



Department of Homeland Security Office of Inspector General

DHS' Efforts to Improve the Homeland Security Information Network



Office of Inspector General

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



**Homeland
Security**

October 29, 2008

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, efficiency, and effectiveness within the department.

This report addresses the strengths and weaknesses of the Homeland Security Information Network. It is based on interviews with employees and officials of relevant agencies and institutions, 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.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary	1
Background	2
Results of Audit	4
Increased HSIN Use Reported But Limited Nationwide Sharing	4
Improved Training Delivery Methods	5
Stakeholder Involvement and Communications Challenges	5
Information Sharing Process Not Defined	7
Stakeholder Dissatisfaction	8
Performance Measures Not Developed	8
Recommendations	9
Management Comments and OIG Analysis	11

Appendices

Appendix A: Purpose, Scope, and Methodology	13
Appendix B: Management Comments to the Draft Report	15
Appendix C: Major Contributors to this Report	20
Appendix D: Report Distribution	21

Abbreviations

COI	Community of Interest
DHS	Department of Homeland Security
HMCC	HSIN Mission Coordination Committee
HSIN	Homeland Security Information Network
HSIN-AC	HSIN Advisory Council
HSIN Next Gen	HSIN Next Generation
HS SLIC	Homeland Security State and Local Intelligence Community
I&A	Office of Intelligence and Analysis
IT	Information Technology
OIG	Office of Inspector General

Table of Contents/Abbreviations

OMB	Office of Management and Budget
OPS	Office of Operations Coordination
SLC	System Life Cycle

Executive Summary

We evaluated the Homeland Security Information Network's (HSIN) support of information sharing as a followup to our June 2006 audit report, *Homeland Security Information Network Could Support Information Sharing More Effectively*. The audit objectives were to determine: 1) progress toward addressing our recommendations from the June 2006 HSIN report; 2) the status of information sharing among select HSIN stakeholders; and 3) challenges and barriers to HSIN's use and implementation.

The Department of Homeland Security (DHS) made some progress in addressing our recommendations, and is taking steps to upgrade the current version of HSIN. To be successful, however, DHS' planned future upgrades of HSIN need to address a number of concerns identified in the previous audit.

Specifically, DHS needs to identify HSIN's users and determine their information sharing requirements. Lacking a good understanding of the HSIN user community, DHS has been unable to define the information sharing process or provide adequate user support. In addition, although HSIN stakeholders report increased use of the tool within states, nationwide information sharing remains limited. Finally, DHS has not developed performance measures to enable it to track or assess information sharing using HSIN.

We are recommending that DHS:

- Provide sufficient resources to improve stakeholder relations, ensure adequate stakeholder involvement and communication, and meet the needs of its customers at the federal, state and local, tribal, and private industry levels;
- Develop scenario-based training for stakeholders and communicate the availability of existing training;
- Ensure that system performance and information sharing metrics are included in any and all future HSIN developments; and
- Define and communicate DHS' information sharing process to ensure that users understand what information to share and what DHS does with the information.

Background

A critical aspect of the DHS mission is information sharing. This responsibility requires a robust information-sharing environment. HSIN is the department's sensitive but unclassified level, internet-based, information sharing tool designed to support this facet of DHS' mission. DHS obtained the system in 2003 to establish a secure communications and information technology (IT) infrastructure. HSIN enables the department and its intelligence, law enforcement, and emergency management partners to collect, analyze, and disseminate information in order to detect and deter threats to the security of the homeland.

In February 2008, the department reported to the Congress that DHS has spent approximately \$69 million on HSIN over the past 5 years. Additionally, the department reported to the Office of Management and Budget (OMB) an estimated annual cost of \$21 million for the HSIN program for budget year 2008.

The DHS Office of Operations Coordination and Planning (OPS) manages the HSIN program. OPS is responsible for monitoring the security of the United States on a daily basis and coordinating activities within the department and with governors, homeland security advisors, law enforcement partners, and critical infrastructure operators in all 50 states and more than 50 major urban areas nationwide. In order to achieve these goals, OPS developed and maintains HSIN as the primary means for communication, collaboration, situational awareness, and information sharing.

