# DEPARTMENT OF HOMELAND SECURITY

## Office of Inspector General

# Homeland Security Information Network Could Support Information Sharing More Effectively


## Office of Information Technology

**OIG-06-38** **June 2006**

*Office of Inspector General*

**U.S. Department of Homeland Security**
Washington, DC 20528

# Homeland Security

## Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, effectiveness, and efficiency within the department.

This report assesses how well the Homeland Security Information Network (HSIN) supports information sharing across federal, state, and local entities to prevent and deter terrorist activities; and, prepare for and respond to emergencies and natural or man-made disasters. It is based on interviews with employees and officials of the Office of Intelligence and Analysis and the Office of Operations Coordination, as well as other relevant agencies and organizations, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

# Contents/Abbreviations



## Appendices



## Abbreviations

| | |
|---|---|
| DHS | Department of Homeland Security |
| DIA | Defense Intelligence Agency |
| GAO | Government Accountability Office |
| HSIN | Homeland Security Information Network |
| HSOC | Homeland Security Operations Center |
| IT | Information Technology |
| JRIES | Joint Regional Information Exchange System |
| LEO | Law Enforcement Online |
| OIG | Office of Inspector General |
| RISSNET | Regional Information Sharing System Network |

# Contents/Abbreviations

## Figures

## Executive Summary

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* assigned responsibility to DHS to coordinate the federal government's communications relating to homeland security with state and local government authorities, the private sector, and the public. As part of this responsibility, the Act assigned the Information Analysis and Infrastructure Protection directorate within DHS, in conjunction with its chief information officer, responsibility to establish a secure communications and information technology (IT) infrastructure that allows federal, state, and local governments, and other specified groups to access, receive, and analyze data, and to disseminate information acquired by DHS as appropriate.[1] To meet this mandate, DHS is implementing the Homeland Security Information Network (HSIN).

As part of our ongoing responsibility to assess the efficiency, effectiveness, and economy of departmental programs and operations, we conducted a review of HSIN. The objectives of this review were to (1) identify DHS' plans and activities for sharing information with state and local governments; (2) determine how well HSIN supports these plans and activities; and, (3) identify challenges to information sharing among federal, state, and local government agencies. The scope and methodology of this review are discussed in Appendix A.

Due to time pressures, DHS did not complete a number of the steps essential to effective system planning and implementation, hindering the success of the HSIN system. Specifically, DHS did not clearly define HSIN's relationship to existing collaboration systems and also did not obtain and address requirements from all HSIN user communities in developing the system. In addition, DHS did not adequately evaluate each of its three major HSIN releases prior to their implementation. Further, the department has not provided adequate user guidance, including clear information sharing processes, training, and reference materials. Without establishing a baseline and developing specific performance measures, DHS has no effective way to track or assess information sharing using HSIN.

[1] The Information Analysis and Infrastructure Protection directorate no longer exists under the current DHS organization. Under the new DHS structure created as a result of the Secretary's 2005 Second Stage Review, former functions of the directorate were divided among the Office of Intelligence and Analysis, Preparedness, and Operations Coordination.

As a result of these system planning and implementation issues, HSIN is not effectively supporting state and local information sharing. Although users generally like the web portal technology because of its user-friendliness and flexibility, those we interviewed said they are not committed to the system approach. Users are confused and frustrated, without clear guidance on HSIN's role or how to use the system to share information effectively. Because some lack trust in the system's ability to safeguard sensitive information, and because the system does not provide them with useful situational awareness and classified information, users do not regularly use HSIN. Instead, users resort to pre-existing means such as related systems and telephone calls to share information, which only perpetuates the ad hoc, stove-piped information-sharing environment that HSIN was intended to correct. Resources, legislative constraints, privacy, and cultural challenges–often beyond the control of HSIN program management–also pose obstacles to HSIN's success.

To ensure effectiveness of the HSIN system and information sharing approach, we are recommending 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 crosscutting representation and participation among the various stakeholder communities to determine 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.

## Background

HSIN is a secure, unclassified, web-based communications system that serves as DHS' primary nation-wide information sharing and collaboration network. HSIN offers real-time chat and instant messaging capability, as well as a document library that contains reports from multiple federal, state, and local sources. HSIN supplies suspicious incident and pre-incident information, mapping and imagery tools, 24x7 situational awareness, and analysis of

terrorist threats, tactics, and weapons, too. The network provides connectivity between DHS' Homeland Security Operations Center (HSOC), critical private industry and federal, state, and local organizations responsible for or involved in combating terrorism, responding to critical incidents, and managing special events. The HSOC, which provides oversight responsibility for HSIN, is the primary national-level center for real-time threat monitoring, domestic incident management, and information sharing.

Across the various levels of government, a number of communities share information through HSIN, including law enforcement, emergency management, fire departments, homeland security, counter-terrorism, and the National Guard. As shown in Figure 1, HSIN is comprised of a group of portals organized along the lines of the various community groups. Users within the communities access HSIN directly through the internet; there are no special software requirements. All users have access to the counter-terrorism portal. However, access to the remaining portals is limited to the members of each corresponding community, with access provided to nonmembers on an as needed basis.

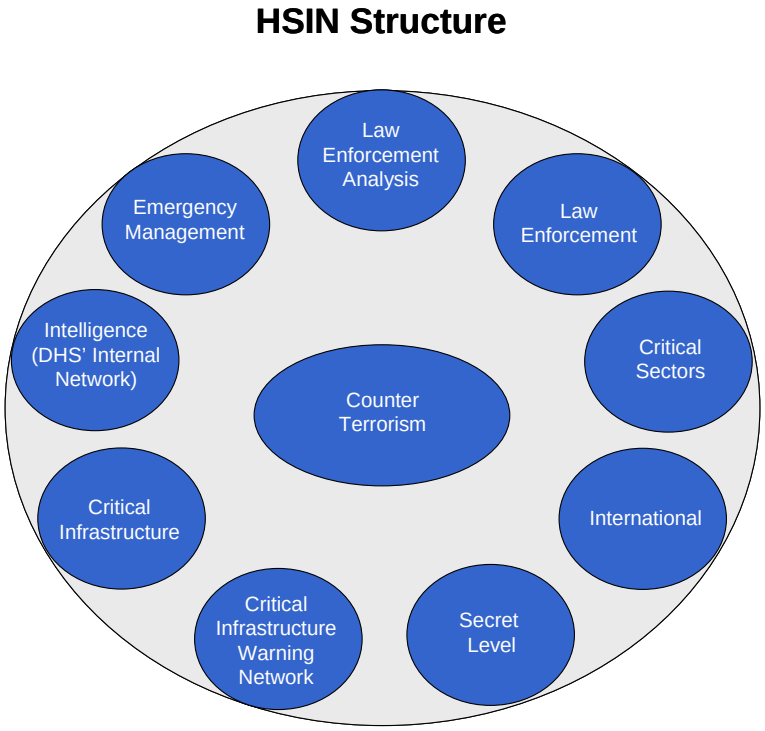


Figure 1: HSIN Structure

The current HSIN portals include:

- HSIN Counter-Terrorism – the common portal for all federal, state, and local government agencies to share information relating to counterterrorism and incident management.

- Law Enforcement Analysis – the portal for all major law enforcement intelligence centers.

- HSIN Law Enforcement – the portal for all departments that manage law enforcement sensitive data.

- HSIN Critical Sectors – the portal designed to enhance the protection, preparedness, and crisis communication and coordination capabilities of the nation's 17 critical infrastructures.

- HSIN International – the portal for information sharing and collaboration with foreign components during major crises.

- HSIN-Secret – the portal used to support classified information sharing among all state emergency operation centers and selected police departments.

- HSIN Critical Infrastructure Warning Network – a government network within HSIN that provides mission-critical, survivable connectivity and communications.

- HSIN Critical Infrastructure – a regionally coordinated portal used by the private and public sectors for local, regional, and national information sharing and all hazards alerts and warnings.

- HSIN Intelligence – an internal DHS intelligence and analysis network.

- HSIN Emergency Management – the portal that provides connectivity among federal, state, territorial, and local government emergency managers during major incidents.

HSIN was created as an extension of a pre-existing system, the Joint Regional Information Exchange System (JRIES). Figure 2 provides a timeline, key milestones, and system ownership for JRIES and HSIN from inception until the present.

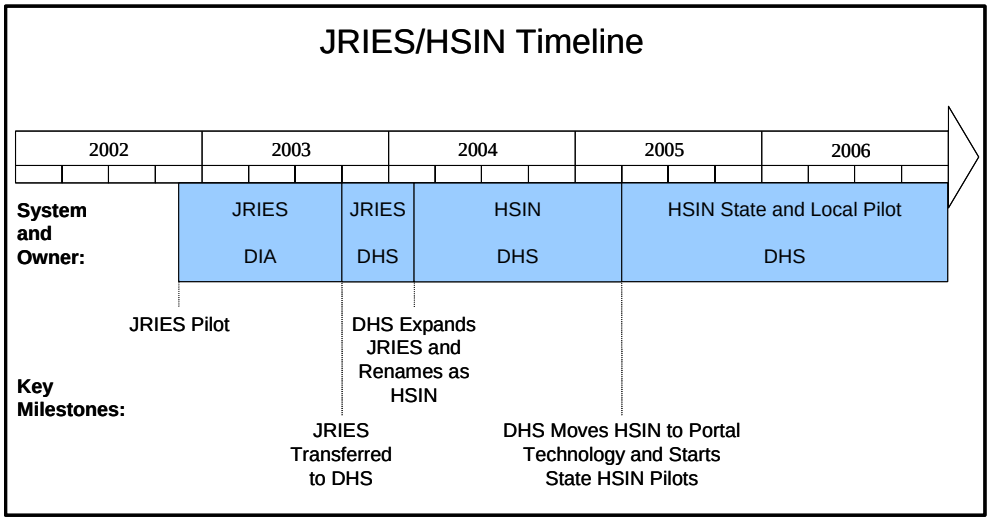


Figure 2: JRIES/HSIN Timeline

JRIES began 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). These groups designed JRIES, which was first deployed in February 2003, to facilitate the exchange of suspicious activity reports, register events potentially related to terrorist activity, and foster real-time intelligence and law enforcement collaboration in a secure environment across federal, state, and local jurisdictions. JRIES used "Groove" software to enable multiple groups to share the information securely.[2] A JRIES executive board, comprised of representatives from the participating groups, provided guidance and structure to help manage the system. 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. The system provided a very simple and efficient way for the law enforcement community to obtain situational awareness concurrently, without the need for hundreds of phone calls.

