide a better linkage for information sharing. We are currently engaged in talks with DHS to have the HSDN system installed in our fusion center. However, it is my understanding that only DHS analysts will have access to the system at this time. When the DHS analysts are not present, this will present a problem. I encourage DHS to allow access by appropriately cleared fusion center personnel as soon as possible.

From the standpoint of my fusion center, I would encourage future databases to be housed under one system. Consolidating information and having fusion center personnel enter as few systems as possible to elicit information making sharing of information more efficient. This also provides the fusion centers a centralized location to report information. This would allow state fusion centers to be responsible for the dissemination of information to the proper consumers and make the dissemination more timely and responsive to community needs.

Fusion centers should become the focal point in each location for the sharing of information and for disseminating it to their consumers. Currently, the State Homeland Security Advisor receives most of the critical alerts from DHS. While it is important that they have the information, the fusion centers should also be notified by DHS concurrently. In addition, fusion centers need to have connectivity to talk freely and share information and resources. This may be a benefit of a joint information network, possibly a product of HSDN. They also need to build a solid relationship and sharing protocol so in times of crisis, a timely free flow of information will occur. In times of crisis, this information flow from fusion center to fusion center will be critical.

The flow of information also needs to work in the reverse. As fusion centers mature information must flow in both directions. Federal agencies need to recognize that local and state agencies have valuable information that could benefit the overall knowledge base. Information developed at the local level can be analyzed and vetted best by those who are familiar with the communities where the information originates. The information can then be sent through the state center to the national center(s). This allows the national center to review the information in the context of the national and international arenas and determine if the information ties into any broad threats that may require action.

Another advantage of fusion centers and the expansion of information sharing has been the personal relationships between local, state and federal employees. Knowing the appropriate person to contact and having an established relationship with that person is still one of the best ways to facilitate the flow of information. And by developing the human interaction, many of the problems associated with a system that lacked credibility are now being bridged. Even in our age of technology, this is still one of the most reliable methods of building solid information links that lead to reliable, actionable intelligence.

Two other programs from DHS have been very beneficial to our center as well. One is the Protective Service Advisor who has been invaluable in navigating some of the intricacies of the DHS infrastructure. This position has also helped us develop pathways for information flow from many of our critical infrastructure segments. The private sector has many key elements that must be included in any plan to safeguard communities. Likewise, the information they collect and use can be very beneficial in designing overall threat plans. The second has been the assignment of a DHS analyst to our SAS section. While part-time at this point, this analyst has added depth to our operation and has availed our center of information and training that has proved beneficial. In addition to any information sharing systems, these types of linkages are essential to develop working relationships among agencies. These important roles also work to bridge the gaps between federal and local partnerships.

Another critical area for state and local centers is the development of training for analysts and for managers that run fusion centers and intelligence units. For analysts the training would focus on the intelligence cycle and the difference between typical crime analysis and intelligence gathering and analysis. This is critical to bring the mix of analysts assigned to fusion centers and intelligence units to a common understanding of functions. This should also enhance their abilities to commu-

nicate and develop usable products that translate into actionable intelligence. For managers, training should allow for an increased understanding of the role of intelligence, the need to know, and to minimize conflicts in information sharing.

In the future, I would look for DHS and other intelligence agencies to find a way to coordinate intelligence sharing by combining information into the least number of networks as possible. Also in limiting the number of national intelligence centers. Then developing a national system of classification that allows for the maximum dissemination of intelligence to the lowest levels possible. This national system should provide for a universal classification lexicon for information. In short, not only do we need to be on the same page, but speaking the same language. We should also increase the number of state and local leaders that have obtained clearances this will allow more leaders the ability to share information at the classified levels. Leaders at all levels need to be comfortable with their decisions when addressing potential threats, but under the current system, the tear lines sometimes do not contain sufficient information to make an informed decision. Often these decisions involve significant disruptions of community activities and the communities demand reasons for the decisions. Often these reasons cannot be shared in detail, but local leaders need to be confident with the information used to make a decision, because they are frequently asked to defend them.

Additionally, the sustainability of the fusion centers needs to be addressed at the federal and state levels. Relying on grant funds is not a beneficial method of operating these valuable centers. Long-term planning becomes problematic. Turnover of personnel increases training costs and impacts experience levels. Leadership changes can have an enduring detrimental impact on centers particularly in the early stages of development. These issues must be addressed to insure that these centers will thrive and provide integrated layers of security for our country.

I would like to conclude by noting that each of the fusion centers I am familiar with have a unique structure tailored to meet their state's needs. While they may be structured differently, they need to be supported by all levels of our government because their functionality and value are critical to our national security.

Thank you for allowing me to address you and I welcome any questions you have.

Mr. SIMMONS. I thank you for that testimony

Mr. Hay?

STATEMENT OF MR. IAN M. HAY, PRESIDENT, SOUTHEAST EMERGENCY RESPONSE NETWORK (SEERN) INTERIM GOVERNANCE

Mr. HAY. Thank you, Mr. Chairman and Ranking Member Lofgren. I want to thank you for your invitation today, as it is both an honor and a privilege, especially given this subject.

And I would also respectfully request that my written testimony be submitted into the record.

Mr. SIMMONS. Without objection. It is long, with a lot of interesting quotes. I don't know how you are going to summarize it, but do your best.

[Laughter.]

Mr. HAY. Well, I will endeavor to be brief.

Mr. SIMMONS. Okay.

Mr. HAY. And so, since you already know about SEERN, let me begin with my task here this afternoon. And that is that we simply cannot tolerate a "have" and "have not" homeland security world. It can't be fee-based. It can't be some club that we join that you get better information than if you are a general member of the private sector.

We need one system. We need one system that the federal government uses to communicate with the private sector.

And thirdly, we need the leadership, we need the president, Secretary Chertoff and FBI Director Mueller to stand up at one podium and say, "This is the system we are going to use for communicating between the government and the private sector."

So we need to engage the private sector, as you mentioned earlier, Mr. Chairman, because it is almost three times more likely to see the street-level terrorists. Further, in Atlanta, we learned that their incident reporting is typically 10 to 15 minutes ahead of first responders'.

How are we going to do this? Well, state and local is the answer. We have to establish the preeminence of the state and local relationship, ideally I hope through the state fusion center.

We need to facilitate that understanding of critical infrastructure and its potential loss and economic impact, in that case.

Third, we need to create self-sufficiency. By driving it through the state and local, we will avoid another Katrina, because the people who are there are going to be the ones who have to deal with the situation.

So, moving on to the HSIN–CI background, I think there is really little I need to say here. The I.G.'s report says it all. We had very similar experiences.

And on June 30th, we completely changed the rules on our customers. We took what was largely a push and quiet network and turned it into a login portal with the new technology?something our customers were not used to. They were used to attached documents, not having to log in and get their information. And that is why only 2,200 members have re-vetted in that program. That is a disaster.

Second, we were promised early delivery. And, in reality, we reviewed that product 7 days before its launch. Now, as a former software salesman?and I hesitate to say this; I am not trying to place blame?I think it is the entire contracting system, the way the federal government does this, that caused this problem. Because, as a software salesman, I never would have let it happen.

I think, lastly, we were crippled by the volunteer structure. There wasn't enough paid staff, and they simply couldn't execute these great plans from the private-sector leaders.

Specifically with regard to SEERN, you know, we had a unique background. We were the first pilot established under DHS Secret Service, as opposed to the FBI. We elected an interim governance. The remaining programs, I think, were all appointed. And sadly, we had three program managers in less than a year. That was a real problem, in terms of continuity.

And also, DHS leadership, who came into town in August?General Broderick, the entire brass, the national governance leaders?came a year ago, and they have not returned since. You know, Katrina is an obvious?I understand that it is an obvious excuse as to why they couldn't come back. However, we need them to return.

Finally I will close the SEERN experience with two excruciating examples. One is Georgia's food and agriculture?you know, they left their Food and Ag ISAC, their Intelligence Sharing and Analysis Center, in an attempt to save Georgia taxpayers some money. And what happened is its HSIN–CI didn't live up to what they were promised.

And they still, to this day, have no tool in which to communicate to that vital community. Now, with Georgia having the number-one

poultry-producing state in the nation, can you imagine the impact of bird flu, avian flu, or even just simple international trade?

Secondly, the Water and Waste Water organization is completely fed up. They have recently considered disengaging from the program and designing their own system.

So what is SEERN's vision? Well, SEERN's vision is that even despite the program's stilted beginning, we honestly believe that we have the right players in the room and that we will be able to repair it.

I think, without fixing it, the nation will never develop one clear and united common operating picture for the private sector. Right now we have about 15, with different ISACs, trade associations, et cetera. We need to have that one common operating picture that the secretary is looking for.