In February 2008, DHS announced that it planned to upgrade the current version of HSIN to meet the needs of its growing user base in state and local governments and private sector communities. The upgrade, referred to as the Next Generation of HSIN (HSIN Next Gen), will be phased-in after the May 2008 contract award for HSIN Next Gen. The effort will involve upgrading current HSIN system capabilities to support DHS' objective to significantly increase information interoperability and security with security partners and their systems.

HSIN Next Gen will follow best practices for system implementation and integration, including the use of a System Life Cycle (SLC) framework for system acquisition and development efforts. DHS' SLC, though still in draft, identifies specific steps to take prior to beginning the system development process, including the gathering of data requirements, development of a concept of operations, and definition of business processes. DHS developed the SLC to ensure that IT resources are managed effectively, and that solutions meet user requirements and support DHS' strategic goals and objectives. Following the SLC framework during the creation of HSIN Next Gen should help ensure that stakeholders are involved in the process and, therefore, will better understand how they can use HSIN to support nationwide information sharing.

Further, the HSIN Next Gen requirements document for the planned upgrade recognizes the importance of being able to monitor and evaluate system effectiveness. The system will be able to produce performance reports relating to:

- System use, showing how end users interact with the system;
- System health or availability, showing the operational state of the system; and
- System content, to track trends in information sharing using HSIN.

Building these metrics into HSIN Next Gen will provide a basis for program management to monitor and evaluate the tool's information sharing effectiveness.

In June 2006, we reported that DHS did not define HSIN's relationship to existing systems, obtain and address user requirements, provide adequate user guidance, or develop performance measures for HSIN.¹ These system planning and implementation issues limited HSIN's ability to effectively support state and local information sharing.

To improve the effectiveness of HSIN in support of the department's information sharing environment, we recommended that DHS:²

¹ DHS OIG, *Homeland Security Information Network Could Support Information Sharing More Effectively*, OIG-06-38, June 2006.

² Recommendations 1, 3, 4, and 5 were assigned to DHS' Office of Operations Coordination. Recommendation 2 was assigned to DHS' Office of Intelligence and Analysis.

-
- Clarify and communicate HSIN’s mission and vision to users, its relation to other systems, and its integration with related federal systems.
 - 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.
 - Provide detailed, stakeholder-specific standard operating procedures, user manuals, and training based on the business processes needed to support homeland security information sharing.
 - 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.
 - Identify baseline and performance metrics for HSIN, and begin to measure effectiveness of information sharing using the performance data compiled.

DHS made progress in addressing the issues identified in our June 2006 report. Specifically, increased use of HSIN within the states is reported and training delivery methods have improved; however, challenges remain. Because the department has decided to devote resources to the new HSIN Next Gen initiative, we are closing our previous report recommendations. Further, in the following sections, we identify a number of areas where DHS can improve HSIN Next Gen’s information sharing effectiveness, and we make new recommendations to address those areas.

Results of Audit

Increased HSIN Use Reported But Limited Nationwide Sharing

HSIN users indicated that their use of HSIN has increased, but this use appears to be restricted to within their respective state boundaries. Staff at six of the eight fusion centers we contacted said that HSIN use has increased over the past year, and that information sharing effectiveness through HSIN has also increased.³ For example, a Tennessee fusion center official said

³ A fusion center is a collaborative effort of two or more agencies that provides resources, expertise, and information to the center with the goal of maximizing the ability to detect, prevent, and respond to criminal and terrorist activity.

that the center uses HSIN daily, and HSIN has become crucial to the center's operations. The center successfully used HSIN to share information when tornadoes struck Tennessee in February 2008.

However, only three of the eight centers use HSIN for sharing information with federal partners; the remaining five use HSIN for sharing information mainly within their state. Additionally, only three of the eight centers reported using HSIN as their primary information sharing tool. DHS could not produce user statistics to verify whether HSIN use has increased, decreased, or remained the same.

Improved Training Delivery Methods

DHS has improved its user support and guidance since our last audit by developing internet-based training on how to use HSIN, and job aids that provide quick reference tips on how to navigate through the HSIN portals. DHS also has provided on-site, system-specific training; but stakeholders receive training only if they request it. However, many users are unaware that training is available. For example, officials at five of the eight fusion centers we contacted did not know that HSIN training was available.