Although DIA originally operated and maintained JRIES, DIA transferred program management of the system to DHS in September 2003, due to funding constraints. DIA was concerned that managing JRIES to support domestic intelligence activities conflicted with its military intelligence role. As of February 2004, approximately 100 organizations–with more than 1,000

[2] Groove Virtual Office is a Microsoft application that has five main capabilities: synchronization, offline use, firewall traversal, always-on encryption, and bandwidth optimization(Groove2,5). The application also tracks contacts, alerts users to new activities, and provides a series of personal communications mechanisms(Groove2,5).

law enforcement and intelligence analysts from federal, state, and local government agencies–were using JRIES.

After acquiring JRIES, DHS recognized that the system's utility could be expanded beyond its existing counter-terrorism intelligence and threat awareness mission because JRIES met DHS' requirements for senior executive communications, crisis planning and management, and coordination and communications with first responder, emergency management, and military organizations. As such, in February 2004, DHS announced the expansion of JRIES as its primary communication, collaboration, situational awareness, and information-sharing system. The DHS Secretary renamed JRIES as HSIN in order to reflect the system's broader scope. By December 2004, DHS had deployed HSIN to all 50 states, 53 major urban areas, five U.S. territories, the District of Columbia, and several international partners. DHS extended 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. DHS equipped each location with two laptops installed with the Groove software.

In March 2005, because of the lack of scalability to accommodate a large increase in users, DHS decided to move HSIN away from the Groove software and to develop a series of web-based portals as replacements. Nonetheless, DHS continues to operate both the Groove software and a portal to support the law enforcement community.

DHS has expanded the role of HSIN through a state and local initiative. The goals of this initiative are 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 network. As of January 2006, eight states had deployed HSIN throughout their respective departments and agencies. Declaring HSIN the primary system for operational information sharing and collaboration, the DHS Secretary asked that the department's senior managers as well as headquarters and field personnel support the ongoing growth and utilization of HSIN.

Prior to DHS' implementation and expansion of HSIN, reports by various nonprofit, industry, audit, and congressional organizations documented problems with homeland security information sharing and the need for a single, effective collaboration system. Specifically, in August 2003, the Government Accountability Office (GAO) reported the results of its survey, which showed that federal, state, and city government officials did not routinely share information on terrorist threats, methods, or techniques. GAO stated that the information that was shared was not perceived as timely,

accurate, or relevant.[3] Further, in two key reports, the Markle Foundation stressed the importance of creating a decentralized network of information sharing and analysis to address the challenge of homeland security.[4]

Subsequent to HSIN's implementation, other reports revealed problems with the system. For example, in a September 2004 report, GAO identified 34 networks that supported homeland security functions–six of the 34 were used to share information with state and local governments, while four shared information with the private sector.[5] Further, citing significant problems with HSIN development and deployment, the U.S. House Committee on Homeland Security Democratic Staff reported in 2006 that DHS had failed in its promise to create a single, effective network for sharing intelligence with state and local officials.[6] The staff reported that police agencies were not sharing sensitive information and that there was a lack of JRIES executive board cooperation with the HSIN program.

## Results of Audit

## HSIN Planning and Development Efforts Have Had Limited Effectiveness

Due to time constraints, DHS did not follow a number of the steps essential to effective HSIN system planning and development. Specifically, DHS did not clearly define and communicate HSIN's role, particularly in relation to other systems in use for similar purposes. Further, DHS efforts to obtain input and address requirements from all HSIN user communities were inadequate. Also, the department did not develop clear and complete information sharing policies and procedures or provide system users with sufficient training and reference materials. Further, DHS has yet to develop metrics for assessing HSIN performance in supporting information sharing. Although DHS has taken actions to address some of these issues, more remains to be done.

[3] *Efforts to Improve Information Sharing Need to Be Strengthened* (GAO-03-760, August 2003).
[4] *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.
[5] *Major Federal Networks that Support Homeland Security Functions* (GAO-04-375, September 2004).
[6] *Leaving the Nation at Risk: 33 Unfulfilled Promises From the Department of Homeland Security*, An Investigative Report by the U.S. House Committee on Homeland Security Democratic Staff, 2006.

## Accelerated Deployment

Given concerns about ensuring connectivity and communications across the various levels of government in a heightened counter-terrorism environment, the HSIN system was implemented according to an accelerated schedule. As previously stated, DIA quickly built the original JRIES system after the attacks of September 11, 2001, to support information sharing between federal, state, and local law enforcement and intelligence agencies. After assuming ownership of the system in 2003, however, DHS quickly expanded the system to provide access to users beyond this limited group. The HSIN strategy was to implement a tool for nation-wide connectivity right away in case of major emergencies or terrorist incidents and address operational problems and details later.

In 2004, as DHS was implementing HSIN, pressure to complete the system persisted. For example, White House officials issued warnings that terrorists were threatening to disrupt the 2004 presidential elections. Correspondingly, due to intelligence about possible bomb attacks on specific financial institutions, DHS raised the threat level to code orange for parts of the banking sector. Such pressures created an environment that was not conducive to thorough system planning and implementation; DHS began expansion of the system in February 2004, and by December of that same year had established connectivity to all 50 states, major cities, and five U.S. territories. The rush to implement the system resulted in inadequate definition of HSIN's role with respect to other systems, insufficient identification of user requirements, ad-hoc system rollouts, a lack of user guidance, and inadequate performance measures.

Some members of the law enforcement intelligence community raised concerns early on that DHS was expanding HSIN access and capability too quickly. Specifically, in an April 2004 issue paper, the JRIES executive board stated that DHS was proceeding at a rapid rate in implementing the system without providing user training on standard operating procedures, laws, regulations, and governance policies related to information sharing and HSIN. The board contended that this rapid deployment increased the risk of system misuse, security breaches, privacy violations, and user confusion as well as dissatisfaction. The board pointed out that DHS' newness as a department and its lack of established relationships also hampered its ability to quickly gain the trust and commitment of states and major cities to the HSIN approach. The board ultimately stopped participating in the HSIN program for such reasons.

## Relationship to Existing Information Sharing Systems Not Clearly Defined

According to the *Homeland Security Act of 2002*, DHS is responsible for establishing an IT infrastructure, i.e., system, for sharing homeland security information with its federal, state, local, and private partners. According to the Act, such DHS efforts are to avoid duplication and consider existing systems. According to Office of Management and Budget Circular A-130, establishing a roadmap that outlines the goals, objectives, and strategies of a system, as well as how the system will fit within the context of the overarching IT environment, is a key means of avoiding duplication.

DHS intended HSIN to be the primary tool to help unify the counter-terrorist effort. However, prior to HSIN development, DHS did not assess the current IT environment or the relationship of HSIN to other existing federal systems that served similar missions. Without doing so, DHS could not make comparisons to identify potential areas of duplication or opportunities for sharing information between HSIN and the other existing systems. In Figure 3, we identify a number of systems that other federal, state, and local officials use to share situational awareness and intelligence information. Several of these systems have functions and capabilities comparable to those of HSIN.

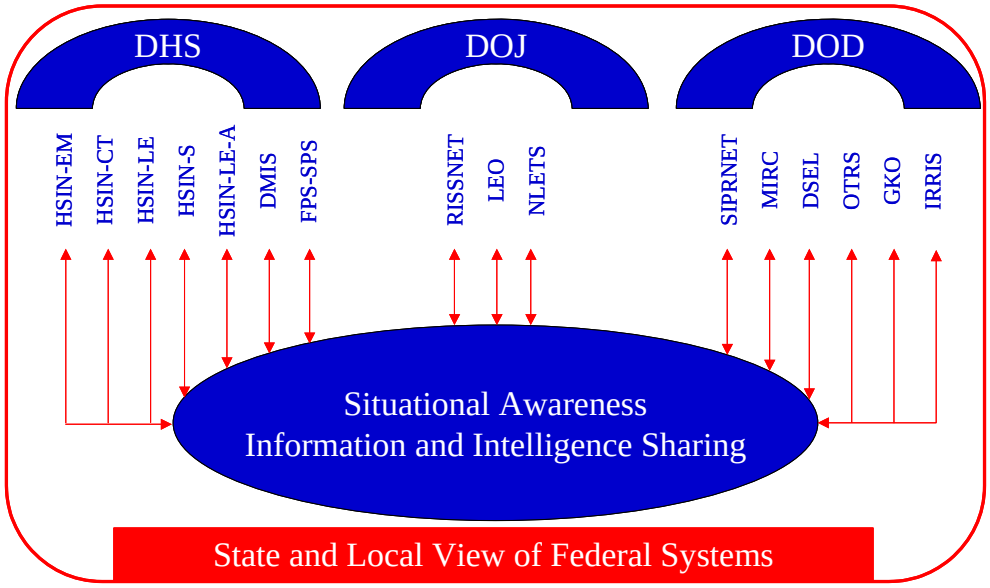


Figure 3: Federal Situational Awareness Information and Intelligence Sharing Systems

The Department of Justice, for example, has operated the Regional Information Sharing Systems (RISS) program for approximately 25 years to facilitate the exchange of critical information across federal, state, and local law enforcement agencies. Law Enforcement Online (LEO) is another

internet-based system that, like HSIN, law enforcement agencies use for information sharing. In its original HSIN press release in February 2004, DHS stated that RISSNET and LEO together address a much wider spectrum of criminal activity than does HSIN. As these systems expanded to include counter-terrorism and HSIN shifted to an all-crimes approach, the distinctions among the systems have diminished.

