STATEMENT OF FRANK W. DEFFER

ASSISTANT INSPECTOR GENERAL, INFORMATION TECHNOLOGY

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING AND TERRORISM RISK ASSESSMENT

U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 13, 2006

Mr. Chairman and Members of the Subcommittee:

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.[1]

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,

[1] *Efforts to Improve Information Sharing Need to Be Strengthened* (GAO-03-760, August 2003); *Protecting America's Freedom in the Information Age*, A Report of the Markle Foundation Task Force, October 7, 2002; *Creating a Trusted Network for Homeland Security*, The Second Report of the Markle Foundation Task Force, December 2, 2003.

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.[2] 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

[2] Groove Virtual Office is a Microsoft application that tracks contacts, alerts users to new activities, and provides a series of personal communications mechanisms.

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.[3] 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.

[3] Fusion centers are two or more agencies collaborating to provide resources, expertise, and/or information to maximize the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity.

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.