During one site visit, we observed "train-the-trainer" training. The HSIN Outreach Team delivers the training, upon request, to fusion center employees who then train local law enforcement employees about HSIN. The trainers discussed why stakeholders should use HSIN, and they demonstrated the functionality of HSIN. The trainers also provided examples of how HSIN was used to track activities and provide situational awareness during catastrophic events.

However, the training did not include teaching stakeholders what type of information should be entered into HSIN, nor did it provide specific scenarios illustrating when and how the stakeholders should use HSIN. A former HSIN program manager said that the absence of a clear HSIN mission and vision, coupled with the lack of a complete concept of operations and data flow model, impeded DHS' ability to create scenario-based training to help users understand how to perform their information sharing duties.

Stakeholder Involvement and Communications Challenges

DHS does not have a sufficient understanding of HSIN's communities of interest (COI), which include law enforcement

agencies, emergency management and first responder agencies, intelligence agencies, private sector infrastructure stakeholders, DHS components, and international partners. As of October 2007, there were over 700 COIs, of which only approximately 300 were actively used. According to HSIN Outreach Team members, there is no documented definition of HSIN COIs and, in the past, if HSIN users wanted to develop a COI, they simply did so.

The Outreach Team, which is composed of stakeholder relationship managers and trainers, was established to improve communications with HSIN stakeholders. It is responsible for interacting with stakeholders to communicate not only system-specific functionality, but also information about the HSIN program in general. Initially, the team had up to 32 members to provide program support and focused its efforts primarily on actively recruiting potential stakeholders. As the number of COIs increased, the team was realigned to focus its efforts on the existing COIs, but its resources were reduced to four or five members. One team member said that the current resource limitations have hindered the team's communication and coordination with stakeholders.

DHS has developed two additional groups, the HSIN Advisory Council (HSIN-AC) and the HSIN Mission Coordination Committee (HMCC), to increase stakeholder representation and participation. For stakeholders outside of DHS, the HSIN-AC is a key body for addressing state, local, and private sector issues. HSIN-AC was formed to assist in the development of nonfederal user requirements, and provides recommendations on the improvement of operational requirements. Its purpose is to generate recommendations for the improvement of policy, business processes, governance structures, and training programs to enhance information sharing between federal, state, local, and private sector communities. Although established in January 2006, HSIN-AC did not hold its first meeting until October 2007. According to a program official, this lag time occurred because of a lack of leadership support, lack of agreement about HSIN's goals, and the lengthy process required to select members.

The HMCC focuses on HSIN issues within DHS. The goal of HMCC is to identify and validate operational enhancements to HSIN that are critical to the successful accomplishment of the mission of DHS components and the federal external partners they represent. Although HMCC's first meeting was held in March 2007, the HMCC charter has not been ratified and a permanent

chair has not been appointed, resulting in ineffective leadership and a lack of focus.

As we reported in June 2006, DHS did not sufficiently involve stakeholders during the development of HSIN and, therefore, did not clearly understand their needs. Despite their concurrence with our previous recommendations and the existence of several bodies designed to facilitate this effort, almost 2 years later DHS has yet to adequately identify HSIN users or determine their information sharing requirements.

Information Sharing Process Not Defined

DHS has not defined and communicated its homeland security information sharing process to HSIN stakeholders. Without this guidance, HSIN users do not know what information they should share or, once provided, what DHS does with the information. None of the eight fusion centers we contacted had received any guidance about what information to enter into HSIN or what information DHS would provide to them. Individuals responsible for HSIN's planning, development, and implementation said that the lack of clearly defined business processes that serve the stakeholders has been a significant problem because users are unsure about how HSIN should be used. Stakeholders and advisory committee members we spoke with echoed the same sentiment.

Additionally, some users do not know or trust who has access to the information in HSIN. Individuals from five of the eight fusion centers we spoke with expressed concern about who can access the information they enter in HSIN. For example, users at one fusion center said that they are reluctant to share sensitive information with states that have laws that may require the release of such information in response to freedom of information requests. These concerns have perpetuated the existence of barriers to information sharing.