In addition to not conducting an assessment of HSIN's relationship to other existing systems, prior to HSIN expansion, DHS did not identify, document, or communicate to user communities how the system would support information sharing among federal, state, and local users. Specifically, DHS did not define the roles and responsibilities of the various stakeholders, what information would be shared through HSIN, and how the information would be processed, analyzed, and further disseminated.

It was not until almost two years after HSIN expansion began that DHS made efforts to clarify its systems relationships and its mission role. In August 2005, DHS assessed the Federal Protective Services Secure Portal System, a DHS system which supports secure communications and collaboration. This system, used across the law enforcement community, manages information to help ensure the safety and security of federal buildings, protection officers, and visitors. Although HSIN's mission is broader, DHS' internal analysis revealed that it significantly overlaps the mission of the Federal Protective Services Secure Portal System in supporting the law enforcement community. The analysis concluded that the two systems should be migrated to a common service portal.

It was not until August 2005 that DHS drafted a concept of operations for HSIN. However, the concept of operations document does not identify or classify the major categories of HSIN users. The document does not provide details on the variations in work processes corresponding to the different user communities or how they might apply the system to carry out their different responsibilities. Further, DHS posted the concept of operations to the HSIN portals without notifying system users. Therefore, infrequent HSIN users were unaware of the document's existence. Senior DHS officials stated that when they surveyed users they discovered few had read the document.

DHS has taken steps to improve understanding of HSIN. For example, a Frequently Asked Questions document, created in early fiscal year 2006, helps clarify the HSIN vision. The document describes HSIN, incentives to using the system, how it compares to other systems, and how it regulates as well as safeguards information. Further, DHS has made progress in establishing interoperability between HSIN and similar federal systems. For example, it has begun to allow products to be posted and shared between HSIN and

RISSNET and LEO, and is working with Department of Justice representatives to achieve complete interoperability in 2006. DHS has begun to coordinate with other intelligence and emergency management officials on ways to achieve interoperability, too.

## Ad Hoc System Development and Deployment

As a result of its accelerated schedule, DHS did not complete a comprehensive collection or analysis of user requirements prior to HSIN implementation. Consequently, successive rollouts of the HSIN versions were not well planned or adequately evaluated prior to each release.

### Identification of User Requirements

Office of Management and Budget Circular A-11 directs agencies to reduce project risk by involving stakeholders in the design of IT assets.[7] Involving users in requirements helps ensure a better understanding of system users, their technological environments, and the types of content they desire. Where users are not involved in system development, there is no way to ensure that the system will provide for their needed functions.

Despite these guidelines, DHS did not sufficiently involve users in the initial design of HSIN. According to a DHS official, the department did not complete an analysis to understand who would potentially benefit from the system. Instead, DHS expanded the system to additional homeland security, emergency management, and other user groups without clearly understanding their needs. In so doing, DHS also did not understand how allowing one group of users access to the system could adversely affect other participants. In general, DHS did not sufficiently gather requirements from the various system user groups. Instead, DHS developed HSIN using the same requirements obtained for JRIES, its predecessor. The JRIES requirements did not address the needs of the broader HSIN user base, but were the limited input of a functional working group of 25 law enforcement officials.

Requirements for subsequent HSIN releases were also not well defined. DHS relied solely upon requirements obtained from the law enforcement community when it moved the system from the Groove software to a series of portals in March 2005. DHS designed all of the portals to be identical in terms of applications and services, and assumed that they later could be tailored to meet specific community needs. Other communities, comprised of various officials such as firefighters, the National Guard, state homeland

[7] Circular A-11, Part 7, *Planning, Budgeting, Acquisition, and Management of Capital Assets*, Executive Office of the President, Office of Management and Budget, June 2005.

security advisors, and emergency managers, carry out significantly different functions and require different system functionality, information, and reporting capabilities than those considered.

As such, the emergency management portal did not share information with existing state emergency management systems. In addition, the emergency management portal was based off of law enforcement requirements such as "requests for information" and "for your information" postings, and emergency managers stated they do not use these features. HSIN program managers had hoped to work with Federal Emergency Management Agency officials to make the emergency portal useful, but the agency did not provide user requirements; ultimately, it did not want to take ownership of the portal. Further, state homeland security advisors said that HSIN postings are too detailed and do not provide the strategic level of information they need to perform their duties. Instead, state homeland security advisors obtain the information they need from other sources.

Our review of two separate listings of HSIN system requirements and user change requests revealed DHS deficiencies in tracking individual user community needs as well. We determined that the documentation did not group the requirements by the different user communities. Further, according to one official, the change requests that DHS provided were derived from a limited set of users at the HSOC and not from the broader HSIN user base.

DHS has begun to reach out to the broader user community to gather requirements input. In November 2005, DHS held a working group meeting in Jacksonville, Florida, to gather system user input and lessons learned DHS plans to hold similar quarterly symposiums with users in the future to discuss issues and gather recommendations for improvement. Additionally, in January 2006, DHS created the HSIN Advisory Committee to provide recommendations on the system requirements of users within the various communities of interest. At the request of the DHS chief information officer, the DHS Office of Intelligence and Analysis reviewed intelligence information sharing requirements, independent of technology. DHS officials stated that, while not a true system requirements document, the final report from this review will contain a combination of system and business requirements to support intelligence data flows.

## Numerous Ad-Hoc System Rollouts

Effective system development processes include evaluating systems prior to implementation to ensure that they successfully meet user requirements. However, according to a DHS comparison of HSIN to a related portal system, DHS did not evaluate adequately each of its three major HSIN releases prior

to their implementation.[8] Technical problems that went undetected given the lack of pre-deployment test and evaluation hindered system performance.

For example, DHS implemented one release of the system without first obtaining the legal approvals necessary for posting information contained in the HSIN document library. The library included daily and periodic reports from multiple sources such as the Homeland Security Operations Morning Brief and the DHS Cyber Report, constituting a critical resource and selling point of HSIN. Lacking a pre-deployment review that would have identified this issue early on, DHS had to shut down the entire document library for three to four months until the needed approvals could be obtained.

Similarly, DHS did not assess in advance the impact that HSIN expansion to an increased number of users would have on system performance. According to a DHS official, the additional users logging onto HSIN impacted the system's speed. Because system processing became so slow, new and infrequent users stopped using the system. It was at this point that DHS switched to the web portal technology after realizing that the Groove software was not able to meet the requirements of additional HSIN users.

DHS' rollout of HSIN to counties was problematic, too. The county rollout was an effort to connect DHS to major city police chiefs, sheriffs, and first responders in all 3,086 counties nation-wide. However, DHS did not adequately assess the impact that connecting directly to the counties would have on other system stakeholders. DHS also had not involved the states in this decision to connect to the counties. After beginning the rollout, DHS received criticism from state officials who felt that the states had been bypassed. At this point, DHS shifted the scope of the HSIN deployment from a county-level back to a state-level rollout.

State and local officials expressed gratitude towards DHS for shifting to the state level. Both DHS and state and local officials have since begun working on interoperability, information sharing protocols, and registration and vetting procedures. In some states, DHS is working to integrate HSIN with state systems, while in others it is creating new portals for the states. Further, the HSOC has begun to reach out to the other DHS components to encourage them to use the system. In January 2006, the DHS Secretary sent a memo to all department components affirming HSIN as the primary system for information sharing and collaboration within DHS and with its security partners.

[8] *Comparative Analysis of Homeland Security Information Network and the Federal Protective Service Secure Portal System in Consideration of the Department of Homeland Security Enterprise Portal*, Department of Homeland Security, Directorate of Information Analysis and Infrastructure Protection, August 19, 2005.

## User Guidance Needs Improvement

According to federal regulations, agencies should provide users with the skills, knowledge, and training needed to manage information resources effectively. However, DHS has not provided HSIN users with adequate guidance, training, or reference materials on what or how information should be shared using HSIN.

### Information Sharing Processes Need To Be Defined

According to Office of Management and Budget Circular A-130, agencies should simplify or redesign work processes before implementing new technology.[9] Such efforts, including defining and documenting business processes, can demonstrate to users how the system can be used to improve their work activities. However, DHS implemented HSIN without defining the sharing process for homeland security information. As previously discussed, the goal was to establish nation-wide HSIN connectivity first, and then decide on the information to be shared. Without a data flow process, DHS is unable to provide clear guidance on the information sharing process. As a result, users are not sure what information should be shared or in what format.

