Department of Homeland Security
Office of Inspector General

Homeland Security Information Network
Improvements and Challenges

June 13, 2013

MEMORANDUM FOR: Richard Chávez
                      Director
                      Office of Operations Coordination and Planning
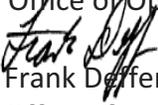
FROM: Frank Deffer
                      Office of Assistant Inspector General
                      Information Technology Audits

SUBJECT: *Homeland Security Information Network Improvements
                      and Challenges*

Attached for your information is our final report, *Homeland Security Information
Network Improvements and Challenges.* We incorporated the formal comments from
the Director, Office of Operations Coordination and Planning in the final report.

The report contains three recommendations aimed at improving the Homeland Security
Information Network. Your office concurred with all three recommendations. As
prescribed by the Department of Homeland Security Directive 077-01, Follow-Up and
Resolutions for Office of Inspector General Report Recommendations, within 90 days of
the date of this memorandum, please provide our office with a written response that
includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target
completion date for each recommendation. Also, please include responsible parties and
any other supporting documentation necessary to inform us about the current status of
the recommendation. Until your response is received and evaluated, the
recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we are providing
copies of our report to appropriate congressional committees with oversight and
appropriation responsibility over the Department of Homeland Security. We will post
the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Richard Harsche, Director,
Information Management Division, at (202) 254-5448.

Attachment

Table of Contents

Appendixes

Abbreviations

CIO	Chief Information Officer
COI	Community of Interest
DHS	Department of Homeland Security
GAO	Government Accountability Office
HSIN	Homeland Security Information Network
HSIN NextGen	Next Generation of the Homeland Security Information Network
I&A	Office of Intelligence and Analysis
IT	information technology
JRIES	Joint Regional Information Exchange System
NOC	National Operations Center
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPS	Office of Operations Coordination and Planning
SLIC	State and Local Intelligence Community

Executive Summary

The Homeland Security Information Network is a secure, unclassified Internet portal that enables information sharing and collaboration across the homeland security enterprise. In 2006 and 2008, we reported on challenges that the Department of Homeland Security (DHS) faced to define the system's role, meet user requirements, provide user support, and increase system use. We conducted a followup audit of this system to determine the progress made and the system's effectiveness in supporting information sharing among select stakeholders. Appendix A describes the present audit's scope and methodology.

Since 2008, DHS has made progress in addressing the planning and governance issues we identified. Specifically, system program management performed an analysis of alternatives, revalidated stakeholder requirements, and developed other strategies to realign the program to address system challenges and concerns. Formalized governance processes established and supported by a new policy office contributed to these accomplishments. These efforts allowed the program to meet Office of Management and Budget requirements for program improvement, as well as acquisition review gateway criteria for the development of a new system release.

Still, system program management has faced challenges implementing the new system release on schedule. Migration from the legacy system to the new platform has been delayed because of contracting and technical challenges. As a result, there is increased risk that schedule delays will lead to additional costs. Further, delays have caused some user communities to pursue other solutions for their information sharing needs.

Although certain communities were using the system to share information successfully, the system was not routinely or widely used to share information throughout the homeland security enterprise. Specifically, the number of system account holders remained limited, and the extent to which those account holders were using the system was also constrained because of challenges with system content and performance. As a result, the system had not fully met its objective to support effective information sharing among homeland security partners.

We are recommending that the Director of Operations Coordination and Planning develop a plan to increase DHS components' adoption of the system, address current system performance issues through the planned system upgrade, and develop a plan to improve communication and collaboration with State and local stakeholders to expand exposure to HSIN and the capabilities that the system can provide. The Director concurred with the report recommendations.

Background

The Homeland Security Act of 2002 assigned DHS responsibility to coordinate the Federal Government's homeland security communications with State and local government authorities, the private sector, and the public.[1] In support of this responsibility, the Department developed and continues to manage the Homeland Security Information Network (HSIN), a secure, unclassified Internet portal that enables these various stakeholders to collaborate and share homeland security information.