The DHS Office of Intelligence and Analysis (I&A) provides homeland security intelligence to the department, various components of DHS, and other partners within the intelligence community at the federal, state, local, tribal, and the private sector levels. In order to better define the process, I&A initiated a pilot project to collect information on current processes, analyze the processes for deficiencies, recommend improvements, and observe the implementation of those improvements to enhance the intelligence information exchange between I&A and the fusion

centers. I&A has also conducted an internal study of how it disseminates intelligence information. Despite these efforts, an I&A program official said that I&A has not been able to define an intelligence data flow model for HSIN, nor has DHS' information sharing process been defined and disseminated to users.

Stakeholder Dissatisfaction

Because HSIN does not address all of their needs, some stakeholders are developing alternative systems. For example, I&A, which is a primary HSIN stakeholder, has developed a separate, secure portal, the Homeland Security State and Local Intelligence Community (HS SLIC), for the state and local intelligence community. I&A officials said that HS SLIC grew from the intelligence community's lack of confidence in HSIN's ability to provide a secure, trusted environment in which they could share sensitive information. Although these stakeholders provided their requirements for additional security to the HSIN program office, the HSIN platform was unable to meet their needs. Intelligence analysts said that their business needs were solicited before the HS SLIC portal was deployed, and they have received communications on a daily basis from the I&A staff supporting the portal. They also expressed their confidence that the information they entered in HS SLIC was protected and used by DHS.

Other stakeholders are looking for alternatives to HSIN as well. Although the Florida fusion center uses HSIN as its primary method of sharing documents within the state, two of the seven regions in Florida are considering moving away from HSIN. These regions are looking for a system that will allow them to maintain more local control over their information and newer technology that may provide them with alerting capabilities and Internet messaging to groups.

Performance Measures Not Developed

DHS has not developed performance goals and measures for HSIN, and cannot readily obtain the data needed to track performance. Specifically, the system does not provide statistics for HSIN usage. During our 2006 audit, HSIN program management provided us with data on HSIN usage such as:

-
- Number of monthly HSIN logons,
 - Number of HSIN account holders per month,
 - Number of account holders who logged onto HSIN daily per month by COI,
 - Total number of HSIN users per month by COI, and
 - Number of account holders who posted documents to HSIN per month by COI.

However, when we requested the same information during this audit, the department was not able to provide it. A DHS operations official said that the HSIN program office does not, at present, have the capability to report data readily at this level of detail. Although a former manager said that obtaining such data is possible, it must be collected through a laborious manual process.

Further, DHS cannot track other important program performance information. For instance, there are no automated mechanisms to track information sharing statistics that would reveal how often posted documents are shared and with whom. HSIN program officials believe that this type of information, if available, would provide tangible evidence to support the effectiveness of HSIN's role in information sharing.

Obtaining such information is difficult because system performance and information sharing tracking capabilities were not built into HSIN. Without performance goals and measures, DHS cannot determine HSIN's effectiveness as an information sharing tool or identify issues that should be addressed to improve system performance and increase information sharing through HSIN.

Recommendations

To enable DHS to achieve its vision for HSIN Next Gen to be the homeland security community's information sharing tool of choice, we recommend that the Director, Office of Operations Coordination and Planning:

Recommendation #1: Provide sufficient resources to improve stakeholder relations, ensure adequate stakeholder involvement and communication, and meet the needs of its customers at the federal, state and local, tribal, and private industry levels.

Recommendation #2: Develop scenario-based training for stakeholders and communicate the availability of existing training.

Recommendation #3: Ensure that system performance and information sharing metrics are included in any and all future HSIN developments.

We also recommend that the Under Secretary for the Office of Intelligence & Analysis:

Recommendation #4: Define and communicate DHS' information sharing process to ensure that users understand what information to share and what DHS does with the information.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Director of Operations Coordination and Planning and the Under Secretary for Intelligence and Analysis. We have included a copy of the comments in their entirety at Appendix B.