As of November 2005–almost two years after assuming responsibility for HSIN–DHS still had not modeled the information sharing process. The results of a DHS HSIN User Working Group documented this need, specifically requesting guidance on the types of information to be shared, the processes for sharing, how the information shared is used, and what users can expect from DHS in return. In the absence of adequate DHS guidance, states such as Virginia, Maryland, and Texas have begun to define information sharing processes and procedures on their own, potentially resulting in duplication of effort and lack of standardization.

DHS officials stated that defining the information sharing process is one of their foremost challenges and that two efforts are under the way to address this issue. First, the DHS Office of Intelligence and Analysis is working to map out how federal, state, and local entities share information in both the classified and unclassified domains. Second, the DHS Information Sharing and Collaboration Office plans to work with the HSOC director, and in coordination with federal, state, and local governments and the private sector, to develop guidance for sharing information via HSIN. Such guidance will include document labeling and handling policies, information sharing regulations, and database standards for HSIN, as well as other systems to

[9] Revision of OMB Circular No. A-130, Transmittal 4, Management of Federal Information Resources, November 28, 2000.

which HSIN may be connected. As of March 2006, DHS was still working to develop these materials.

One model that DHS might reference in defining its own information sharing process is the intelligence model included in the National Criminal Intelligence Sharing Plan. This plan was developed by the Global Justice Information Sharing Initiative Intelligence Working Group in coordination with the Department of Justice and in response to information sharing needs expressed at the International Association Chiefs of Police Criminal Intelligence Sharing Summit.[10] Other intelligence models share the same basic principles and phases. As such, although this model focuses on sharing law enforcement intelligence, we believe that it can be adapted and applied to the broader HSIN user communities. The circle in Figure 4 depicts the law enforcement intelligence sharing process; we have indicated in the boxes the areas DHS needs to address to be in line with this model.

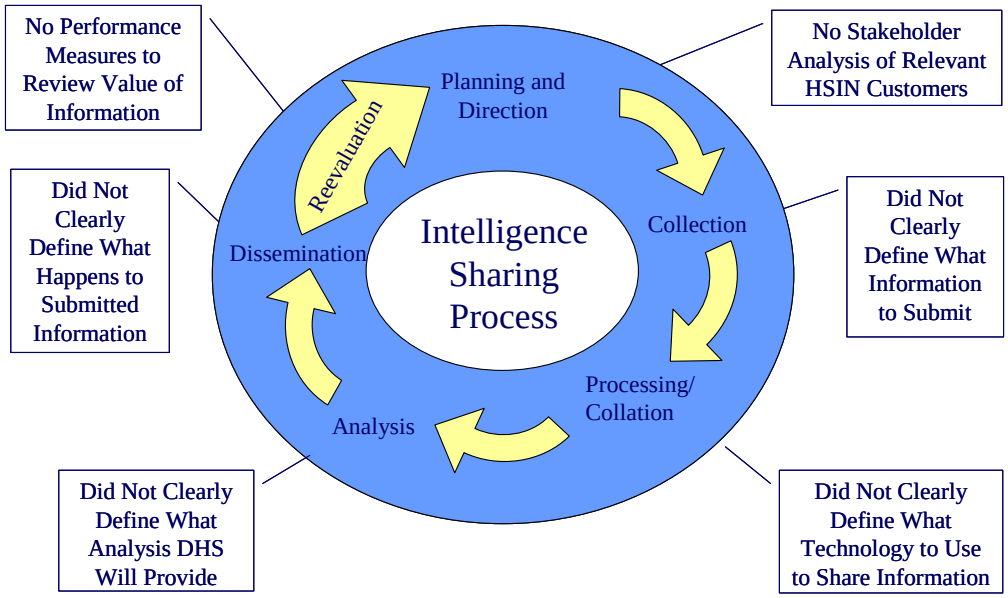


Figure 4: The Intelligence Sharing Model as Applied to HSIN

[10] The National Criminal Intelligence Sharing Plan provides law enforcement agencies with the ability to gather, analyze, protect, and share credible and timely information and intelligence to identify, investigate, prevent, deter, and defeat criminal and terrorist activities, both domestically and internationally, as well as to protect the security of our homeland and preserve the rights and freedoms of all Americans.

## User Training and Support

According to the *Clinger-Cohen Act*, agencies are responsible for ensuring that IT users receive the training and guidance that they need to do their jobs.[11] However, DHS did not provide adequate formal training to support users in the initial system release. A former HSIN program manager stated that providing sufficient user training was perhaps the biggest challenge that DHS faced. Further, a DHS official stated that the department implemented HSIN without providing sufficient business context as to why and how the system should be used to support operations in specific communities, such as emergency management, law enforcement, or state homeland security offices.

In the winter of 2004, DHS followed up with additional training in efforts to provide better business context for system use. However, this did not solve the problem because DHS switched from the Groove software to portal technology right after providing the training. To further complicate matters, DHS did not conduct extensive training on HSIN and its new portal technology, but instead provided instruction on an ad hoc basis. Generally, users in the field expressed the need for more HSIN training, especially how to perform intelligence work on the portal. A number of users were not aware of critical HSIN features, such as "request for information" tabs, document libraries, and chat capability.

In 2005, DHS made several efforts to improve its HSIN training. For example, DHS provided computer-based training, which was accessible directly through the HSIN portals, on how to use the system. Additionally, in the ongoing state and local HSIN rollout, DHS is offering new classroom training on a state-by-state basis. Users in one state provided excellent feedback to us on this training.

In addition to the lack of training, reference materials to support HSIN users need to be improved. DHS released user manuals for several HSIN portals in 2005. The manuals are clear with respect to system capabilities, however they do not provide users with scenario-based instruction on how to apply HSIN to the business process. For example, one user manual provides instructions on how to add a new record to the HSIN database, but does not indicate what types of incidents to report and in what format. A quick reference guide, which DHS created to assist users of one state portal, similarly lacks guidance on HSIN use in the business context.

[11] *Clinger-Cohen Act* (formerly the Information Technology Reform Act of 1996), Public Law 104-106, Division E, Section 5125, February 10, 1996.

DHS, in an effort to describe what information to report, coordinated with the Federal Bureau of Investigation to develop a Terrorism Threat Reporting Guide for use by its state and local partners. However, users found the guide too detailed and difficult to reference in conducting their day-to-day operations. The guide is merely a list of types of suspicious activities and is not tailored to meet the needs of specific user communities. Further, even though the guide is posted on HSIN, it does not mention the use of HSIN as a reporting mechanism, but instead directs officials to report suspicious activities via telephone or email. The general feedback that DHS has received from the law enforcement community regarding the guide is that it needs to be simplified to a laminated card that a police officer can easily reference on the street. However, DHS officials have countered that funding and time limitations prevent them from creating such additional products. In the absence of DHS support, one state has produced a laminated reference card on its own.

## Need For Performance Metrics

According to the *Government Performance and Results Act of 1993* agencies must establish performance goals as well as metrics that assess relevant outputs, service levels, and outcomes of each program activity.[12] Given HSIN's portal technology, DHS should be able to track performance by using a number of measures such as system logons and postings. Such measures would provide a good indication of both system use and the volume of information shared. However, DHS has not developed these performance measures. Instead, DHS assesses HSIN performance based on the number of active user accounts, which is not a good indicator of the quantity of the information shared using the system. Also, DHS measures performance by talking to stakeholders informally to gather anecdotal information on HSIN use. Such anecdotes may be helpful if systematically gathered and assessed to identify system capabilities that could be enhanced.

DHS officials agree that performance metrics are necessary and have begun to pursue ways to address this need. Specifically, in September 2005, a DHS Information Sharing and Collaboration office laid out a three-phased approach to creating performance metrics for DHS information sharing. The office has completed the assessment and planning phase and has begun phase two, metric design and pilot. Further, in conjunction with multiple stakeholders, the HSOC also is working to determine what needs to be measured as well as to establish a performance baseline for HSIN.

[12] *The Government Performance and Results Act of 1993,* Public Law 103-62.

# HSIN Needs To Support Information Sharing More Effectively

Largely due to the planning and implementation issues previously discussed, users are not fully committed to the HSIN approach. Although users we interviewed generally like the technology, they are somewhat confused about the HSIN's role and do not trust the system's ability to safeguard sensitive information. In addition, the system does not provide them with useful situational awareness and classified information. As a result, users do not regularly use the system but instead resort to pre-existing methods for sharing counter-terrorism information.

## HSIN Does Not Fully Meet User Needs

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 also do not fully understand HSIN's role and how the information shared on the system is used. Some users in the law enforcement community, in particular, told us that they do not trust the system to share sensitive intelligence information. Further, 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 content.

### Mixed Feedback on the HSIN Web Portal Technology

State and local users we interviewed generally like the HSIN technology. They stated that the web page design is user friendly and find it easy to search the document library for topics of interest. They appreciate the web technology because, unlike some other systems, it does not require cumbersome software installations at a desktop. Similarly, the portal technology helps ensure that all users always have access to the latest version of the HSIN software. Further, because logging onto HSIN only requires an internet connection, users can access the system from any location and from any computer at any time.