And so, while I find it surreal to be making a request before Congress for 10 items, I hope you will bear me out.

The first is, we need to establish a HSIN–CI oversight committee and have the right people on it.

We need to request private-sector leadership and input. We need to organize. Perhaps consider the FACA guidelines and, above all, ensure geographic diversity from across the nation.

We need to select one technology and get the administration's full support behind it.

I think we should strongly consider rebranding the program as HSIN–Private Sector.

Fifth, we need a joint DHS–FBI announcement that this is the one program, and begin to operate on that one sheet of music.

Sixth, we should re-engage the private sector by securing three contacts for each Fortune 1,000 company for that database.

We should also recruit two points of contact from every state, ideally from the state fusion center, and train them adequately.

Eight is we need to resolve the issues with the DHS–FBI MOU and really consider bringing the DNI to the table, as well.

Ninth, we need to let individual regions choose their unique style of governance, and then let them develop information products which best serve their constituencies.

Ten, we need to at least double the funding and recruit a realistically sized staff, both in Washington, D.C., and in each of the regions.

So, in conclusion, Article I comes first in the Constitution for a reason, and we desperately need the members to help us expand our capabilities and ideally reach out to their constituencies. We need to fully engage the private sector and remove this "have" and "have not" world. Let's make state and local the answer, driving the program through state fusion centers. And we really need that one system.

To borrow from General Washington, "While I have not grown blind in my nation's service, my beard is definitely more gray. I am tired."

We need more help. We simply must act quickly.

And in the immortal words of Sir Winston Churchill, "Please give us the tools, and we will finish the job."

And, Ranking Member Lofgren, I will say that I am not above fishing in that sewer for the change that we might have lost. Be-

cause I think we are all at the right table and we are moving forward.

I sincerely thank you for your service to the nation and your time and attention today.

[The statement of Mr. Hay follows:]

PREPARED STATEMENT OF MR. IAN M. HAY

Chairman Simmons, ranking member Lofgren and distinguished members of the Subcommittee, I want to thank you for your invitation; as it is both an honor and a privilege to be here today, especially so, given the topic and the imminently pressing matter of our Nations' Homeland Security. Testifying before Congress, has been a dream of mine that truly solidified during my studies as a Government Major (now political science) at Beloit College in Wisconsin.

I further appreciate the Subcommittee indulging the miniature State flags of HSIN-CI SEERN (FEMA Region IV) during my testimony; as it is paramount to me that we remain sharply focused upon who our organization seeks to protect. As each of the Members is acutely aware, heading into the final months of the election season, it is only through the consent of the governed that we have the pleasure and honor of serving our constituents.

I appear before you today because Critical Infrastructure (CI) is life. . .And the clock is ticking.It is ticking against Critical Infrastructure due to our enemies' determination and because we now find ourselves fully into the 5 to 7 year operational time horizon in which our enemy has historically executed their attacks. This is not to be sensationalist in any form. I say this because it is excruciatingly clear to me that if we fail to fully engage and integrate the private sector into our Homeland Security operations; 'we may fail to connect the dots.' We may very well, inadvertently, miss a critical piece of information which 'might' just prevent the next disastrous attack.

For this reason, my goal here today, is to share some critical insights into private sector information sharing, then shift to SEERN's experience with the HSIN-CI program and then finally, turn to a ten point section for some potential solutions; in the form of direct and specific requests of the Subcommittee and the Federal Government.

As I begin to lay out this case, I realize full well, that if fail to convince the Honorable Members of the true power of the private sector, I will have failed to impart how the 'eyes' of the private sector generally see things that would turn the average intelligence professional green with envy. I will have missed an opportunity to describe the truly awesome nature and nearly endless resources the private sector can bring to bear, in any given crisis.

In short, I will have failed to help secure that vital 85% Critical Infrastructure, solely in the hands of the private sector; upon which we depend for our daily lives.

No Infrastructure, No Economy. No Economy, No Government

Returning to my initial thesis, the fundamental miscalculation many people make is not recognizing the role Critical Infrastructure plays in our daily lives and our complete and total dependency upon it. That is. . .until it is gone. Without power, we cannot operate the machines and tools necessary to drive our economy. Without technology our financial systems and telecommunications fall back to the dark ages. Without fuel there is no transportation and, thus, no paycheck. And, without potable water, there is no life.

An attack upon any one of these Critical Infrastructure sectors, is likely just effective as an attack upon a soft target, such as a mall, school or nightclub. I would further assert, that the Governors and Mayors of our great States and Cities, have only had a small taste of the potential impact on local economy, tourism and families that the devastation would likely cause, if the infrastructure is disrupted (perhaps with the exception of New York or those in the Katrina region).

Aside from the obvious income factors of our constituents, why do we care?

The 'Have' and 'Have Not' Worlds of Homeland Security

We care, because right now we have 'two Homeland Security worlds' in our country. One 'have' and one 'have not'. In the 'have,' the private sector must pay additional money, on top of their taxes, fees and expenses that they already pay to remain compliant.

In the 'have not,' they feel their taxes ought to be enough to provide for their general security, and so they refuse to pay more (potentially at their peril). Imagine for a moment, what the average private sector organization must contemplate when

it comes to security? Should one pay $10,000 - $15,000 in order to become part of a 'sector specific' Information Sharing and Analysis Center or (ISAC)?

Or, perhaps, that same money would be better spent by hiring a security director, either from, or well connected to, law enforcement, the military, Homeland Security or the Intelligence Community? Or, rather still, should they spend that same money, on a top flight physical or operational security consultant? Tough, tough choices, especially when the increasing cost of security whittles down shareholder value.

This section could alternately be entitled, ″The Over-Crowded Marketplace: Private Sector Outreach, Alert Networks, Information Sharing and Analysis Centers (ISACs) and Consultants.″I mention this because there are far, far too many options the private sector must choose from, all of which generate more questions than answers.

The options for the average Security Director are truly dizzying when you consider them. He or she must ask: ″should I join an ISAC? Do I need to become a member of trade organization, such as ASIS International, Building Owners and Managers Association (BOMA), or Business Executives for National Security (BENS)? Should they sign up for a Regional Information Sharing System - Automated Trusted Information Exchange (RISS-ATIX)?

Or perhaps, simply consider whether this 'free' membership under the HSIN-CI umbrella will cover all the bases and provide for all the business needs? Before we move toward answering this vital question, I beg the Members attention for one final point.

Private Sector—Our Greatest Asset

Can the public sector truly engage all the resources available from the private sector before, during and after a disaster?

The short answer is an emphatic, 'no.' It's simple math really, if we accept that the country has roughly 750,000 law enforcement personnel; and the private sector has roughly 2,100,000 private security professionals (let alone, the number of security savvy employees out there); we can calculate that the private sector is almost three times (2.8 to be exact) more likely to interface with a 'street-level' terrorist than the average public sector agent or first-responder is.

This math is further illustrated, by an exercise conducted in Atlanta, last November called 'Target Midtown,' a simulated attack upon mass-transit. Within minutes of the Business Operations Center (BOC) being 'stood up,' we quickly discovered that the private sector was reporting street level movement and terrorist operations about ten to fifteen minutes ahead of first responders. Further, they were doing so from multiple vantage points via a variety of different communication methods (mobile phone, two-way radio, email, text message, phone camera, and instant messenger).

I specifically mention this because I fear that without fully engaging the private sector in information sharing and Intelligence we will categorically fail to find the next perpetrators in time, before the next 'Big Attack.' And this time, five years after 9/11, I fear the numbers could be staggeringly larger than those already heavy losses suffered on September 11, 2001.

The Government, DHS, FBI, and the DNI are still not yet aware of the enormous potential for intelligence and information sharing via the private sector. Therefore, we must encourage, develop and exercise these capabilities if we ever hope to secure our Critical Infrastructure from harm.

To finally bring this point home, I suggest the following example. Imagine if you will, five city map puzzles with 100 pieces each: Washington, New York, New Jersey, Philadelphia and Boston, all scrambled together, 500 pieces. While there obviously exists, the potential for 'too many chefs in the kitchen,' which option would you choose to solve the puzzle, if it were your loved ones directly involved in the threat picture?

Would you prefer one or perhaps, two Top Secret cleared intelligence analysts from inside the Beltway?

Or would you prefer five teams of three generalists from within the actual local jurisdictions?

Realizing that this example is simplistic; the lesson is both important and accurate. Because the private sector is able to see the puzzle from more angles they can potentially solve the puzzle more quickly. The problem still remains; however, that the private sector may not know, or understand what the threat is and, thus, the completed puzzle is almost worthless to them. They have no idea what to look for within the puzzle.