The HSIN mission is to provide homeland security stakeholders with effective and efficient collaboration tools for decision making, secure access to data, and accurate, timely information sharing and situational awareness. To achieve this mission, HSIN provides a shared place for users to collaborate securely with features such as Connect (a Web conference tool) and Jabber (a chat tool). In addition, HSIN provides a document library for the distribution of homeland security reports and information. As the designated information sharing portal for DHS, HSIN also serves as the principal platform for interoperability with other DHS information sharing portals or for consolidation of such portals.

HSIN is organized into information sharing groups called Communities of Interest (COIs). There were more than 1,300 COIs supporting homeland security missions; State, Federal agency, and private sectors; and task force, event, or incident needs. HSIN users belong to and share information with the COIs that pertain to their particular mission needs, including several nationwide COIs that are intended to support core aspects of the homeland security mission, such as:

- HSIN Critical Sectors – Used by private sector, State and local governments, and Federal stakeholders to support coordination and collaboration across all 18 critical infrastructure and key resource sectors.

- HSIN Emergency Management – Used by emergency and incident management experts nationwide from all levels of government to respond to both manmade and natural disasters.

- HSIN Federal Operations – Used by the DHS National Operations Center (NOC) and other Federal agencies for situational awareness and event response. The NOC uses this community to provide a variety of written deliverables, including analysis of ongoing situations, threat analysis, and more.

---

[1] *Homeland Security Act of 2002,* Public Law 107-296.

- HSIN Law Enforcement – Used by Federal, State, local, and tribal law enforcement agencies to coordinate and implement information-driven and risk-based prevention, protection, response, and recovery efforts with respect to all threats and all hazards during both routine and emergent operations.

- HSIN State and Local Intelligence Community (SLIC) – Used by intelligence officers and analysts from the Law Enforcement, Homeland Security, and Intelligence Communities to meet, avert, or respond to current, emerging, and future threats related to homeland security.

HSIN is the only Federal portal that provides information sharing among DHS and its Federal, State, local, territorial, tribal, international, and private sector partners across the full spectrum of the homeland security mission. It allows these diverse communities to work together to perform investigations, identify terrorist activities, respond to areas affected by natural disasters, and provide coordination during recovery operations.

HSIN History

HSIN has evolved significantly since it was initially developed nearly a decade ago. It began as a Defense Intelligence Agency–sponsored initiative called the Joint Regional Information Exchange System (JRIES). JRIES was designed 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. The Defense Intelligence Agency transferred JRIES to DHS in September 2003 because the domestic nature of the program fit better under the newly formed DHS.

Under DHS, program management sought to expand the scope of the system. In February 2004, the DHS Secretary renamed JRIES as HSIN in order to reflect this broader scope, and designated HSIN as the Department's secure, unclassified sharing and collaboration platform. Further, in January 2006, the DHS Secretary designated HSIN the primary system for operational information sharing and collaboration with the Department and with its homeland security partners, and required all components to use HSIN.

In June 2006, we reported that DHS had not defined HSIN's relationship to existing systems, obtained and addressed user requirements, provided adequate user guidance, or developed performance measures for HSIN.[2] These system planning and

---

[2] *Homeland Security Information Network Could Support Information Sharing More Effectively*, OIG-06-38, June 2006.

implementation issues limited HSIN's ability to support State and local information sharing.

In February 2008, HSIN management announced that it planned to upgrade the HSIN platform. This upgrade, referred to as the Next Generation of HSIN (HSIN NextGen), included plans to change software platforms, enhance security, add capabilities, and provide a new look and feel for users. HSIN NextGen was initially scheduled to be completed by September 2009. The upgrade, however, did not meet deployment timelines and performance expectations.

In October 2008, we reported that DHS continued to face challenges defining user requirements, defining the information sharing process, and providing adequate user support.[3] In addition, nationwide information sharing using HSIN remained limited, and performance measures to track or assess information sharing using HSIN had not been developed.