HSIN's flexibility and easy set up has made it particularly useful for communications and collaboration during special events. For example, in 2004, DHS created portals and adapted the system to support the Group of Eight Summit in Atlanta, the Academy Awards ceremony in Los Angeles, and

the Republican National Convention in New York City.[13] More recently, HSIN proved to be highly useful in supporting emergency response to the Hurricane Katrina disaster in the Gulf States in 2005. When other means of communications became unavailable, first responders were able to track over 22,000 emergency 911 calls via the HSIN-Katrina portal. DHS set up this portal within hours of the hurricane, sustaining critical communications and ultimately helping locate victims and saving lives.

State and local users nonetheless had several suggestions on how to improve HSIN. For example, several users said that the search functionality was not reliable or effective in locating documents or information they needed to perform their work. Some users could not access "Jabber" for online collaborations.[14] Others were especially frustrated by the lack of a directory of HSIN participants when such functionality had existed on the predecessor system. Without an HSIN participant list, users could not determine who had access to the system or easily identify officials with whom they needed to collaborate in other government agencies. Further, users wanted the HSIN logon function to be improved so that they would not have to sign on to each portal separately.

DHS is taking steps to address a number of these HSIN user issues. For example, the department is making efforts to better communicate the availability of the online "Jabber" collaboration tool. DHS plans to include a global directory in the next version of HSIN. DHS also has begun work to provide a single sign-on capability for HSIN.

## HSIN's Role Needs Clarification

In addition to requesting technical improvements, users are confused about HSIN's role with respect to information sharing. For example, they do not understand the purpose of HSIN in relation to other systems with similar functionality and are not clear about which system to use to support their work. We previously identified some of these systems, such as LEO, RISSNET, and the Federal Protective Services Secure Portal System. Multiple HSIN rollouts without adequate communications served to increase user confusion. For example, because DHS did not adequately announce the switch from the Groove technology to the portal system, some users were unaware of system changes and added features. Some users, for instance, told us that they did not know of the existence of the Jabber collaboration tool, made available when the HSIN portals were released. Although DHS officials

[13] The annual Group of Eight Summit brings together leaders of the world's richest nations: Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States.
[14] Jabber is a scalable, secure, real-time instant messaging application.

stated that they often post information on the portals to communicate system changes, users who do not regularly access HSIN do not receive such notifications.

In the absence of clear DHS direction, users are unsure of how to use HSIN. Several state officials said that they did not get clear answers when they asked what type of information to share on the system. Other officials expressed uncertainty about whether DHS wanted raw data or completed analyses posted to the portals. Local officials stated that DHS should provide standard criteria on how each stakeholder should report information. For example, users stated that a template, providing the format and the basic information that they need to share, would be useful.

Users told us that they became frustrated when they received feedback from DHS that the information they supplied was not useful. They said that HSIN program management had not provided clear guidance on what constituted a link to terrorism. In the absence of clear guidance, users therefore posted information on crimes that they believed were precursors to terrorist activities. However, DHS periodically responded by removing the information from the portals or adding "no terrorism nexus" to the postings, without providing clear justification for doing so. DHS has since moved to an "all crimes approach" to information sharing, meaning that any information posted by state and local officials on HSIN will be accepted. However, users said that there also has been no documented guidance to advise users of this policy change so that they will know what information can be shared.

Finally, state and local officials told us they do not understand what DHS does with the information that they supply and therefore lack incentive to provide information via HSIN. One user characterized DHS as a "black hole" into which they funnel information, but from which they receive no response. Users would like to receive DHS feedback and analysis on information that they provide, as well as notice about postings concerning potential threats that have been resolved.

## Lack of Trust

Some parts of the law enforcement community do not trust HSIN to share their sensitive case information. Although a primary function of HSIN is to provide law enforcement with an information-sharing tool, as DHS expanded the system to other communities, including state homeland security advisors, law enforcement users became concerned that their sensitive information would not be adequately safeguarded. Specifically, law enforcement officials we interviewed were worried that posting their information to a wide audience could result in cases being leaked or compromised, intelligence sources

divulged, or personal private data shared with users who do not have a need to know.

This privacy issue was a major point of contention. Law enforcement questioned whether HSIN is compliant with Title 28, Code of Federal Regulations, Part 23, which provides guidelines for law enforcement agencies that operate federally funded, multi-jurisdictional criminal intelligence systems. The regulation mandates that law enforcement systems safeguard the privacy and constitutional rights of individuals. The regulation defines the types of criminal information that can be stored on law enforcement systems, and how long the information can be maintained. Law enforcement officials were not confident that these requirements were met, given the manner in which HSIN was managed.

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 "hi-jacked" the system, federalizing what it believed to be a successful, cooperative federal, state, and local project. After departing, the JRIES executive board continued to promote its initial information-sharing concept as JRIES II, a separate system apart from HSIN. The new JRIES II was designed to restore the capability for secure intelligence sharing within the trusted law enforcement community. The JRIES executive board began by marketing JRIES II to ten key states and major municipalities.

HSIN program management has taken steps to resolve this trust issue. Specifically, the program management obtained a Department of Justice ruling that HSIN is compliant with Title 28, Code of Federal Regulations, Part 23. Also, HSIN program management obtained Department of Justice concurrence that state homeland security advisors can access law enforcement sensitive information since they serve in homeland security roles that have law enforcement responsibilities. Nevertheless, law enforcement officials in the field told us that they were reluctant to allow HSIN users from outside their community to see their sensitive case information. Law enforcement officials said that information sharing among law enforcement personnel is based on trust. Once that trust is lost, it takes time to rebuild.

## HSIN is Not Providing the Information Needed

State and local users said that HSIN does not provide them with the timely and relevant information that they need to support their counter-terrorism

missions. They stated that HSIN does not provide them the situational awareness they need to manage or respond to emergency operations or terrorist-related events. 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 or quicker information by calling personal contacts at law enforcement agencies with connections to the London police, than by using the system. State and local users understand that at times, DHS may not have additional information to post apart from what is already available to the public. However, even though DHS might not have additional information, users said they would prefer that DHS provide periodic HSIN updates to this effect, rather than provide no information at all.

The lack of good situational awareness can lead states and cities to either over-react to reported threats–and potentially waste resources–or under-react and leave themselves vulnerable. For example, the United States Conference of Mayors published the results of a 145-city survey and stated that deploying resources to respond to terrorist alerts can increase costs nation-wide by about $70 million per week. Such expenditures are wasted when the reported threats turn out to be invalid. During the blackouts in the Northeastern United States, cities and states in other parts of the country learned right away through JRIES that the power failures were not terrorist-related. Therefore, these other cities and states did not have to unnecessarily expend additional funds to increase security. Conversely, where officials under-react, their localities may be unprepared and potentially vulnerable to incidents that actually do occur.

## HSIN-Secret Does Not Contain Useful Products

State and local officials said that the HSIN-Secret portal does not provide valuable content. HSIN-Secret is meant to function as a temporary channel to deliver secret-level, classified information to state and local officials until the Homeland Secure Data Network is completed. However, users said that very few documents are available on the classified web site. Figure 5 indicates the number of documents posted to the HSIN-Secret portal since it was created. In general, there have been an average of about 27 logons per month, from a total of 366 account holders across all 50 states.

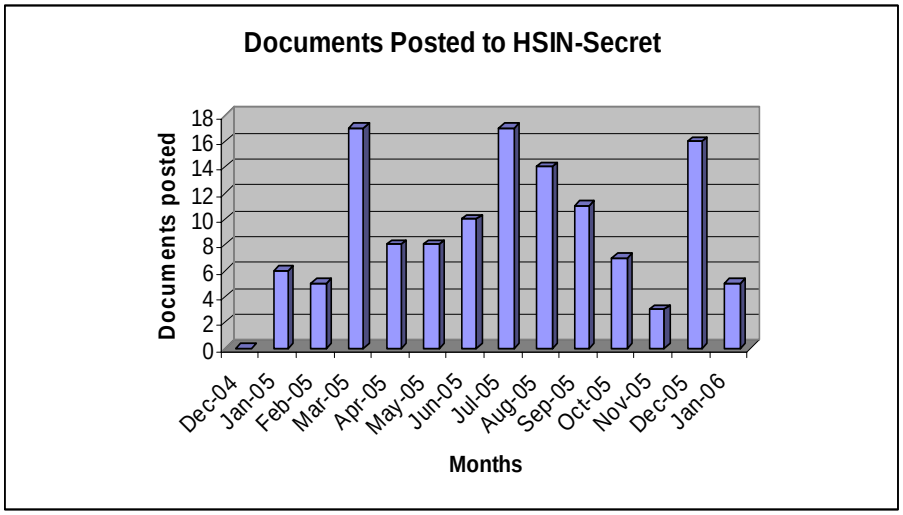


Figure 5: Documents Posted to HSIN-Secret

In addition to the lack of useful content, HSIN-Secret also faces several technical challenges. HSIN-Secret connectivity was established in state emergency operation centers because they had the infrastructure to support it; however, state and local officials believed that state fusion centers are the more appropriate locations for HSIN-Secret connection because the state individuals that primarily require access to the system often are located at the fusion centers rather than the emergency operations centers.[15] Further, HSIN-Secret at several state emergency operation centers does not function at all, due to outdated encryption keys that do not allow users to access the system.

## State and Local Officials Do Not Rely on HSIN

As a result of their frustrations with HSIN, state and local officials do not regularly use the system and instead resort to prior systems and methods to share counter-terrorism information. Data provided by HSIN program management demonstrates that user logons and postings are limited, and that users do not rely upon the system as the nation's primary information sharing and collaboration network as DHS intended.