I burden the Members with this mental exercise because it is simply not enough just to stand up a piece of technology like (HSIN-CI) and hope for the best. We have

to organize the people within the jurisdictions and teach our vetted membership what to look for, or we will never 'connect the dots in time.'

WILL HSIN-CI BE THE ANSWER?—THE HOMELAND SECURITY INFORMATION NETWORK—CRITICAL INFRASTRUCTURE (HSIN-CI)

Local knowledge = Regional Strength = Homeland Security (HSIN-CI Motto)

In The End—State and Local is the Answer

The only way to avoid another disjointed response similar to Hurricane Katrina; will be to drive this program via State and Local Governments, primarily through the State Fusion Centers, ideally to accomplish the following three things:

1. Create the preeminence of the State and Local relationship with the local and regional Critical Infrastructure and its leaders.
2. Support working groups to facilitate a direct understanding of Critical Infrastructure and the potential economic impact within the State and Local jurisdictions.
3. Most important, develop a local self-sufficiency planning model. In the event of a terrorist attack or natural disaster, each sector will need to be mentally aware of what action steps and requirements their respective sectors will have.

It is safe to say that it will be the State, Local, and Critical Infrastructure players who will experience the brunt of the event. Our job should be to ensure both parties (public and private) are fully prepared and integrated within the local jurisdiction, before anything happens or any kind of response is required.

A shining example of how important this concept of local operations is; would be the use of the National Emergency Resource Registry (NERR) during a disaster. If State and Local representatives are fully trained on the NEER, they will have the power to search the database for critical resources 'within' their affected region by zip-code and find their requirements, locally; ideally before FEMA needs to become involved in the acquisition of resources 'outside' the region.

Autonomous Local and Regional Governance

If State and Local is the answer, then prior to any technology delivery, we must let each region chose how to organize their Governance. Only the locals know the 'lay of the land,' the personalities, and, thus, should choose the Governing body to represent them with assistance from program management.

SEERN's Unique Background

SEERN's original program manager, Craig Caldwell, took this approach to heart and identified a group of almost 40 individuals drawn from each of the 17 Critical Infrastructures local to Atlanta.He and the original Infrastructure Advisory Panel (IAP), as it was named at the time, called for nominations and held elections. These elections, held May 20, 2005, resulted in an Officer corps of nine individuals to represent the 3,000 plus members of SEERN, in an interim capacity for two years; or until such time, as a region-wide election could be held.

As far as we are aware, SEERN is the only 'active' region to date, to hold such elections, as the other pilots' regional Officers have been appointed by HSIN-CI program management.

Furthermore, SEERN is one of largest FEMA regions, with eight contiguous States, six of which are hurricane prone. This means SEERN must interface with eight separate State Governments while the average regions are typically comprised by five or six. We must also keep in mind that we have an extremely active region and we will likely require more staff and resources to serve the members properly.

Lastly, despite our repeated requests, SEERN was never able to host a full regional 'All Hands' meeting, in order to bring key leaders from across the region to help organize a more representative SEERN Governance. We also were promised an 'official launch' with a proper announcement from the Secretary of DHS that never came to fruition. That one single event would have boosted our outreach across the region unlike any other initiative imaginable.

Continuity and Proximity of Program Management

SEERN was also the only pilot launched with a program manager from DHS - United States Secret Service (USSS), as the other program managers were drawn from the FBI. To date, SEERN has had a total of three different program managers in less than one calendar year (One from the USSS, and two from the FBI).

This is simply unacceptable. The lack of continuity in program management has seriously stinted SEERN's growth and continues to erode the support from the founding members who have invested a significant amount of time developing the program. Regardless of what management model we choose, we simply must get ev-

eryone on the same page and moving in one direction (like Washington crossing the Delaware).

In late August of 2005 the DHS leadership and National Governance Officers came to Atlanta and SEERN had one of the best Regional Governance turnouts in our history. Since that time, DHS has not returned in a year; and while the devastating impact of Hurricane Katrina is a fair excuse, it is high time the leadership returned to region, to get the program back on track. I honestly fear that we will need to completely 're-sell' the program in order to avoid losing key people.

Lastly, while there are certainly advantages to locating the HSIN-CI National Program Office outside of the beltway, not having representation or key staff close to DHS headquarters in Washington, D.C. will continue to set the program up for failure. The DHS leaders from the key areas: Operations Directorate, Private Sector Office, Intelligence Analysis and the Office of State and Local need to meet more regularly if we are to have any hope of developing and expanding the program.

Governance - Are Volunteers The Answer?

A structure of pure volunteerism, unsupported by professional and paid staff is critically flawed. Relying exclusively upon volunteers meant only a few key leaders were doing all the heavy lifting, working into the wee hours and simply could not dedicate the time necessary to execute all the tasks that needed to be accomplished in a timely fashion.

This is not to say there is no place in the program for volunteers; however, any Governance model DHS leadership and program management contemplates, really ought to be significantly more geographically representative and should strongly consider using the Federal Advisory Committee Act (FACA) standards to oversee its operation.

Finally, no matter the form or structure, the program Governance simply must be adequately supported by program staff, in order to accomplish the important mission of the program.

SEERN Continues to Lack Adequate Resources

From the beginning SEERN has consistently lacked sufficient resources to conduct its operations and the vast majority of travel has been 'paid out of pocket,' by volunteers. And, these are but a few examples. We consistently have to rely upon the generosity of the local private and public sector for conference call bridges and meeting space. After two long years, SEERN still has no printed promotional material, business cards, etc., in which to conduct our vital outreach.

We have long made a joke in SEERN that HSIN-CI is one of the best kept secrets both inside and outside the beltway. We have been stunned by how few people are actually aware of the program, whose main source of PR appears to be generated 'virally' across the region and the nation one person at a time.

Perhaps our greatest challenge is the vetting process for the 900+ 'pending' members of SEERN, some of whom have waited in the 'pending' cue for more than a year. We neither had the resources, nor the time to recruit a sufficient number of gate keepers, to keep up with the ever increasing applicants. Further, the number of 'pending' applicants was so vast (nearly a one-third of the total SEERN membership), that the backlog was honestly insurmountable without significant administrative assistance.

Push Network Vs Login Portal - The New Technology

On June 30th, 2006 we changed the rules on our customers. What once was a 'quiet' and 'push' network, overnight became a 'login portal.' This is not to say the portal is devoid of value, it has some significant advantages such as a master calendar and some great collaboration tools.

However, it is a question of what our membership base was accustomed to. At no time did they ever have to 'login' to get information, as the previous technology 'pushed' the information out via email text and attached documents. If we are going to change the rules, we need the time, resources and staff to help explain the new approach and train the members on the new technology.

The 're-vetting' of the membership on the new ManTech system was also a crippling issue as well. While we should always strive to ensure any 'imported' member is confirmed via the 'double opt in' standard, we simply cannot expect a senior executive to spend 25-30 minutes out of their busy day, re-vetting their HSIN-CI account. We need to find a faster and more robust solution, to safely vet and yet, still quickly process our applicants.

Lastly, the Subcommittee needs to be aware that we were promised in early 2006, that the technology would be ready and delivered early. The truth was that we reviewed the technology only Seven days before we were due to launch and go live with the new system. If this had been the Space Shuttle, wouldn't we have tested

it? Do we honestly think we would have launched that vehicle under similar circumstances? Never.

Will 'One Size Fits All' Information And Intelligence Products Really Work For The Private Sector?

At least in Atlanta, SEERN was never able to get to the stage where we could fully engage all the informational resources available to us, particularly the strong intelligence component of the FBI's Field Intelligence Groups (FIGS) or the local/regional State Fusion Centers within our region.

Our hope, was to create new information products for our private sector customers who have literally been forcing down same old 'gruel,' which arrives in the same form and has become even more diluted over time, than the original IAIP Daily report we started with in 2004.

We must survey our membership and identify their needs. We need to consider State by State and regional reporting, for those with narrow requirements; as well as, multi-regional reports for those members who have more broad responsibilities.

In short, we need to add some much needed substance to our morning oatmeal. . .

DHS—FBI Memorandum Of Understanding (MOU)

I sincerely look forward to a day when DHS, DNI, and FBI have a mutually binding MOU(s) to share information, resources, staff and accountability. Only by getting these and other organizations on the same sheet of music will we ever approach integrated Homeland Security.

With the exception of a few occasions, at almost at every turn, the program has been forced to 'stand down', while we waited for some element of DHS or FBI to 'buy into' the next stage of the program before we could move forward.

We need to resolve this quickly, and the sooner the better. . .as this 'stop - start' approach will result failure and continue the lack of trust felt by the private sector.