In May 2010, the Office of Management and Budget (OMB) designated the HSIN program as high-risk, halted all system development, and conducted a review to determine whether the program would continue to receive Federal funding. At the conclusion of the review, OMB determined that HSIN was a viable program, but OMB established conditions relating to system user growth, portal consolidation, and interoperability targets that the HSIN program needed to meet going forward.

In July 2010, the DHS Office of Operations Coordination and Planning (OPS) and the DHS Office of the Chief Information Officer (OCIO) signed a memorandum of agreement that transferred operational control of the HSIN program to the DHS OCIO while OPS maintained administrative control. The DHS OCIO initiated a series of program assessments to identify the right approach for upgrading the HSIN platform to meet the needs of the Department and its mission partners. This analysis concluded that the best approach was not HSIN NextGen, which involved transitioning to an entirely new software platform. Rather, the analysis concluded that upgrading the legacy HSIN platform based on Microsoft SharePoint software with augmented security was the best path forward. This approach was called HSIN Release 3. The NextGen approach was decommissioned in July 2011, and HSIN Release 3 development began in October 2011. The transition to HSIN Release 3 was scheduled to be completed by May 2013. Figure 1 provides a timeline of HSIN's evolution and major events since its transfer to DHS.

---

[3] *DHS' Efforts to Improve the Homeland Security Information Network*, OIG-09-07, October 2008.

Sep 2003
JRIES transferred from the Defense Intelligence Agency to DHS

Jan 2006
DHS Secretary required all components to use HSIN

Feb 2008
Plan for HSIN NextGen announced

Oct 2008
OIG identified continued challenges with user requirements, guidance, and limited use

July 2010
HSIN moved from OPS to DHS OCIO

Oct 2011
HSIN Release 3 development begins

May 2013
HSIN Release 3 Migration completion target

Feb 2004
JRIES renamed HSIN and designated as the DHS Sensitive but Unclassified portal

June 2006
OIG identified challenges defining HSIN's role, meeting user requirements, providing guidance, and limited system use

May 2010
OMB halts spending on HSIN

July 2011
HSIN NextGen decommissioned

Figure 1. HSIN Timeline

Results of Audit

HSIN Planning and Governance Progress

HSIN program management has made progress in addressing the planning and governance issues we identified in 2008. Management performed an analysis of alternatives, revalidated stakeholder requirements, and developed other strategies to realign the HSIN program to address system challenges and concerns. In addition, program management completed key planning documents such as the Concept of Operations, Business Case, and Segment Architecture to guide and define the new direction for HSIN. Formalized governance processes and increased high-level support and staffing following the HSIN program transfer to the DHS OCIO in July 2010 contributed to these accomplishments. As a result, the HSIN program met OMB requirements for program improvement, as well as acquisition review gateway criteria for HSIN Release 3 development.

Plans and Strategies Revised

HSIN program management revised its plans and strategies to better meet program goals. Federal law and departmental guidance require effective planning to ensure the success of information technology (IT) development

efforts.[4] To meet planning requirements, program personnel analyzed alternative technical solutions to identify the best approach for an upgrade to the HSIN platform. The analysis compared the HSIN NextGen platform, the legacy HSIN platform, and the platform that hosted the Homeland Security SLIC.[5] The analysis indicated that the legacy HSIN platform with upgraded software and enhanced security would be the best alternative because it met the highest percentage of user requirements with the least complicated migration path, and had lower life cycle and administrative costs. The HSIN Release 3 approach, as it was named, was presented to and received support from homeland security mission leadership across the Department and was approved by the DHS Chief Information Officer (CIO) in October 2010.

HSIN program management conducted numerous other planning activities to redirect the program and support the HSIN Release 3 approach. Specifically, HSIN program personnel worked with stakeholders to revalidate system requirements. This initiative defined core requirements for migration to HSIN Release 3. HSIN program personnel also conducted a technical assessment to determine the feasibility of updating the platform to Microsoft SharePoint 2010, reusing existing hardware and software, implementing enhanced user security features, and establishing the implementation timeline. Further, HSIN program personnel developed a knowledge management strategy to improve information sharing across COIs within HSIN Release 3 to avoid information sharing stovepipes that had been a challenge. Program personnel summarized these activities in an overall HSIN Improvement Plan.