### Users Resort to Prior Ways of Sharing

Because HSIN does not fully meet their needs, state and local officials said that they resort to systems and methods they previously used to share information. For example, law enforcement users said that they often use other existing systems, such as LEO, RISSNET, and the Federal Protective

[15] 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.

Services-Secure Portal System. As previously discussed, some members of the JRIES executive board use JRIES II as an alternative to the HSIN portal. 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-piped information-sharing environment that HSIN was intended to correct.

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, too. 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, because they did not receive useful or timely updates through HSIN, law enforcement officials relied heavily upon telephone calls to share information related to the reports in October 2005 that terrorists were threatening to detonate a truck bomb inside the Baltimore tunnel. One official received 96 telephone inquiries in a single day about the incident. Another official said that during the Hurricane Katrina response in 2005, first responder organizations were inundated with phone calls, many of which were not successful due to the heavy call volume.

## User Communities Make Limited Use of HSIN

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

### Limited Logons

Data provided by HSIN program management indicates that the number of daily logons to HSIN is limited. 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 counter-terrorism portals–has remained consistently low. Figure 6 shows the average percentage of account holders who logged onto HSIN daily in

December 2005. That month was the latest time period for which HSIN program management was able to provide usage data.

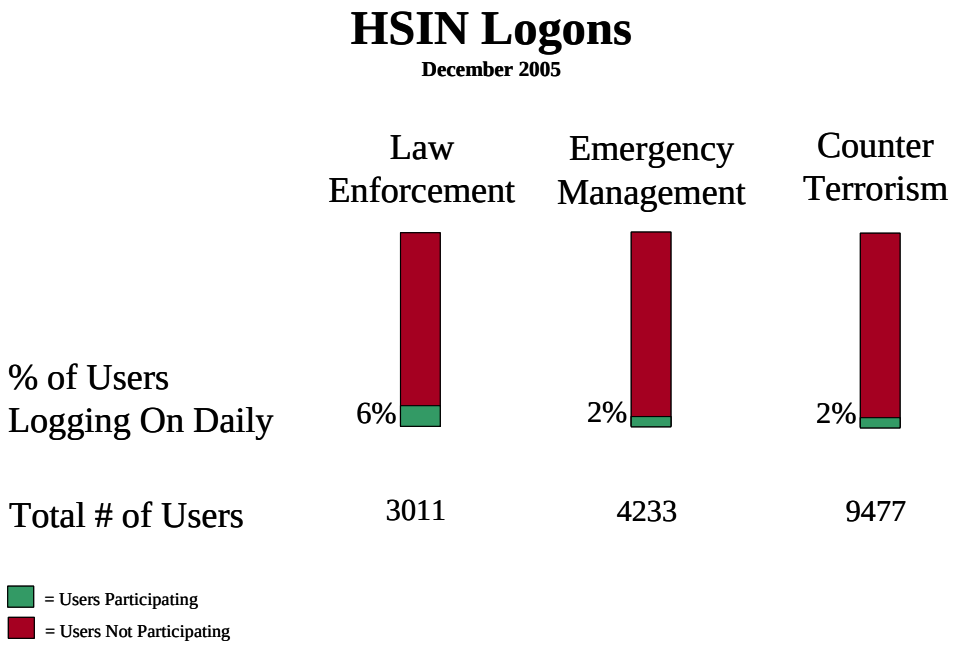


Figure 6: HSIN Logons

Although the total number of accounts for the law enforcement portal has grown over the past year, only a small percentage of account holders log onto the system daily. As Figure 6 indicates, of the approximately 3,000 account holders on the law enforcement portal, an average of only six percent logged on daily in December 2005.[16] The peak average daily logons for any given month in the year 2005 was 12 percent.

Further, of the approximately 4,000 accounts on the emergency portal, an average of only two percent logged on daily in December 2005. Average daily usage reached its highest monthly level, 11 percent, in September 2005, due to inquiries during the Hurricane Katrina response. Usage of the counter-terrorism portal was similar: of the approximately 9,500 account holders on this portal, an average of only about two percent logged on daily. Again, usage peaked in September 2005 due to Hurricane Katrina; the highest level of average daily logons for that time was three percent.

[16] Percentages were obtained by dividing the total number of daily system logons by the total number of account holders. This percentage represents the maximum average number of users who logged on per day.

## Limited Postings

We examined the average number times that users posted documents and information to HSIN each month as a means of measuring use of the system. According to data we received from HSIN program management officials, the number of postings to the law enforcement, emergency management, and counter-terrorism portals has remained fairly constant for the past six months. Figure 7 shows the average monthly percentage of users posting information to three major HSIN portals in December 2005.

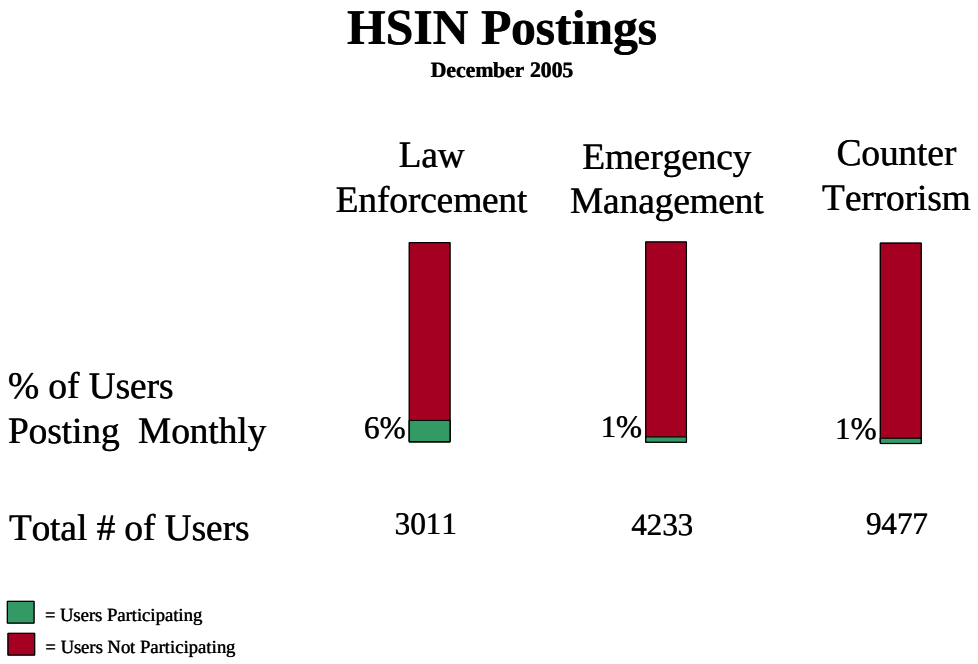


Figure 7: HSIN Postings

As indicated, the average percentages of daily postings for the three communities in the month of December were comparable to the logon levels previously discussed. HSIN program management officials have expressed dissatisfaction with the levels of information sharing on the system over the past year. However, they have not established performance goals to indicate what they believe would be an acceptable number of postings each month.

In another effort to determine the extent to which users are utilizing the system to share information, we compared the numbers of users and their percent of total postings on three major HSIN portals to the number of users and their percent of postings on the legacy JRIES system. (See Figure 8.) In January 2006, the number of total postings by users of the three HSIN portals

and the legacy JRIES combined was 851. For that month, the percentage of total HSIN postings for the 157 users of the legacy JRIES system was over 50 percent–greater than the percentage of total postings by approximately 18,000 users on the three major HSIN portals combined. In other words, a relatively small number of users on the legacy JRIES system accounted for the majority of the total HSIN postings for the given month.

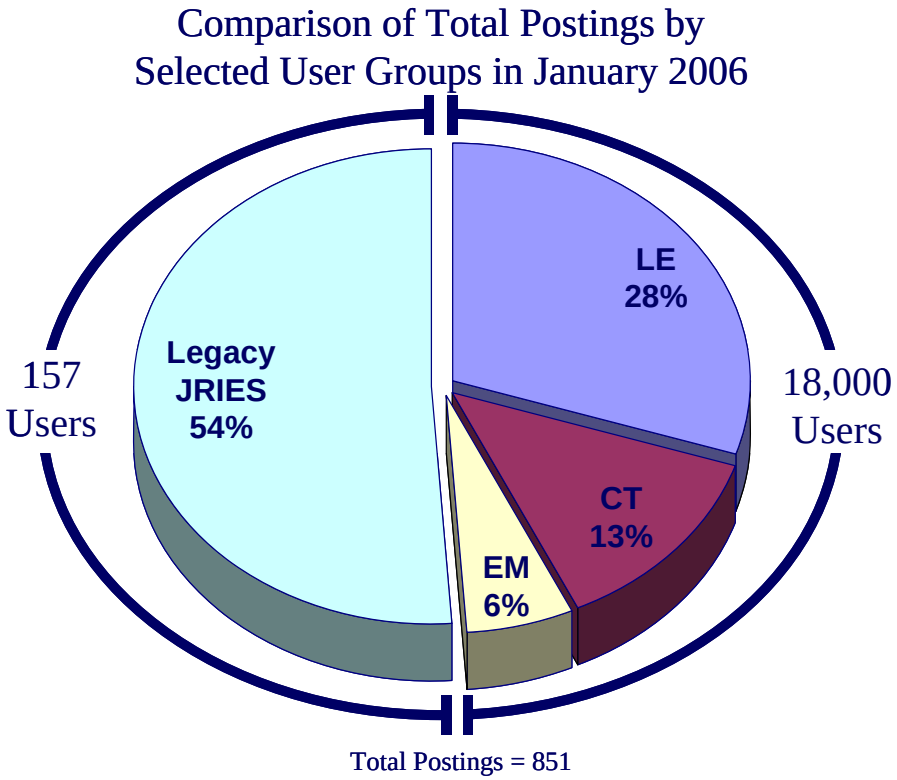


Figure 8: Comparison of Total Postings by Selected User Groups in January 2006

HSIN program management officials plan to migrate users from the legacy JRIES system to the HSIN portals, which are more flexible because they can be accessed anywhere via the internet and also can accommodate a greater number of users across various community groups. In line with this plan, program managers report that since the HSIN portals were created in 2005, the legacy JRIES system has had a declining number of account holders and decreased use. Despite this trend, posting activity on the legacy JRIES system remains strong when compared to postings on the three main HSIN portals. Continued postings on the legacy JRIES system results in additional effort because, to ensure that needed information is accessible to the broader user community, DHS must copy the legacy JRIES data onto the HSIN portals.