The True Cost of Failed Implementation

I'll close this middle section with two excruciating examples:

1. According to the current Food and Agriculture Representative to Georgia's Homeland Security Task Force, their sector still continues to wait for one national platform in which to communicate with their constituency. This Administrator was told that SEERN HSIN-CI's Food and Agriculture sector was going to come to fruition and provide their organization with the same information as the Food and Agriculture ISAC. In their attempt to be responsible and save the Georgia taxpayers from paying for duplicate information, they ended their participation in the ISAC. When HSIN-CI didn't live up to its promise, this group lost critical information and still to this day, does not have one centralized 'tool' to communicate with their vital membership.

In the wake of a potential Avian Flu epidemic, or the impact a Food or Agriculture event would have on daily international trade, this situation is simply unacceptable.

This and other groups need one clearly recognized tool, with a national platform provided by the federal government.

2. Anything short of a unified and well supported network brings us to the second example. A Water and Waste Water organization, has become so fed up with the successive delays of HSIN-CI; that they have recently considered disengaging from the program and designing their own system because they can no longer afford to wait for the Federal government to get its act together.

This is a preposterous situation and simply must be resolved, or it will continue to generate additional 'incomplete' choices, in an already over-crowed marketplace of alert network solutions.

SEERN's VISION—THE ROAD AHEAD—ABOVE ALL ELSE: ACTION!

Vision of SEERN

As the grotesque image of the World Trade Center falling into Manhattan Island retreats into the rearview mirror of our consciousness, SEERN has a sharp eye toward the future. Our focus is on a day where we are more secure than ever because we did hard work upfront. We strived to establish the best relationships and oversight. We performed the hard labor of meeting, planning and integrating both the public and private perspectives in our approach.

We will succeed where others have failed because we will have exchanged business cards before the event even happens. We will move stridently forward: Knowing we have access to the full 'bench strength' of the private sector; knowing we can build a robust alert network, capable of reaching our vetted members by 'any means necessary;' knowing we deliver the best information possible, in a format our private sector partners actually use and finally; knowing our partners will in turn share

what they observe and become that 'x' factor multiplier that helps the region and the nation develop one clear and united Common Operating Picture (COP).

The Ten Requests

As we continue to move forward and identify the best solutions, I respectfully request the Members of the Subcommittee consider the following potential solutions:

1. Establish a DHS HSIN-CI oversight committee, Co-Chaired by Director, Admiral Rufe, Homeland Security Operations Directorate, and Al Martinez Fonts, Undersecretary, Private Sector Office. Further comprise this committee with Chet Lunner, Office of State and Local, and Charlie Allen, Undersecretary of Intelligence Analysis (and anyone else the Subcommittee deems appropriate).

2. Request Private Sector leadership and input. Charge this committee to create a Private Sector Advisory Board under the Federal Advisory Committee Act (FACA) Guidelines. Find someone who is well known and respected by both the public and private sectors alike to head it. Be sure the committee finds individuals from each of the key infrastructures and that this group is drawn with geographical diversity from across the nation.

3. Select a technology. Whether it is the current ManTech software, the previous vendor YHD, or even a different system, let's be sure it works for our private sector members and then put our full support and leadership behind it.

4. Consider a program name change and re-branding as 'HSIN-Private Sector.' It will become clear the private sector members something has significantly changed and, yet still maintains the HSIN nomenclature which the public sector has now become accustomed to.

5. Make the statement in the open and in the press that this is the ONE system the Department of Homeland Security is going to use to communicate with the private sector, period. Request that President Bush, Secretary Chertoff and Director Muller jointly announce the program and its important mission to the country themselves.

6. Secure three contacts from each Fortune 1000 company and enroll them into a database. Let's commit to testing this databases efficacy by December 13th, 2006.

7. Recruit at least two points of contact from each State in the Region (ideally within the State Fusion Center or Homeland Security Advisor) to be trained on the system and act as the direct local conduit for the private sector.

8. Request that Secretary Chertoff and Director Muller (and or their staffs) meet to identify the problems with the DHS - FBI MOU and resolve them quickly. Perhaps consider bringing the Director of National Intelligence to the table as well.

9. Let the individual regions choose their unique style of Governance with some basic guidelines under FACA. Assist them with developing information products which best serve their constituencies.

10. We need to double the funding and recruit a realistically sized staff, both in Washington, D.C. and within each region. We'll need the Members to get behind the program and directly help spread the word in their respective districts to bring the public and private sectors together.

Article I comes first in the Constitution for a reason; and we desperately need the Members to help us expand out capabilities and ideally, assist us by reaching out to their constituencies.

Conclusion

In conclusion, we need to fully engage the private sector and use their sharp eyes to help us 'connect the dots' and ferret out the 'would be' attackers before it happens.

We need to drive the program via State Fusion Centers ideally with the help of individual Members from within their districts.

We need more resources, structure, and a heavy dose of commitment & leadership from the administration. Without it, we are going to lose significant participation and the whole program will have to be 're-sold' at a later time, with a significantly greater cost.

While I have not grown blind, my beard has definitely grown grey in my service to my country. . .In the immortal words of Sir Winston Churchill: ″Give us the tools and we will finish the job.″

Chairman Simmons, ranking member Lofgren and distinguished Members of the Subcommittee, this concludes my prepared remarks.

I sincerely thank you for your service to the nation and your time and attention today. I will leave the Capitol today knowing each of the Members will continue this vital and important work of the Subcommittee and I would be delighted to take your questions.

Mr. SIMMONS. Thank you. We will look forward to the questions. Ms. Baginski?

STATEMENT OF MAUREEN BAGINSKI, DIRECTOR, INTELLIGENCE COMMUNITY SECTOR, BEARINGPOINT

Ms. BAGINSKI. Thank you. Chairman Simmons, Ranking Member Lofgren and subcommittee members, thank you very much for having me here today to talk about this very important issue of information sharing and enabling technology.

As you said, Mr. Chairman, I do have 27 years of experience working in the U.S. intelligence community, during that time most recently at the FBI but also at the National Security Agency for 25 years, where I ran signals intelligence. And I both used and managed the development of a lot of information technology systems, some that worked and some that didn't work.

So what I want to do today is give you some lessons learned based on that experience that might be of value to all of us as we move forward on this very important undertaking.

Access to the right information is a challenge that every organization faces?public, private, every organization in the world.

And I think it is important to remember that we don't share information for the sake of sharing information. There is actually a much more important reason we share it. And that is to improve collective and individual decision-making and to actually reduce decision-making cycle time for those who have to actually act.

So the value of information and the information to be shared, as my colleague have said, is in the eyes of the user, not in the eyes of the producer.

And one of the things that we have learned, among the most painful lessons I think we have all learned, is that information doesn't come marked, "Terrorism information," "Criminal information," "Critical infrastructure information." So it is incredibly important that the stewards of that information, whether they be at the state or local level or at the federal level, invest far more energy and time in understanding the decision domain of those they want to serve with information.

The decision-making domains of the people charged with protecting the homeland are vast and they are different. And users of information have to be able to tailor that information to their specific decision-making domain.

And I will give you an example. A highly classified, detailed, technical report on risin will be of use to certain members of our community. But perhaps for the patrolmen on the street, it is the unclassified picture of the castor bean plant that gives the actionable intelligence that can be used in their decision domain, in roll call, to enable their decision-making.

So what we face are global threats. Information sharing is about allowing us to be a network, so that each of us is optimized in our ability to respond to the threat. The information-sharing systems that we are developing are just a means to achieving that end.

And as they achieve that end, they have three very important jobs in defending the country. One is to protect the country with the information they contain. The second is to ensure that, in producing it and sharing it, they are protecting the privacy rights of U.S. citizens and other rights of U.S. citizens. And third, to ensure that taxpayer dollars are spent responsibly in their development.

Now, what I just described, in terms of an information-sharing system, where we can each customize the data to our decision-making domain, is a very complex undertaking. It actually requires components related to the organization, to people, to processes, to technology, and to organizations themselves. And yet, of all the components I just listed, technology is the one that we always talk about. And technology is rarely the reason that any information system fails to deliver the promise that it initially made to the users.

Instead?and in my testimony I have given you examples of places where this works?instead, really what information systems and information-sharing success depends on are what I think are six critical factors.

First, establishing a clear purpose and clear metrics for measuring mission outcomes. Not volume of data, not number of things posted, but what have we done to secure the nation as a result of doing it.

Securing active sponsorship at all levels of leadership of the organization.

Involving all stakeholders, particularly the user community, in the development of the system.

Communicating required change in culture. And I know that sounds like a very touchy-feely thing to say, but the management of the change that information sharing requires of all entities must be managed as carefully as the delivery and development of the system itself.

Defining the business processes the system is supposed to enable.

And having strong program management.

Those are six things. Information technology systems are essentially, I say pejoratively, dumb. They do only what business practices and business rules tell them to do.