HSIN Release 3 Development Planning Activities Completed

HSIN program personnel completed additional planning activities and documents to support the HSIN Release 3 development process. Specifically, HSIN program personnel completed a business case in January 2011 that provided justification for the new direction of HSIN, an analysis of the current and proposed future states of HSIN, and the HSIN master schedule and development approach. HSIN program personnel also completed a combined Mission Needs Statement/Operational Requirements Document/Concept of Operations in May 2012. This document defined the major use scenarios for HSIN, identified the major capability gaps that hindered the system's effectiveness, and defined how

---

[4] Public Law No. 104-106, Division E, February 10, 1996. The law, initially titled the *Information Technology Management Reform Act of 1996*, was subsequently renamed the *Clinger-Cohen Act of 1996* in P. L. 104-208, September 30, 1996. DHS AD 102-01, Interim Version 2.0, *Acquisition Directive*, Instruction Appendix B, September 21, 2010.

[5] The Homeland Security SLIC was managed by DHS Office of Intelligence and Analysis (I&A) and hosted independently from HSIN on a separate platform. It has since migrated to HSIN and become HSIN SLIC.

HSIN Release 3 would resolve these gaps once fully implemented. For example, this document identified six capability gaps that HSIN Release 3 would address, including the ability to improve search and retrieval of content using standardized content tagging terms.

In addition, the DHS OCIO completed the DHS Sensitive but Unclassified Portal Interoperability Segment Architecture and Transition Plan in January 2011. This architecture provided the basis for consolidating DHS component portals onto HSIN. In addition, this architecture established the basis for interoperability with other Federal Sensitive but Unclassified portals such as the Department of Justice's Regional Information Sharing Systems Network, the Federal Bureau of Investigation's Law Enforcement Online, and the Director of National Intelligence's Intelink-U system.

HSIN program personnel also completed an acquisition plan for HSIN Release 3 in July 2012. The plan described the new agile development approach and methodologies to be used for HSIN Release 3.[6] The plan also described how the program would tailor its agile approach to meet DHS system life-cycle requirements. This approach was intended to avoid the type of schedule overruns that hindered the HSIN NextGen initiative. The plan identified major milestones and target dates for the acquisition process.

Governance Processes Established

HSIN program management established several entities to provide formal governance processes for system development and operations. The primary entity for HSIN governance is the Executive Steering Committee. The mission of the committee is to provide effective oversight and guidance to the HSIN program. The committee is led by high-level officials with the Director of OPS and the Principal Deputy Undersecretary for the Office of Intelligence and Analysis (I&A) serving as co-chairs, and the DHS CIO serving as a voting member. It meets every month, at a minimum, to discuss the cost, schedule, and performance of the program. It also reports to Department-level information sharing governance bodies such as the Information Sharing Coordinating Council and the Information Sharing and Safeguarding Governance Board.

In addition, HSIN program management established the HSIN User Working Group to manage stakeholder requirements better. Begun in April 2011, the group was composed of more than 200 core HSIN users from multiple

---

[6] Agile development is a group of software development methods based on an iterative and incremental approach. It promotes adaptive planning, and encourages rapid and flexible response to change.

stakeholder communities. Members participated in monthly meetings to guide development and implementation of HSIN. The group played a critical role in advising program management of the feasibility and potential of system upgrades and soliciting user comments. At a high level, the group has ensured that the HSIN program has collaborated with stakeholders and system experts to develop and validate the upgraded information sharing platform to meet users' needs.

Additional governance entities have played a role in HSIN development but have been in transition. The HSIN program management created the Mission Operators Committee in 2009 to ensure that DHS components could provide input into HSIN policy and to prioritize and review requirements. However, HSIN leadership determined that it would be more effective to dissolve the Mission Operators Committee and add key members of the committee to the Executive Steering Committee. In addition, the HSIN program management created the HSIN Advisory Committee in 2007 to provide independent advice from non-Federal stakeholder groups. The HSIN Advisory Committee, however, has been inactive for more than a year and a half since the Secretary initiated a Department-wide review of all Federal advisory committees. This governance body, which ensures that non-Federal partners have a voice in HSIN development and operations, will be reactivated upon completion of the review. Figure 2 lists the major HSIN governance entities.