## Other Major Challenges

DHS faces multiple challenges in successfully implementing HSIN to support homeland security information sharing. In addition to the technical system issues discussed above, promoting the use of HSIN for information sharing across federal, state, and local governments, including law enforcement, intelligence, and emergency management communities, is a complex, multi-faceted undertaking that has proven problematic. Figure 9 groups the various challenges related to HSIN implementation into four broad categories: resources, legislation, privacy, and culture.


Figure 9: HSIN Challenges

Acknowledging and addressing these challenges will not only improve the quality and quantity of information shared using HSIN, but also help efforts to deter terrorism and respond to incidents overall. However, because these challenges are often beyond the control of HSIN program management to resolve, DHS cannot address them alone. Devising solutions to successfully overcome these concerns will require coordination and collaboration across the range of government, community, and organizational stakeholder groups.

## Resources

Resource limitations have hindered the ability of organizations at all levels of government to effectively share information and will undoubtedly continue to pose challenges in the future. DHS officials cited a lack of sufficient personnel as a reason for being unable to provide vital support to HSIN users, especially during its initial release. For example, since implementing HSIN, DHS has participated in information sharing conferences, suspicious activities forums, and large advisory meetings along with the range of system stakeholders. However, because DHS did not have adequate personnel to develop professional relationships with individuals in the various user communities, department officials stated that their initial contacts were limited and short-lived. Establishing longstanding and dependable relationships with users is an important factor in gaining and sustaining their support and trust.

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. Intelligence analysts in another state said they could not concurrently monitor both the JRIES and HSIN portals so their supervisor told them just to monitor the JRIES portal. State officials are concerned that DHS is planning to monitor their usage of HSIN to help determine future allocations of grant funds to states.

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. To illustrate, some state officials said that states are dependent upon federal funds to enable them to fully operate such intelligence centers and actively participate in information sharing with federal agencies. In addition, states that do not have sufficient resources to establish their own web presence for sharing information welcome the HSIN state portal pilot program, under which the HSOC funds and manages the system and its operations. State officials are concerned, however, that the Homeland Secure Data Network, the eventual replacement for the HSIN-Secret portal, may not be provided to states with federal funding. Some states may not be able to afford participating on the portal at their own expense.

## Legislation

Legislative requirements also 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. The new program manager plans to build on the collective capabilities of HSIN and other federal systems to establish the mandated environment. However, at the time of this audit, it was not clear what HSIN's role will be in this context. Identifying that role, and ensuring the success of the new information-sharing environment, will require close coordination and collaboration by all of the federal stakeholders involved.

State laws, which differ from state to state, 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.

In the past several months, DHS has taken steps to collaborate with the individual states to better understand their respective legislative environments. DHS began reaching out to several states as part of the HSIN state portal pilot program, which should give the department the opportunity to assess each state's information-sharing laws. HSIN program managers also are working with the states to develop memorandums of agreement that will define how the states will cooperate with DHS to effectively share information. These efforts have been well received by state representatives and should increase the likelihood of successful information exchange between the department and its state and local counterparts.

## Privacy

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 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.

By not appropriately considering privacy concerns, HSIN could face a similar outcome before realizing its full potential. As required by the *Homeland Security Act*, and in efforts to assuage civil liberty concerns, DHS performed a privacy impact assessment of HSIN portals before deploying them. As a result of the privacy impact assessment, DHS had to shut down the HSIN document library, which contained reports from nation-wide sources, significantly hampering system usefulness. In addition, DHS is currently creating another database that will need a privacy impact assessment prior to implementation. This database is to 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 necessary to ensure and to demonstrate to concerned consumer groups, that the information gathered through HSIN does not violate the rights of American citizens.

## Culture

A culture that is not receptive to knowledge sharing is one of the foremost hurdles to widespread adoption of collaboration software. Such cultural issues have limited HSIN's use and, therefore, its effectiveness.

HSIN users comprise diverse communities, including state and local government officials, emergency managers, law enforcers, intelligence analysts, and other emergency responders. All have different missions, needs, processes, and cultures. Because of these differences, the various user groups often 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. As discussed previously, a lack of trust in the law enforcement community has led to low use of HSIN to share sensitive information. 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.

Despite the availability of HSIN, some state and local users continue to share information with agencies other than DHS with whom they developed trusted relationships in the past. For example, local law enforcement communities have developed close associations with the Federal Bureau of Investigation's network of Joint Terrorism Task Forces, which investigate and respond to reports of terrorist-related activities and incidents in their areas. Law enforcement officials told us that, although they have access to HSIN, they typically share information on suspicious activities with their Joint Terrorism Task Forces contacts and expect them to pass the information to DHS. These officials explained they prefer to notify the Joint Terrorism Task Force first instead of DHS, because they know that the task forces will send personnel to the field to investigate. Conversely, it is unclear to these officials what DHS does with information on suspicious activities.

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.

## Recommendations

To ensure effectiveness of the HSIN system and information sharing approach, we recommend 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 crosscutting 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.

## Management Comments and OIG Evaluation

We obtained written comments on a draft of this report from the Acting Director, Office of Operations Coordination. We have included a copy of the comments in their entirety at Appendix B.

In the comments, the Acting Director concurred with our recommendations in their entirety. The Acting Director further said that the recommendations are solid, and when implemented, will improve the effectiveness of the HSIN system and information sharing. The Acting Director added that there are two primary reasons why HSIN is not more effectively supporting information sharing. First, the HSIN program lacks many aspects of a typical federal program due to the expedited effort to roll out the program. Second, according to the Acting Director, the Secretary has directed that a coordinating body within DHS, consisting of the Under Secretary for Policy, the Assistant Secretary for Intelligence and Analysis, the Director of Operations, and the Chief Information Officer, coordinate an accelerated information sharing enterprise. This effort hindered HSIN implementation.

In response to recommendation 1, the Acting Director acknowledged the need to clarify and communicate HSIN's mission and vision to users, its relations to other systems, and its integration with related federal systems. Specifically, the Acting Director said that the Office of Operations Coordination has engaged external partners to improve coordination and clarify the purpose of existing information systems. Additionally, the Acting Director indicated that there is a need for customer satisfaction performance metrics to determine progress toward meeting communication objectives successfully.

In response to recommendation 2, the Acting Director of Operations indicated that the Assistant Secretary for Intelligence and Analysis is working to define an 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. The Assistance Secretary for Intelligence and Analysis will define and publish the intelligence data flow for the Homeland Security community. Further, the Office of Operations Coordination will partner with Intelligence and Analysis to ensure that the entire user community understands the data flow model and uses it effectively to both supply and consume information that fuels this information sharing system.

To address recommendation 3, the Acting Director is exploring plans to reorganize the program management function of HSIN into a program office dedicated to supporting all aspects of the HSIN program including providing detailed, stakeholder-specific standard operating procedures, user manuals, and training based on the business processes needed to support homeland security information sharing. Further, the HSIN Program Management Office will have a dedicated program manager to engage all HSIN stakeholder groups to assess deficiencies in training materials and standard operating procedures to optimize operational effectiveness.

In response to recommendation 4 regarding ensuring crosscutting representation and participation among the various stakeholder communities to determine business and system requirements, the Acting Director established a governance program for HSIN, called the HSIN Advisory Council. This Council provides a forum for user communities to provide feedback on ways to improve information sharing among all communities of interest.

Finally, to address recommendation 5, the Acting Director said that a Program Management Office would be established to partner with HSIN user communities to identify and implement robust performance metrics.

As background for this audit, we researched and reviewed IT laws, regulations, and other federal guidance applicable to DHS' responsibility for coordinating terrorist-related information sharing with state and local governments. We reviewed prior GAO and DHS OIG reports related to homeland security information sharing. We searched the internet to obtain testimony, published reports, documents, and news articles regarding DHS' information sharing approach and the use of the JRIES and HSIN systems. Additionally, we met with organizations that had researched terrorist-related information sharing, including GAO, the Congressional Research Service, and the National Governors Association. Using this information, we designed a data collection approach, which consisted of focused interviews and documentation analysis. We developed a series of questions and discussion topics to facilitate our interviews.

We interviewed DHS management officials and staff to obtain an understanding of DHS' approach to sharing terrorism-related information using HSIN. These officials discussed their roles, responsibilities, and activities related to planning and implementing HSIN. We collected and reviewed numerous documents from DHS officials about their plans and current initiatives for HSIN, too.