So having admired the problem, I would just offer that there are some very promising solutions that I have seen under way. Much like for the development of?I don't know if you are familiar with the capability maturity model for developing software, but it is fundamentally about diagnosing whether an organization has repeatable processes that mean their software will function well.

And I think that there is a way of looking at information sharing and actually using an information maturity model approach to force all of us who are developing these systems to take all six of those dimensions into account when we are developing the actual systems themselves. You can develop great technology and, if you have not settled on business practices, the business rules to which you have to map the data will not be there to develop the system that people need.

And then, just in closing, I would like to say that I think, in terms of systems, where you are is actually where you sit. Now on the outside, very easy to sit here and offer these wonderful ideas. And I have also been on the inside and I have lived with a terribly unforgiving operations tempo that does not allow you to fail in any dimension, and it actually does make it difficult to focus on these core issues, regardless of the fact that you know they are the right ones to focus on.

So success for the country is going to require a partnership among all of us to get this right. I think this hearing is a measure of your commitment to that partnership, and I want to thank you for allowing me to participate.

[The statement of Ms. Baginski follows:]

PREPARED STATEMENT OF MS. MAUREEN BAGINSKI

Chairman Simmons, Ms. Lofgren and Subcommittee members, it is my pleasure to appear before you today to discuss the vital issue of information sharing and enabling technology. I served in the United States Intelligence Community for a total of 27 years, most recently as Director of Signals Intelligence at the National Security Agency and Executive Assistant Director for Intelligence at the FBI. In those positions I both used and managed the delivery of many information technology systems--some of them successful and some of them not. My purpose today is to share with the Subcommittee lessons learned from those experiences that may be of use to the Department of Homeland Security as it moves ahead with the development and deployment of vital information sharing systems. Those lessons learned have been considerably enriched by my tenure at BearingPoint, where I have been exposed to the power of the commercial sector's approach to similar challenges.

Information is a tool that each of us uses every day to inform decision making. Our decision making domains are often very different, and we tailor available information to our specific roles and responsibilities at any given point in time. The quality of our decisions is dependent on the quality of information available to us. We do not necessarily need more information; we need the right information for our decision domain. This is the core challenge facing all information sharing systems today. Among the painful lessons learned in recent years is that information does not come marked ″terrorism information″, ″war fighting information″, ″policy information″, ″criminal information″, or ″natural disaster information″. The threats facing our nation today are global in nature and no single source of information or single organization can defend against these threats alone. It will take all of us working as a network to defend against these global threats and the goal of information sharing programs is to create that network.

For the producers of information-particularly those in the Intelligence Community--, the new threat environment requires that they judge their performance not on information output, but on the outcomes their information enables for the nation. First and foremost that means that information stewards-whether they are at the federal, state, local or tribal level-- must invest considerable time and effort in understanding the domains of those who must act on their information. Then they must provide information to those users in the form that is of most utility to them.

At the risk of gross oversimplification, intelligence is vital information about phenomena that would do our nation harm. The value of intelligence is judged by the user of that intelligence and not by its producer. Intelligence protects our nation in three ways: by the information it provides, by providing it a way that safeguards the rights of all U.S. citizens, and by spending taxpayer money responsibly. These are shared imperatives and each must be fulfilled. In today's world of global threats, the user base of intelligence has been greatly expanded, extending now from the President, to the soldier, to the patrolman and beyond. For example, a detailed, scientific paper about RICIN written at the classified level may be of enormous value to our scientific and health communities. For our patrolmen, the most valuable information in that report may be the unclassified photograph of the castor bean plant that could be used at ″roll call″ to inform the officers to be on the alert for it in the course of normal duties, i.e. in their unique decision domain. With timely, actionable information tailored to the operating environment of individual users we are more likely to be successful in getting inside and ahead of the adversaries' decision making cycle and prevent the harm they would do.

The creation of an information sharing environment with the characteristics described above is a complex undertaking and has many inextricably linked components related to people, processes, organization and technology. Information systems rarely ″fail″ because of technology. Information sharing systems are essentially ″dumb″; they do only what business processes and business rules tell them to do. They are more likely to fail because:

1. their purpose is unclear
2. they fail to involve all stakeholders, particularly the user community
3. the changes in organizational culture that they require have not been communicated or prepared for effectively
4. the business processes that they are to enable have not been defined.

5. they lack sponsorship at all levels of leadership
6. weak program management

Below are examples of successes and failure in each of the dimensions listed above.

Clear Purpose

The need for a clear understanding of the purpose of an information sharing system is critical to its success. Often this purpose is sketched out at a high level using a Concept of Operations or Conops. The Department of Justice took the Conops approach to information sharing and began in 2003 to develop within DOJ (with DHS and state, local and tribal law enforcement participation) the Law Enforcement Information Sharing Plan, or LEISP. The guiding principle of LEISP was that there would be a ″one DOJ″ information sharing platform for DOJ partners in law enforcement. The Conops process was not without considerable pain and difficulty, and completion took well over a year, largely because of very understandable concerns about the how information would be used, and what might be fairly characterized as ″turf issues″. In addition, In information the CONOPs' completion was delayed by concerns that it lacked sufficient detail to be implemented. The effort was very ably led by DOJ CIO Vance Hitch and had the personal sponsorship of Deputy Attorney General James Comey.

Just as the Conops effort appeared to be foundering, Deputy Attorney General Comey made an important decision. Essentially he decided that the details desired by those working on the Conops could be developed more quickly if the concepts were tested in a real world environment. In partnership with then Secretary of the Navy Gordon Englund, DAG Comey ordered all DOJ elements to make specific information available to a functioning information sharing system in Seattle called LINX. LINX unified federal and state and local law enforcement information in a single system to improve information sharing. DAG Comey personally sponsored the project, set deadlines, and made hard decisions in the face of some resistance and legitimate concerns about the resource demands of the program. In the end, deadlines were met and DOJ was able to implement the LEISP concepts, now called ″one DOJ″ in a real world system. This is an excellent example of both strong leadership and the utility of testing concepts in small pilot offerings to inform further development of information sharing processes.

Involve All Stakeholders

In 27 years of Federal service, the best example I have seen of the power of involvement of all stakeholders in an information sharing has been in the Law Enforcement Community.

The FBI's Criminal Justice Information Services (CJIS) Division serves as the focal point and central repository for criminal justice information services within the FBI and is responsible for day-to-day management of the following programs administered by the FBI for the benefit of local, state, tribal, federal, and foreign criminal justice agencies:

Integrated Automated Fingerprint Identification System (IAFIS)
The National Crime Information Center (NCIC)
Unified Crime Reporting Program
National Instant Criminal Background Check System (NICS)
Law Enforcement National Data Exchange (N-DEx)
Law Enforcement on Line (LEO)

CJIS administers these systems through an Advisory Process that has existed since the inception of these systems in 1969. The philosophy underlying the advisory process is one of shared management; that is the FBI along with local and state data providers and system users share responsibility for the operation and management of all systems administered by the FBI for the benefit of the criminal justice community. The CJIS Advisory Process consists of two components: the Working Groups and the Advisory Policy Board (APB). The CJIS Working Groups review operational, policy, and technical issues related to CJIS programs and policies and make recommendations to the APB or to one of its subcommittees. All fifty states, as well as U.S. territories and the Royal Canadian Mounted Police are organized into five working groups. The APB is responsible for reviewing appropriate policy, technical, and operational issues related to CJIS programs and for making appropriate recommendations to the Director of the FBI.

Law Enforcement On-line (LEO) is a system developed under this process. LEO is very much like HSIN and provides a secure information sharing capability based on communities of interest. In the early stages, LEO was not universally well received by the user community. First, it was not considered user friendly, particularly in its password regimen. Second, the information on LEO was not of sufficient value to the law enforcement community to make the pain of the password regimen worth the effort. Through the APB, CJIS worked to modify the password regimen

and ensure that information placed on LEO was of more value to the user community. These improvements made LEO of more utility and usage increased. The process of improving and refining LEO continues today through the APB process.

Although this process has not been without points of pain, it has engendered both trust and mission success. The CJIS process has created a shared governance model in which all users agree on the elements of information to be shared, understand that the ″price of admission″ to system access is to flag and tag that information such that it is available to all, and defines sanctions for misuse of information that is shared. This is a powerful model that could be leveraged or emulated in DHS's continued work on HSIN and related systems.

Change Management

Information sharing on the scale required by the new global threat environment is new for the vast majority of participants. Change of this magnitude must be managed every bit as carefully as the technology implementation itself. For many the change will be threatening or not understood. Success hinges on communication, training and clarity of vision.