In the comments, the Director of Operations Coordination and Planning and the Under Secretary for Intelligence and Analysis expressed appreciation that we acknowledged progress made and closed the recommendations from our June 2006. They also acknowledged the need for improved stakeholder relations and procedures for defining the information sharing process.

In response to recommendation 1, the Director of Operations Coordination and Planning concurred with our recommendation and stated that resource shortfalls will be augmented through “over-guidance” provisions in their fiscal year 2010 budget submission to the Congress. These provisions request funding specifically to support increasing staffing levels dedicated to building and strengthening stakeholder relationships with DHS’ information sharing partners in the federal, state, local, and private sectors. Additionally, the Director stated that as evidence of their plans to improve stakeholder relations, involvement, and communication opportunities, their Outreach Team’s strategic plan would be revised to provide goals for increased awareness and collaboration. These goals specify improved awareness of HSIN mission and capabilities, by mission areas, at all levels; establishment of mission models; and increased internal collaboration within DHS components as well as collaboration with external information sharing partners.

In response to recommendation 2, the Director of Operations Coordination and Planning stated that HSIN’s current training engagement model provides for the delivery of mission-based training. Training is delivered in five different methods; and, at least three of those methods allow HSIN mission advocates to tailor training to meet the needs of the specific stakeholder community for which the training is being delivered. In addition to training provided to individual communities of interest, the HSIN program manager is also developing a strategy for providing training that transcends mission areas and highlights HSIN as a transparent information sharing tool. The response also introduces plans for making HSIN training availability more visible to the stakeholder communities.

In response to recommendation 3, the Director of Operations Coordination and Planning further acknowledged the need for an automated means of measuring HSIN system performance and information sharing activities, and that information sharing data, in particular, is not currently being measured. However, the Director related that the future version of HSIN, the HSIN Next-Generation platform, will provide for enhanced information sharing capabilities, and an automated means of gathering mission-critical data. Specifically, HSIN Next-Generation's functional requirements document targets the collection of statistics such as data specific to the performance of HSIN, as well as what information is shared, how and with whom the information is shared, and the nature or content of information being shared.

Finally, to address recommendation 4, the Under Secretary for Intelligence and Analysis reiterated their commitment to information sharing that is "functionally-oriented." Therefore, the Under Secretary proposed the creation of shared mission communities which would serve to help define policies, workflows, and data standards for information sharing. The Under Secretary envisions the establishment of shared mission communities as a means of further defining an information sharing process for the department that includes and addresses the unique needs and concerns of each community of stakeholders; thereby establishing trust in the overall information sharing process.

We began our followup audit work by reviewing the five open recommendations from our June 2006 report, *Homeland Security Information Network Could Support Information Sharing More Effectively* (OIG-06-38). Additionally, we reviewed followup documentation provided by the HSIN program office and the program office's 90-day responses to the first audit. Furthermore, our background research included reviews of reports issued since the last audit related to HSIN prepared by the OIG, Government Accountability Office, other federal agencies, public interest groups, and the Congress. We also reviewed records of congressional testimony that occurred since the issuance of the first report.

To obtain information on the current status of information sharing and to identify challenges to HSIN's use and implementation, we obtained internal DHS correspondence that established policies and procedures relative to HSIN and future information sharing initiatives. We also researched the department's internal website to obtain relevant information about HSIN since the last audit. Due to the high visibility of the HSIN program, we researched media articles that pertained to HSIN specifically and information sharing in general. We also researched legislation that established the nation's information sharing environment and imposed additional business and technical requirements on the HSIN program.

We conducted our audit fieldwork from November 2007 to March 2008 at HSIN Program Office headquarters in Washington, D.C. We met with key department officials responsible for HSIN's planning, implementation, and program management to obtain information on the progress made toward addressing previous recommendations, assess the current status of information sharing among select HSIN stakeholders, and identify new challenges to HSIN's use and implementation. These officials included members of DHS' Office of Operations Coordination, the Office of Intelligence and Analysis, and the Office of the Chief Information Officer. Additionally, we met with members of stakeholder working groups and advisory boards; specifically the HSIN-AC and the HMCC.