We visited seven state capitals and five major cities where we interviewed various employees including political appointees, senior managers, and intelligence analysts. We focused on the systems they used, the business processes, communication with DHS, and training. We obtained information on how HSIN is being used in the field and if DHS is providing the necessary tools and guidance to the state and local governments. Where possible, we obtained reports and other materials to support the comments and information they provided during the interviews.

Specifically, we visited:

- State homeland security advisors, to learn about the role of HSIN in the state-wide strategy for homeland security.
- State police, to gain an understanding of how they utilize HSIN to process terrorism-related information.
- State emergency management agencies, to understand how HSIN is used at the state level for emergency management and situational awareness.
- State fusion centers, to learn about their role in coordinating intelligence gathering and analysis for states and facilitating with the HSOC.
- State national guards, to understand how they are using HSIN in their operations.

- Major city police departments, to learn how HSIN supports terrorism-related intelligence information sharing and analysis in large cities.
- Major city emergency management agencies, to understand how HSIN is used at the city-level for emergency management situational awareness.
- Major city fire departments, to learn about the role of HSIN in passing terrorism-related information with fire departments.

Additionally, we met with two external groups that have completed work on terrorism-related information sharing. To gain a perspective on the roles of related IT systems, we met with the Western State Information Network and discussed its system's role in the terrorism-related information sharing process in relation to HSIN. Further, officials from the U.S. Department of Justice Anti-Terrorism Advisory Councils described their role in facilitating information sharing with state and local governments as well as how they interact with various federal, state, and local entities.

We limited our audit of HSIN to a specific set of portals, focusing on the law enforcement, law enforcement analysis, emergency management, secret, special events, and the national capital region portals. Due to time and scope limitations, we did not review the critical infrastructure, private sector, or international portals. Throughout the course of this audit, we provided regular updates to the DHS management on progress and discussed key issues identified by the stakeholders.

We conducted our review from September 2005 to January 2006 at locations in Harrisburg (PA); Sacramento (CA); Los Angeles (CA); Las Vegas (NV); New York City (NY); Albany (NY); Boston (MA); Austin (TX); Springfield (IL); Chicago (IL); Reisterstown (MD); Richmond (VA); Chantilly (VA); and, the Washington (DC) metropolitan area. We performed our work pursuant to the Inspector General Act of 1978, as amended, and according to generally accepted government auditing standards.

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, and Sondra McCauley, Director, Information Management. Major OIG contributors to the audit are identified in Appendix C.

*Office of the Director of the*
*Operations Directorate*
**U.S. Department of Homeland Security**
Washington, DC 20528

Homeland Security

**MEMORANDUM TO:** Richard L. Skinner
Inspector General

**FROM:** Wayne Parent
Acting Director of Operations Directorate

May 5, 2006

**SUBJECT:** Response to Draft Audit Report – *Homeland Security Information Network Could More Effectively Support Information Sharing*

This is in response to the April 6, 2006, memorandum requesting the Operations Directorate's comments on the draft Office of the Inspector General report, *Homeland Security Information Network Could More Effectively Support Information Sharing*. We appreciate the opportunity to respond to the draft report. The attached document provides comments on the five recommendations directed to Operations.

Attachment

cc: Steven Pecinovsky

**DHS Response to draft Office of Inspector General Report recommendations in *"Homeland Security Information Network Could More Effectively Support Information Sharing"***

**Overall Comments:**

The draft Department of Homeland Security (DHS) Inspector General's Report identifies shortfalls and gaps in the Homeland Security Information Network (HSIN) Program. Moreover, the report properly placed HSIN in the larger context of information sharing by identifying DHS plans and activities for sharing information with state and local governments; determining how well HSIN supports these plans and activities; and identifying challenges to information sharing among federal, state, and local governments. The recommendations are all solid suggestions that, when implemented, will improve the effectiveness of the HSIN system and information sharing.

From the Operations Directorate's perspective there are two primary reasons why HSIN is not more "effectively supporting information sharing." The first is that the present HSIN "Program" lacks many aspects of a typical Federal government program. As noted in the report, the expediency to roll out HSIN meant that several critical elements of the program such as requirements definition, program goals, milestones (metrics) and understanding user needs were not thoroughly assessed. The Directorate will address the problem of inadequate program oversight and management by creating a HSIN Program Management Office with an experienced GS-15 to manage all aspects of this program.

The second major issue related to HSIN can be found in the memo titled "Information Sharing at the Department of Homeland Security" dated December 16, 2005, which addresses the Secretary's guidance to ensure that " . . . all information pertinent to the security of the homeland is provided to all who need it in a comprehensive and timely manner." Seen in the larger context of the Department's information sharing system, HSIN has the potential to become a more important DHS conduit between Federal, State, local and tribal and private sector partners. As you know, information sharing is a collaborative process; it cannot be done in isolation. The Secretary has directed that a coordinating body within DHS consisting of the Under Secretary for Policy, Assistant Secretary for Intelligence and Analysis, the Director of Operations and the Chief Information Officer coordinate an accelerated information sharing enterprise. Our stakeholders and partners will benefit from this comprehensive and collaborative effort.

For all its shortfalls, at present HSIN is the most viable DHS option for sharing information across a wide spectrum of users – but its potential has not been realized. With the creation of the Department's "Common Operating Picture" (COP) situational awareness tool, users will soon gain access to information that will improve decision making. The prescribed means for sharing the COP will be HSIN – we need to make this system work.

**Comments on Recommendations:**

**Recommendation 1: Clarify and communicate HSIN's mission and vision to users, it relations to other systems, and its integration with related federal systems.**

Concur. The Operations Directorate has directly engaged many of the external partners in information sharing to improve coordination and clarify the purpose of existing information systems. HSIN is linked to Department of Justice systems (LEO and RISSNET). This effort may help reduce user confusion – but admittedly until there are established metrics to measure the impact, the Directorate cannot directly measure "user" satisfaction.

**Recommendation 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.**

Concur. The Assistant Secretary for Intelligence and Analysis (IA) is working to define and publish the intelligence data flow model for the Homeland Security community. IA has assumed responsibility for the management of all classified content shared on the HSIN Secret system and is also focusing on an information sharing model that will maximize the quantity and quality of unclassified, actionable information available on the Sensitive but Unclassified (SBU) system. The Operations Directorate will partner with IA to ensure that the entire user community understands the data flow model and uses it effectively to both supply and consume information that fuels this information sharing system.

**Recommendation 3: Provide detailed, stakeholder-specific standard operating procedures, user manuals, and training based on the business processes needed to support homeland security information sharing.**

Concur. The Director of Operations will elevate the importance of this programmatic responsibility for HSIN. The program management function is being reorganized into a program office dedicated to support all aspects of the HSIN program. This reorganization will establish a dedicated HSIN Program Manager who will report directly to the Director of Operations. This person will engage all HSIN stakeholder groups to assess deficiencies in training materials and standard operating procedures and ensure that adequate training material and support is available to optimize the operational effectiveness of this capability. The program office will also provide regular reports to the governance board which has been approved by the Secretary.

**Recommendation 4: Ensure crosscutting representation and participation among the various stakeholder communities to determine business and systems requirements, and encourage community of interest advisory board and working group participation.**

Concur. The guidelines for developing the Operations Directorate's crosscutting representation among user communities is addressed in the Secretary's memo "Information Sharing at the Department of Homeland Security", *" Ensure Mission Critical Collaboration (Liaison) Including Cross-cutting Homeland Security Operational and Policy Liaison.* Additionally, we will seek external requirements through the establishment of a governance program called the HSIN Advisory Council. This Advisory Council will be created within the next six months. The Advisory Council will provide a forum for the user communities to provide feedback to DHS concerning measures that should be taken to improve information sharing within and among all communities of interest.

The HSIN Program continues to work closely with the State Homeland Security Advisor offices to complete the deployment of HSIN to the city and county level agencies in all 50 states. The local level rollout of HSIN has been completed in eight states and is progressing in 24 additional states. The current focus of deployment efforts is on localities that are likely to be impacted by hurricane activity. Operations will provide dedicated training to user communities in these areas to improve HSIN effectiveness prior to the beginning of hurricane season.

**Recommendation 5: Indentify baseline and performance metrics for HSIN, and begin to measure effectiveness of information sharing using the performance data compiled.**

Concur. The Operations Directorate will establish a Program Management Office that will ensure that performance measurement is focused on relevant programmatic metrics, and not simply on counting activity. The HSIN program management office will partner with the HSIN user community to identify and implement robust performance metrics program that will drive improvement in mission effectiveness.

## Information Management Division

Sondra McCauley, Director
Richard Harsche, Audit Manager
Steve Ressler, Auditor
Steven Staats, Auditor
William Matthews, Referencer

**Department of Homeland Security**

Secretary
Deputy Secretary
Chief of Staff
Director, Office of Operations Coordination
Director, Homeland Security Operations Center
Program Manager, Homeland Security Information Network
Office of State and Local Government Coordination
Office of Information Sharing and Collaboration
Assistant Secretary, Office of Intelligence and Analysis
Under Secretary for Preparedness
Chief Information Officer
Chief Information Security Officer
Preparedness Directorate, Audit Liaison
Executive Secretariat
General Counsel
Assistant Secretary for Policy
DHS Legislative Affairs
DHS Public Affairs
DHS GAO OIG Audit Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch
DHS OIG Budget Examiner

**Congress**

Appropriate Congressional Oversight and Appropriations Committees

**Additional Information and Copies**

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

**OIG Hotline**

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations–Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.