Virtual Case File (VCF) may seem like an unlikely choice as an example of good changes management process, but it is instructive. As the Subcommittee is aware, Director Mueller's transformation of the FBI from a law enforcement only to a law enforcement and intelligence entity has two core pillars: intelligence and information technology. Recognizing the magnitude of the change required in FBI operations, in 2003 Director Mueller required that all senior managers in the FBI attend a week-long course at North Western's Kellogg School of Management, entitled ″Navigating Strategic Change″. In those sessions managers received presentations on both VCF and Intelligence, and discussed the imperatives for each. In addition, managers worked through a series of case studies designed to provide them with the tools to manage the cultural change that both VCF and the new intelligence mission would entail. Managers then returned to their operational duty stations with the mandate to ″cascade″ the change throughout all levels of their organization.

This well-planned and executed component of the change management process, however, was not sufficient to make VCF a success.

Define Business Processes

According to the FBI's own analysis, one of the major contributing factors to the failure of VCF was the lack of well-defined and agreed upon business processes to drive and define the requirements for the system. As the Subcommittee is aware, VCF was the third component of the FBI's Trilogy Program-a program designed to deliver the core functionality for an FBI information technology enterprise. Phases I and II of that program (the backbone and computer hardware) were delivered on time and within budget. Phase III, VCF, was an FBI enterprise-wide case management system. That system was not a success and following an extensive independent review, was terminated. The independent review cited two primary reasons for the termination recommendation:

1. it appears that either the FBI was unable to clearly communicate requirements so that they were completely understood by the Contractor, and/or
2. that the Contractor deviated from those requirements without exercising change management and ensuring customer buy-in along the way.

The Trilogy Program illustrates clearly the criticality of business process definition in the delivery of information sharing systems. The information backbone and hardware could be delivered without critical business process definition and were delivered successfully. VCF was a collection of software applications that required a clear set of business rules to which system developers could map data. In the absence of agreed upon enterprise-wide business processes, those business rules could not be developed. The FBI learned a hard lesson from this experience and has launched an enterprise-wide business process definition initiative to drive the development of the Sentinel system. The success of that program will depend largely on the success of that process.

Leadership Sponsorship

Leadership sponsorship and commitment is the key to the success of any initiative, but may be even more critical for information sharing initiatives that challenge existing views about data ownership. There are many examples of strong senior leadership and its positive effect on information sharing capabilities, such as the DOJ LEISP pilot cited above led by DAG Comey. Another example is the Intelligence Community's intranet, called INTELINK. INTELINK was designed to create an intelligence product sharing capability across the IC and was personally championed by then D/DCI Admiral William Studeman in the early 1990's. At the time there was not only considerable resistance to the concept, but real obstacles to implementation in then extant IC information sharing policies. D/DCI Studeman care-

fully steered the initiative through the policy issues, made hard decisions, and mandated the implementation across the Intelligence Community. Today the majority of IC members cannot remember a time when there was not an INTELINK, but its implementation took time, patience, and most of all strong leadership support.

Strong Program Management

The FBI considers that lack of strong program management practices to be a root cause of the VCF failure and cites weaknesses in acquisition management and requirement/change management as particularly critical. At the highest level the FBI cites shortcomings in three areas:

1. The quality and ability of people to motivate and manage multi-disciplined teams of diverse specialties
2. The lack of effective program management processes and methodology
3. The lack of sufficient technology to forecast and measure risk, to manage and monitor earned value, and to perform to requirements.

Given these concerns, the FBI has focused corrective action plans and initiated a number of programs to guard against a recurrence of these problems. In acquisition management, the FBI has restructured and modernized the acquisition management process, including career development for contracting officers. Most importantly, the FBI has learned the definition of requirements in acquisition documents is paramount and has invested experience personnel in managing requirements definition. Simply stating needs and detecting what is deemed a responsive offering does not guarantee mutual understanding between the Government and the Contractor. The FBI is committed to taking whatever amount of time it takes to come to a meeting of the mind on requirements, and only then to establish contractual agreements, penalties, and awards.

For requirements management, the FBI has learned that program management is a professional discipline requiring specialized talents and training in which it must invest. Clear requirements definition and the inevitability of changes in those requirements must be understood and managed effectively. Integral to that process is a comprehensive Change Management Plan, according to which requirements changes are introduced, evaluated for impacts to schedule and budget, and agreed upon. In addition, the new program management process includes the creation of a risk management matrix that identifies each risk and the projected and actual cost of risk mitigation.

A Way Ahead

Information sharing/access is a challenge faced by virtually every organization in the world. For that reason, many commercial technology organizations like BearingPoint are devoting considerable effort to developing solutions for the challenges inherent in information sharing systems. One promising solution centers on the development of a series of ″maturity models″ that both assess the ability of organizations and communities to implement complex information sharing programs, and provide specific criteria for moving from the lowest to the highest maturity level. Because the successful implementation of information sharing systems depends on people, processes, organizations and technology, the maturity models measure readiness in all of those dimensions.

The ″maturity model″ approach is outlined below:

Enterprise Maturity Model

Organizational Maturity—The degree of maturity related to leadership, strategic direction, human capital management, and communication and collaboration

Business Process Maturity—The degree of maturity of business process management and automation

Information Maturity—The degree of maturity of data and information quality and availability

Application Maturity—The degree of maturity of applications supporting the business processes

Technology Maturity—The degree of available shared services and components use

Security Integration—The degree of security pervasiveness

Provider Maturity—The degree of ownership of information technology resources

Information Sharing Maturity Model

Policy/Strategy Maturity—The degree to which information sharing policy, strategy and metrics has been defined and are understood across all participating organizations

People/Organization Maturity—The degree to which leadership, strategic direction, human change management, communication, and training are being effectively implemented across all participating organizationsProcess Maturity—The degree to which information sharing processes are defined and implemented in a consistent fashion across all participating organizationsGovernance Maturity—The degree to

which governance processes are in place for coordinating and controlling information sharing activities across all participating organizationsArchitecture Maturity—The degree to which standards, best practices, guidelines, reference architectures, etc have been defined ad agreed upon so as to provide guidance to the participation organizations so that they can efficiently and effectively implement the information sharing initiativesTechnology Maturity—The degree to which the participating organizations have the information services, technical infrastructure, and security in place to efficiently and effectively support the information sharing initiatives

The above maturity models must be supported by performance measures.

Information Sharing Metrics Library and Process Library

Outcome Metrics—Measures the extent to which information sharing initiatives improve mission/government/department/agency outcomes

User Metrics—measures the extent to which users are provided with or have access to the information they need to get their job done effectively

Process Metrics—measures the extent to which information sharing initiatives improve key information sharing processes (many of these processes take weeks today because they are done manually-these metrics will measure the effectiveness of automating the processes across multiple agencies)Information Metrics—measures the extent to which information is accessible, visible, understandable, and trustworthy

Finally, it is important to note that in the development of information sharing systems, where you are is very much where you sit. Now, sitting on the outside, it is easy to articulate issues and offer solutions. I have also been on the inside and have lived with the unforgiving operational tempo that often confounds the best intentions to remain focused on these core issues. Success will require a partnership of all parties and all branches of government to provide critical oversight, resources and time necessary to implement these critical systems. This hearing is a measure of your commitment to that partnership. Thank you for allowing me to participate.

Mr. SIMMONS. Thank you very much for those comments. Again, the written testimony is very detailed and very insightful.

And I will rephrase my prior question and put it to the panel. In the prior testimony, we heard the DHS chief intelligence officer talk about some of the improvements to the system that went to the issue of providing more classified information and trying to get more people with clearances to access that classified information. And he commented that he felt that a lot of the private-sector players would have those clearances as well.

That is a legitimate point; I don't disagree with that point.

But then I look at the other side, and I say one of the major problems that we encounter in information sharing is the fact that, if you have to rewrite the classified product, are you really giving your customer anything other than just garbage? And if the customers in the field are feeding up into the system, is that going to be valued because it is not classified?

So it seems to me that we are in a quandary here. Those with your background, for example, who have lived in the secrecy system, tend to say, "Well, if it is secret, it is good, so we have to share the secrets, but not too much, because, you know, if you share it too much, then somebody might disclose it."

People from another background might say, "No, we have really got to open up the system. These fusion centers have to work better. They are only going to work better if people at a fusion center are confident that they are really getting some good stuff and that the process is really working."

Where are we in all of this? What path do we need to follow? And I hope you won't say both, because that is troublesome.

How do you, Mr. Hay, how do you resolve Mr. Allen's comments, for example, based on what you have testified?

Mr. HAY. And this is certainly not to slight Mr. Allen at all?

Mr. SIMMONS. Of course not.

Mr. HAY. ?I think the way I would describe it is, the public sector almost has a blind spot when it comes to open sources and how much information is available.