We also visited stakeholders at the following select fusion centers; Santa Fe, New Mexico; Los Angeles, California; Richmond, Virginia; Sacramento, California; and Woodlawn, Maryland; and conducted telephone conferences with the Florida, Tennessee, and

Vermont Fusion Centers. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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

Appendix B
Management Comments to the Draft Report

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



**Homeland
Security**

September 15, 2008

Richard L. Skinner
Inspector General
Office of Inspector General
Department of Homeland Security

Dear Mr. Skinner,

The Office of Operations Coordination and Planning (OPS) and Office of Intelligence and Analysis (I&A) appreciate the opportunity to comment on the Department of Homeland Security (DHS) Office of Inspector General (OIG) draft report, "DHS' Efforts to Improve the Homeland Security Information Network." OPS and I&A are working together to ensure the Homeland Security Information Network (HSIN) will be able to support the Sensitive But Unclassified (SBU) information sharing and collaboration requirements for the Department. OPS and I&A are pleased that the OIG saw the progress toward addressing and bringing to closure the June 2006 report recommendations.

OPS and I&A are aware that challenges remain with supporting HSIN stakeholders and defining the information sharing processes. The HSIN Program Manager will roll out new capabilities on the HSIN Next Generation (NextGen) platform consistent with a shared segment architecture between DHS, the Department of Justice, Director for National Intelligence, and the Department of Defense, aligned with the Information Sharing Environment (ISE) Architecture Framework and the DHS Information Shared Segment Architecture. The following responses address the draft report recommendations:

Recommendation #1: Provide sufficient resources to improve stakeholder relations, ensure adequate stakeholder involvement and communication, and meet the needs of its customers at the federal, state and local, tribal, and private industry levels.

Office of Operations Coordination and Planning Response:

The Office of Operations Coordination and Planning is addressing the recommendation to establish adequate resources to support stakeholder relationships through our outreach team. The HSIN Outreach Team interacts with organizations external to the HSIN Program. The external interactions require resources and activities focused on Relationship Management, Training, Communications, and Requirements Management. In January of 2008, OPS directed the Outreach Team to revise the HSIN Outreach Strategic Plan. The revision addressed user support shortfalls. The updated plan addressed the following four goals:

Page 1 of 5

Appendix B Management Comments to the Draft Report

1. Improve national awareness of HSIN: mission, capabilities, roles, and accomplishments (by Mission Area) at the Federal, state, local, tribal, nongovernmental, and private industry levels
2. Establish HSIN as a core integrated component of regional (state, local, and private sector) partner mission models
3. Increase collaboration and communication with DHS components
4. Increase collaboration and communication with DHS partners utilizing, supporting, and/or promoting complementary missions and technology platforms.

The current HSIN Outreach Team resource levels cannot address all partner concerns related to the four major goals. As part of the budget planning process for FY10, the OPS Chief Information Officer (CIO) submitted an over-guidance request to be included in the next budget cycle for increased staffing in support of the HSIN Outreach Strategic Plan. The augmented HSIN Outreach Team will build on our diverse partner community relationships to facilitate integrating HSIN into the partner communities' day-to-day operations that map to the DHS mission (Awareness, Prevent, Protect, Respond, and Recover). These new funds will be dedicated entirely to mission integration with our partners and focused on our Federal, State, local, and private sector partners.

The OPS CIO plans to fill ten additional billets beginning in FY09, pending Departmental approval. These billets will support architecture, security, privacy, and other functions. These specialists will ensure HSIN addresses statutory and interoperability requirements with partner tools. These resources will provide more robust requirements management and process control.

As HSIN NextGen progresses, the HSIN Outreach Team will continue various outreach initiatives and build upon current and potential partners to ensure the gathering of community-wide requirements. The HSIN Outreach Team is in the initial phase of an important engagement with the Commonwealth of Virginia, among others. Working closely with operational personnel in Virginia, the Department will be able to further understand the information sharing needs of the Commonwealth and aid in supporting their homeland security mission. By engaging with additional partners in the future, the Department will be able to further examine the needs of our State, local, tribal and Federal partners. Additionally, the HSIN Advisory Committee continues to develop and refine recommendations to improve the mission integration outreach strategy.

Recommendation #2: Develop scenario-based training for stakeholders and communicate the availability of existing training.

Office of Operations Coordination and Planning Response:

HSIN Outreach Team members develop, coordinate, and deliver HSIN and Common Operational Picture (COP) training to new and existing users. Training is conducted through the following methods:

- Web-based Training (WBT)
- Pre-scheduled Webcasts
- Session-Specific Webcasts (Supported or conducted by Mission Advocates (MAs))
- Onsite Instructor-led Training (Supported or conducted by MAs)
- Exercise Training and Support (Supported or conducted by MAs)

Appendix B Management Comments to the Draft Report

The current training engagement model, as documented in the HSIN Training Plan, supports the broad spectrum of training needs while controlling program costs. The model supports the need for quick response times, training large user groups under difficult circumstances and just-in-time mission-based training (i.e. national exercises and Principal Federal Official (PFO) training sessions). New communities receive tailored training sessions lead by HSIN MAs. WBT and/or prescheduled webcasts provide existing users with refresher training. Also, the outreach plan supports training requirements that routinely arise for exercises support and real world event responses.

The HSIN MAs and other DHS subject matter experts support mission-based training. At this time, scenario-based training requires customization for each new community. The HSIN Training Team has two approaches for HSIN scenario-based training: customized training and train-the-trainer. With adequate advanced notification of training requests, the MAs work with community subject matter experts to deliver customized training. The train-the-trainer method, where identified individuals are trained on system functionality as it relates to their information sharing mission needs, is used to reach larger audiences. This individual can then train the associated Community of Interest (COI) with specific scenarios relevant to their mission needs.

As the MA staffing levels increase, the team will gain more time and real world experience allowing them to develop a scenario-based training library. Further, the HSIN Program Manager foresees that major communities will develop other scenarios as necessary. Because HSIN serves a diverse and extensive audience, there will be development of cross-domain scenarios. These cross-domain scenarios will highlight the unique capability that HSIN provides as an information sharing tool.

A communications strategy will be prepared to use multiple modes of communication to ensure that our partners are aware of these training packages. Examples of these modes include posting information on the training pages of HSIN and aggressive awareness campaigns where the MAs attend key national, regional, and local association meetings.

Recommendation #3: Ensure that system performance and information sharing metrics are included in any and all future HSIN developments.

Office of Operations Coordination and Planning Response:

There is a need for future HSIN development to include the capability to support system performance and information sharing metrics reporting. Current HSIN performance measures do not specifically address information sharing. The current HSIN platform supports limited reporting through a manually intensive process. Available HSIN performance metrics are reported through the annual OMB Exhibit 300s and quarterly FYHSP reporting.

The current HSIN system does not have an automated monitoring tool across all COIs to provide specific performance metrics. OPS previously recognized this need and included it in the HSIN NextGen Functional Requirements Document (FRD). The HSIN NextGen solution will provide automated usage reports across all COIs. HSIN NextGen will support monitoring system performance and provide a level of detail for COI owners on portals usage. The system will generate reports on these metrics for the HSIN Program Manager and COI owners. Authorized users will be able to access these configurable reports. HSIN NextGen will support formal systematic measures of usage, availability, and content reporting. The following broad categories of metrics will be collected as part of the HSIN NextGen solution:

Appendix B Management Comments to the Draft Report

- **User and usage metrics:** Characterize how the end-users are interacting with the HSIN Next Generation System.
- **System health metrics:** Describe and characterize the operational state of the HSIN Next Generation System.
- **Content metrics:** Track the subscription and access of the system's informational content.

The FRD provides more detail for each metrics area listed above. These requirements will be tracked through design and user acceptance. This automated system tracking will improve the HSIN Program Manager's ability to monitor on report on performance as it relates to the system's mission.

Recommendation #4: Define and communicate DHS' information sharing process to ensure that users understand what information to share and what DHS does with the information.

Office of Intelligence and Analysis (I&A) Response:

In the first five years of DHS's existence, information sharing within the Department and with non-DHS mission partners at any level has been met with both visible successes and failures, as well as presenting continuing challenges to overcome.