And I will use one quick comment. I can elaborate on it later in a closed session, just to bring up the identities. However, when I was operational for the G–8 summit in Sea Island, Georgia, within 2 hours of running that, being the director of that private-sector information-sharing group, we had somebody who captured a guy photographing the U.S. attorney's office in a powder-blue Bug. He was a skinhead. Two days later, when he parked that car in front of a bank, we had 14 different law enforcement agencies descend upon this guy. And it ended up being nothing. However, it could have been something. So, on the one hand, I think we have to fully engage those people.

Now, to answer your question, I think you honestly need to have a translator. You need somebody, you know, such as myself?I actually hold a Georgia position of trust?it is not a federal clearance; we are getting there, baby steps?who really sits in between a massive amount of information that comes from the private sector and then understands the intelligence world and secrecy so they are able to only pass those things along that are important and then pass the things down that are absolutely critical.

And it is that person in that role that gives the private sector saying, "Hey, I am not going to see the sexy intelligence information. However, I know somebody who is, and I trust them."

I hope that answers your question.

Mr. SIMMONS. Anybody else?

Mr. RAPP. Chairman Simmons, if you don't mind, yes, that is a good issue because a lot of the classified information I have seen, you could also obtain a lot of that information from open-source documents. So I don't quite see why it is classified.

The other side of that is, we do have classified information that contains information that people below our level, at the TS level at the fusion center, don't need to know.

But what they have to be confident in, particularly commanders in my department that don't have that ability to obtain the classified information, what they have to be confident in is that what I am telling them is correct and that the information I give them they can take some action based on that.

Frequently the tear lines off of classified information are so vague that I wouldn't feel comfortable, as a commander, making it. But I know, because I have the clearance, I have a little bit more information.

I think that is what we have to get over, if that addresses your question a bit better.

Ms. BAGINSKI. I think it is a very important question, coming from that community.

Generally I think it is imperative that the intelligence community decide what it is it is trying to protect. And generally it is not the information; it is the sources and methods. And it is proven that one can separate the two and write the information such that it is releasable.

So this is a big cultural change for the I.C. but it basically says the first document you put out should be unclassified. And I think

that is?John Negroponte and others, I think, are working very, very hard on that.

To your comments about open source?and I will tell you why I think that. Otherwise, we will clear every man, woman and child in America.

[Laughter.]

And I simply don't think you can scale that. While I think clearances are very important, as you just described it is a great solution, but you certainly clear everyone who could possibly take action.

Open source is also, I think, more culturally different for the intelligence community. It grew up in a time when there was no CNN. The open-source world and information, by definition, the targets were denied.

So this is a huge shift that has to occur, with starting from what is already known and then using the secret methods and sources to go after what is not known, secrets worth knowing. And this is a big shift that has to occur and, I think, speaks to your point about leveraging private industry and leveraging all your guys that are out there every day.

Mr. SIMMONS. I agree with everything you said. Thank you.

Ms. Lofgren?

Ms. LOFGREN. Thank you, Mr. Chairman.

And I was just kept enrapt. As you spoke, it reminded me of my former colleague in the city of San Jose, one of the members of Congress, Tom Campbell. And Tom is now retired?dean of the business school at Berkeley. We didn't agree on a lot of things, but he gave me a piece of advice, which was: Never go to a classified briefing.

[Laughter.]

He said, "You will only learn what is on CNN, but then you won't be able to discuss the CNN program."

[Laughter.]

I want to talk, Ms. Baginski, a little bit, if I can, about your experience at the FBI and the Trilogy program. It wasn't your fault, I know that. It was designed to be a high-speed network with modern work-station software and application, Virtual Case File, to really improve the organization access and analysis of information.

And the program was canceled in March of 2005. I believe the I.G. said it was canceled because of poor management and oversight. The bottom line is it was $170 million essentially just crushed.

I would like to know, what?I mean, having been over there to observe what happened, what lessons could we draw from that experience as we roll out a system here in the Department of Homeland Security?

Ms. BAGINSKI. I think there are very good lessons to be learned from that.

As you described Trilogy backbone, essentially networks and essentially systems on the desk. So, easy to deploy those things.

VCF, however, Virtual Case File, was a set of software that was supposed to instantiate business processes. And it is the VCF component of Trilogy that failed. And I think there are three reasons.

First, the business process re-engineering actually was not done. So, instead of having one way that the FBI managed cases, one way they open-sourced it, one way the enterprise did things, there was more like an instantiation of 56-plus–400 number of field offices and resident agencies the FBI had ways of doing things. And that led, actually, to a system that could not technically perform in scale. I think that was one dimension.

The FBI itself learned the lesson from that, and business practice re-engineering is one of the set pieces of the Sentinel program, to resolve that issue, so that the system knows what business rules it is to implement and there is something to map the data to. So that is very important.

I think the second thing that the FBI would point to is program management weakness, beginning with an inability to actually define requirements. They, themselves, will hit themselves fairly hard for that: Nobody met a requirement they didn't like, the ever-creeping list of requirements, and no ability actually to manage changes with the contractors and keep track of that. And then not a very good review process to ensure that those changes were being made.

I think the third thing they would say is not sufficiently engaging the users of the system in the development of the VCF. So that was also addressed during Sentinel with a huge corporate process to have the actual users of the system engaged in its design and requirements development.

I think those are lessons in those six dimensions that I described.

And VCF is also interesting from another dimension. The change management of Virtual Case File was handled very well. Director Mueller said all of us to Kellogg School of Management for a week of change. We learned about the I.T. systems, and then we were also given a series of tools to actually cascade the change down through the organization. And it was fascinating, because it was the best example of change management I had seen I think in my entire career. And yet, even as well-handled as it was, it was not enough to ensure the success of the system.

So you can't just have one dimension that works well. It has to be all those dimensions.

Ms. LOFGREN. Looking at what is going on now with HSIN, some of the information we have gotten is that, because there is a long-term relationship in most departments with the FBI, rather than deal with that, they will just pick up and call their contact at the FBI. And it really feeds into whose turf is it and really doesn't lead us in the direction of changing the method so that we actually all do better.

You are going to be advising Mr. Allen, I understand, and you have substantial expertise to do that. Certainly Mr. Allen has a strong commitment to making this work. What advice would you give him, given what has happened already and the deficits that were created and that he has inherited, to overcome these issues?

Ms. BAGINSKI. I would give him the advice to make the fusion centers the set piece for HSIN future deployment and development. And learn the lesson that?I mean, when the military goes overseas to fight a war, the intelligence community and those who serve it

with information don't actually say, "Could a bunch of you stay back and sit in our fusion center?" We go with them.

So the idea of this would be to actually deploy the federal government to those who are fighting the war in the homeland, learn how they make decisions, and make that information available to them.

I think that that would give a focus on the business process issues. That would give us a controlled environment to try to deal with all six of these dimensions, because none of these issues are easy. Policy is hard; it is hard with the states.

But if we focused it on a fusion center where the states come together and the fed comes together, instead of, go to this county, that county, this thing, this thing, and this thing, you would be sitting with the decision-makers. And I think, as you have already suggested, that you would probably have less frustration, both on the federal side and the state and local side.

Ms. LOFGREN. Thank you, Mr. Chairman. I see my time has expired.

Mr. SIMMONS. Yes. The gentleman from Indiana, Mr. Souder?

Mr. SOUDER. Thank you. I appreciate your comments on the importance of having a commonality of how you input information and just down at the basic levels. Because information systems can't match up if they aren't starting similar, at least separating out what is in common and then rebuilding.

But I wanted to go down a slightly different path. My primary expertise is in product cycling. I have worked with that since I have been in Congress and chair of the Narcotics Committee and the Speaker's Drug Task Force.

And we have been through a lot of this in narcotics. In the HIDTAs, which the best example right now is New York City because they didn't have a chance to wait around for the federal government to get organized, they basically converted the drug HIDTA to a terrorism HIDTA as well, and Connecticut and New Jersey have since come in too, because we have these problems that the major metro areas often overlap state lines and we get state structures, and it is how to do this.

And there, the federal agents are, in fact, on the ground with the local. Like you have just suggested, the DEA and FBI, ATF, others, go in with state and local. We set up a system that forced that interaction. It occasionally gets under attack, but nevertheless has survived over time.

And I am wondering why, when we have that relatively successful model, and one that state and locals in the major metropolitan areas are already used to working with, why this is so hard to conceive.

Now, there are some working with narcotics, I would suggest?and I have a particular question for Ms. Baginski coming from this. I think the state and locals are extra-sensitive about how information is classified and shared because of their experience with narcotics.