DHS is required as part of its statutory mission and Executive Branch responsibilities to facilitate information sharing. Until quite recently, information sharing processes had either not been developed or matured to a level that allowed the Department to seriously examine the feasibility of adopting a common information sharing standard for DHS. While it is still a possibility, a single standard may not be feasible nor desirable because various information sharing functions have distinct requirements that must be addressed. Furthermore, it becomes exponentially more difficult to institutionalize processes consistent with the specific interests, laws and policies of any local jurisdiction, as well as overall objective of doing so in a manner that protects the constitutional rights and privacy of the citizens of the United States of America. Many of the potential information sharing partners have their own local laws that manage, restrict or allow certain information to be shared, and how they handle much or all of the information they receive from external sources.

One example of how these challenges have been successfully managed is the Homeland Security State and Local Intelligence Community of Interest (HS SLIC). This group was formed to encourage collaboration between Federal, State and Local entities on intelligence issues. Getting non-DHS users to provide relevant information required establishing trust among participant organizations. To build this trust, a governance structure was established through the direct participation of the non-DHS partner organizations. Out of eight voting members of the community, six were non-federal partners. It was apparent that if data is to be shared amongst Federal and non-Federal entities, it must be have systems in place to ensure users know the rules of handling information and the technical capabilities of the system provide necessary security to protect information from unauthorized access and support oversight and audit requirements.

In the case of this I&A community, DHS initiated and fully encouraged the sharing of relevant information and intelligence amongst the homeland security stakeholder community. For example, DHS provides homeland intelligence reports (HIRs) and coordinates permission for

Appendix B
Management Comments to the Draft Report

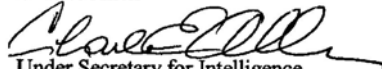
release of Federal Bureau of Investigation raw intelligence reports to cleared personnel via a single repository to HS SLIC members. The future of these collaborative exchanges is still evolving. While we have initially aimed to provide technical mechanisms that protect the information from unauthorized access, we have increased direct person-to-person collaboration between DHS (especially I&A analysts) and State and local partners. These efforts have provided extremely valuable, with several instances of this direct interaction driven actions taken by homeland security and law enforcement personnel at the State and local level.

While some functions are indeed unique, flexible information sharing models are still needed that can be replicated across the diverse homeland security missions. Elsewhere in DHS, the Information Sharing Coordinating Council, through the full support of the DHS Information Sharing Governance Board (ISGB), has begun to foster functional information sharing across DHS components and between their respective mission partners. One such approach, that is becoming institutionalized, has been to establish Shared Mission Communities (SMCs). These mission communities are organized around specific mission-related functional areas (law enforcement, intelligence, emergency management, critical infrastructure protection, border security, etc.). For example, the Law Enforcement Shared Mission Community (LE SMC) includes each of the law enforcement elements of DHS. DHS expects to establish other SMCs within the coming year. These communities have tremendous value and potential. SMCs provide a collaborative space for mission operators to bring information sharing challenges for discussion and that space is most closely related to the functions that they serve. These challenges can include information sharing policies, enhanced information sharing workflows and processes, standards on data required for system interoperability and access, among others. Appropriately institutionalizing this mechanism will support the establishment of a flexible model that can both mature and be used in other DHS and non-DHS communities as well. Not only is information sharing functionally-oriented, but cuts across other communities, enabling community interoperability.

DHS is firmly committed to information sharing, both across the Department and its missions, and amongst its non-Federal partners. DHS respects the laws and policies of these partner organizations by committing to develop a structure that will effectively protect the information from unauthorized access and unauthorized use. As this trust is earned, processes within each of these functional areas will be more broadly implemented using the "full partnership, full transparency" approach.

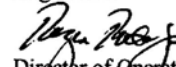
Sincerely,

Charles Allen



Under Secretary for Intelligence
and Analysis

Roger Rufe



Director of Operations Coordination
and Planning

Information Management Division

Richard Harsche, Director
Beverly H. Bush, Audit Manager
Steve Ressler, Auditor
Swati Nijhawan, Auditor
Melissa Keaster, Auditor
Kristina Hayden, Referencer

Department of Homeland Security

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

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate



ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, 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 our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.