That there has been a feeling that often they are working a case, and the information here isn't classified for national security reasons, it is classified almost as if, "We don't want to share the glory in a bust," or, "Your case isn't as big as my case." "We are not going to take this one down in Fort Wayne because we are working

a bigger one in Indianapolis. And we are not going to take down Indianapolis because we are working a bigger one in Kansas City. We are not going to take Kansas City because we got one in Houston. And Houston is trying to deal with the Southwest border; therefore we are going to let your cocaine dealer work, even if it is the biggest one in the United States."

This historic skepticism, they are not used to working with the CIA, and they are not used to working with NSA. On the other hand, NSA and CIA are used to working in a military sphere and don't understand the distrust at the state and local level of what is protected and what is classified and the types of sources because it is a different ballgame. Similarities with Colombia and Afghanistan, particularly Afghanistan as we are getting overwrapped in heroin.

But you had a statement, that you said that different lanes need different information. And it is really, then, the assumption with that is, since the federal government has most of that classified information, that the federal government decides which lane you are and what you need to know.

The challenge here is that, since in terrorism, unlike narcotics, we don't know whether the information is, in fact, information, it is very difficult to figure out what lane you are in and what information you need to know. So then the question comes back to, who gets to dispense and decide what information is important?

And I understand the other variables, but I wanted you to clarify that a little bit, because the way you sounded is, what would I think would give some rise to concern out of state and local that, if we don't really know whether a person is a terrorist or not, and you are trying to decide and parcel down the information, how would you do that?

Ms. BAGINSKI. I thank you for giving me the opportunity, because it is exactly the opposite of what I believe.

I think that there is a legitimate way to do this. And the model that I would point?I think the law enforcement model is very powerful.

You asked a number of questions. Let me try to see if I can get at most of them.

The law enforcement model that you described is very important. The HIDTA model is very important, has been very successful. The fusion centers would allow you to move to an all-crimes, all-hazards approach and out of the strictly law enforcement component and involve the private sector.

So while I think the HIDTA business process and the model itself is what becomes the fusion center, the fusion center is actually going to be dealing with more issues than just law enforcement.

But I think what you are focused on is the model of working together and operators and intel driving one another. That is going to be the model for the fusion centers. So?

Mr. SOUDER. And one key part of that is they had a vote.

Ms. BAGINSKI. Absolutely. That is the critical part.

Now, what you describe in terms of information, when I went to the FBI, having been cloistered behind the fence of Fort Meade, you know, for 25 years and not believing there was a world out

there, I was enormously impressed to find something that I actually think the law enforcement community has not gotten enough credit for.

The Criminal Justice Information System's organization, the operation that is in Clarksburg, Virginia, CJIS, and all of those systems, here is a model for managing this problem. Fundamentally you have a federal entity that has agreed to take responsibility for the operation of the system on behalf of state and local law enforcement and tribal law enforcement in this particular case.

But that is done through a shared management model?and I know you know this?the CJIS advisory policy board. And that has got a bunch of subcommittees. And they all sit in a room; they have a shared governance model; FBI operates, and they do the following things: They make decisions about, what are we going to do, what do we want it to do?

They proactively decide, "We will flag and tag and share the following elements of information. And if you, California, want them from New York, you got to index them this way and you got to flag and tag them this way. And then, guess what? If anybody misuses this," to the operational trust issue, "you are cut off. You are sanctioned, and you cannot use it again."

Now, that model, for those of you who have ever been stopped by a patrolman?I, of course, have never had that happen?that time that that person is taking behind you, he is doing essentially what I, as an intel officer, would say is a first protection mission for himself: Is it safe to approach?

I think there is something in that model. Broaden it our past law enforcement, make some agreements about flagging and tagging elements of data. Not giving databases?people, places, things, weapons, bridges?I don't know, I am making all this up now, guys. But that separates it from the source, to begin with?

Mr. SOUDER. Even at the start with the airports. How about just in an airport when you buy a ticket, there is a pop-up on your name.

Ms. BAGINSKI. Exactly. That is?

Mr. SIMMONS. If the gentleman would yield for a moment, I know that another committee has use of this room at 3 o'clock. It is a fascinating discussion. I was hoping we could go longer. And we have one member who remains. So, in fairness to Ms. Jackson Lee, I would like to recognize her for some questions. And then we will have to suspend and clear out of here because we have other members in other committees wanting to use the space.

Ms. JACKSON LEE. Let me thank both Mr. Simmons and Ranking Member Lofgren for this hearing.

Let me express the sense of frustration, because, as we listen to you and listen to the other witnesses?and I offer my apology; I was delayed in another meeting for the other panel?we notice that we are about to move to a new concept, the HSDN system versus the HSIN system. And I guess the mountain of frustration collapsed the poor HSIN system.

I come to this from a perspective of many members who go home to their districts and really deal with local and state officials, particularly law enforcement, who are front-liners every day. So I am

going to pose to Captain Rapp, Mr. Hay, if you would, to focus yourself on the robustness of what we have coming.

My understanding is one of the failures of the HSIN is, who wants to look at unclassified information? You know, who wants to read the newspaper? And there might have been some information about weather or some other things that might have been helpful?and I always view that unclassified means I have got to read it and then, sort of, read something from it. It is a newspaper that I didn't get to read.

Tell me how we can jump to make the HSIN robust, impenetrable, if you will, to a certain extent, and gain the trust of those who would, as you have said?and I am looking to make sure I am pronouncing it correctly, because I didn't hear it?Mrs. Baginski? Or the story about the blue?I think that was you, Mr. Hay, the blue Beetle. But how are we going to do that?

And I would like to go forward. And I know I can speak about the failures. And it was a mountainous failure. But let's see how we can move forward and get this actual new vehicle as trustworthy as it can possibly be.

Captain Rapp?

Mr. RAPP. Sure, thank you.

The HSIN system, the problem with that has been, to this day, it does have some good historical information, some good intelligence products, but current real-time data is very limited on there.

To give you an example, the London plane threats that we had a month or so ago, it took over 2 hours before anything at all was posted on HSIN that would help our fusion center. We were getting more information off of CNN and some of the other networks than we could get off of the classified systems.

The second piece?

Ms. JACKSON LEE. That is not good.

Mr. RAPP. No, no. The second piece?

Mr. SIMMONS. That is not necessarily bad, though, either. I mean?

Mr. RAPP. Well, we did get a lot of information over the open source.

[Laughter.]

But the second piece is, they are still notifying the homeland security directors for the state, and they are not inputting that information into a system. What a network system, in addition to posting real-time information, would benefit us?

Ms. JACKSON LEE. So real-time is crucial?

Mr. RAPP. That is crucial.

It is also crucial for us to talk fusion center to fusion center when an incident occurs. Because we clear a lot of information out that either comes open source or is rumored through the law enforcement or emergency management community, by talking directly to the NOC in D.C. or one of the fusion centers in Texas or Kentucky. We can clear that information out very quickly and/or get appropriate information to the first responders more quickly than we see it coming through the classified federal system.

Ms. JACKSON LEE. Thank you.

Mr. Hay?

Mr. HAY. I would probably limit it to three points.

First, I think we need a strategy. Whatever that is, you have to have a strategy to move forward.

Second, we have to involve the right people in it, the people who are respected. Sitting right next to me, for one, needs to be involved.

Thirdly, I think you need to provide value. And if we can provide value?pretty much if you think about the private sector and HSIN–CI, we have been eating out of the same tub of gruel for 2 years. And yet, I learned a lot from reading those open-source documents, and I was able to put together a common operating picture.

And that is really what we need. If there was one thing that we could do within that system, it would be a private-sector common operating picture that they could just keep posting information to. And that way my friend in the fusion center can see it. And if it becomes overwhelming, he can task somebody to give me the highlights of that.

And I think that, if we can do that, rebrand it under a different name, you know, whatever it looks like, if it provides value, everybody is going to come to it.

Ms. JACKSON LEE. I think that is a key point.

Ms. Baginski, could you just amplify, then, how we provide value and how we have this common operating effort? And also, how do we get local authorities that are engaged in this to say, you know, "This is not, if you will, the local cereal that they are giving me, this is not pablum they are giving me; this is real and I am going to utilize it"?

Ms. BAGINSKI. I would suggest that, from my perspective, the responsibility of the state and local is to stand up and shout very loudly about what they care about and say what they need to know and take the lead, through the fusion centers, defining their requirements. And the federal government needs to deploy this capability to the fusion centers.

Once you bring information to the decision-makers, the rest generally takes care of itself.

Mr. SIMMONS. All time having expired, I want to thank my colleagues for their questions.

I want to thank the panel for their very incisive testimony.

I remind members that if they have additional questions for the record, the record will be held open for 10 days.

And, without objection, this hearing is adjourned.

[Whereupon, at 3:11 p.m., the subcommittee was adjourned.]

○