HSIN Governance Entities	
The Information Sharing Governance Board	Provides a forum for senior DHS leaders to ensure consistent information-sharing
The Information Sharing Coordinating Council	The coordination body for the Information Sharing Governance Board to address State and Local Fusion Center issues on behalf of the Department
The Executive Steering Committee	Provides oversight and guidance to the HSIN program and informs development and management best practices
The HSIN Advisory Committee	Provides independent advice from non-Federal stakeholder groups
The HSIN User Working Group	A multi-stakeholder group that will guide development and implementation of HSIN R3 with over 200 members that participate in monthly meetings

Figure 2. HSIN Governance Entities

To support these governance processes further, HSIN program management established the HSIN Policy Office in January 2012 to ensure transparency and

accountability. The mission of the HSIN Policy Office is to ensure that the HSIN program obtains the trust of its stakeholders and governance bodies through the development of effective HSIN policy. The office has developed extensive user policies, ensured program compliance with privacy and paperwork reduction laws, and updated policies associated with HSIN governance bodies. It also defined the decision processes for the bodies governing HSIN to ensure consistent and effective management.

Department-Level Leadership and Increased Staffing

HSIN program management was able to reorient a high-risk program and develop a strategy and plans for HSIN Release 3 implementation in part because of the HSIN program realignment from DHS OPS to the DHS OCIO. The DHS OCIO was better positioned than DHS OPS to integrate information sharing, interoperability, portal consolidation, enterprise architecture, and knowledge management into the overall HSIN strategy. The move also demonstrated DHS' commitment to the program and its future. In addition, the DHS OCIO and OPS increased HSIN program staffing levels following the management shift. In 2010, when the DHS OCIO assumed HSIN management responsibility, five full-time government employees supported the HSIN program. By 2012, the number of staff had increased to 23.

Program Oversight Requirements Met

As a result of the formal planning and governance processes, the HSIN program has met OMB program oversight requirements. Specifically, OMB concluded in November 2010 that HSIN was a viable government program that should continue. HSIN program personnel were also making considerable progress with the implementation of the HSIN OMB improvement plan. Specifically, program management had completed five of eight conditions and demonstrated progress on the remaining three.

The HSIN program has also met departmental acquisition oversight requirements timely. In August 2012, the HSIN program received approval from the DHS Investment Review Board for the first two phases of the system engineering life-cycle process: the solution engineering and planning phases. Further, the Under Secretary for Management granted provisional approval for the next major program review and delegated the review process to the HSIN Executive Steering Committee because of the program's success in the first reviews.

HSIN Release 3 Schedule Challenges

DHS has faced numerous challenges implementing HSIN Release 3 on schedule. Specifically, migration from the legacy HSIN system to the new HSIN Release 3 platform has been delayed because of contracting and technical obstacles. As a result, there is increased risk that schedule delays will lead to additional costs to maintain the legacy HSIN past the contract expiration in May 2013. Further, user frustration with delays has caused some user communities to pursue other solutions for their information sharing needs.

User Migration Delay

Migration to the HSIN Release 3 platform was planned in four waves. During each wave, a distinct group of COIs and users were to be migrated to HSIN Release 3. Migration of the first wave of users was scheduled to begin in August 2012 but actually began in November 2012, after a 4-month delay. Consequently, the migration schedule for the remaining three waves has been compressed in order to meet the May 2013 completion deadline, when the contract for the legacy HSIN environment expires and the system will no longer be supported. The migration that was planned over a 9-month period must now be completed in just 5 months. As of January 2013, Wave 1 was considered completed, but it had been scaled back to include only 8 COIs instead of the 15 originally included, and only 50 users instead of 300. Figure 3 shows the planned and revised migration schedule.
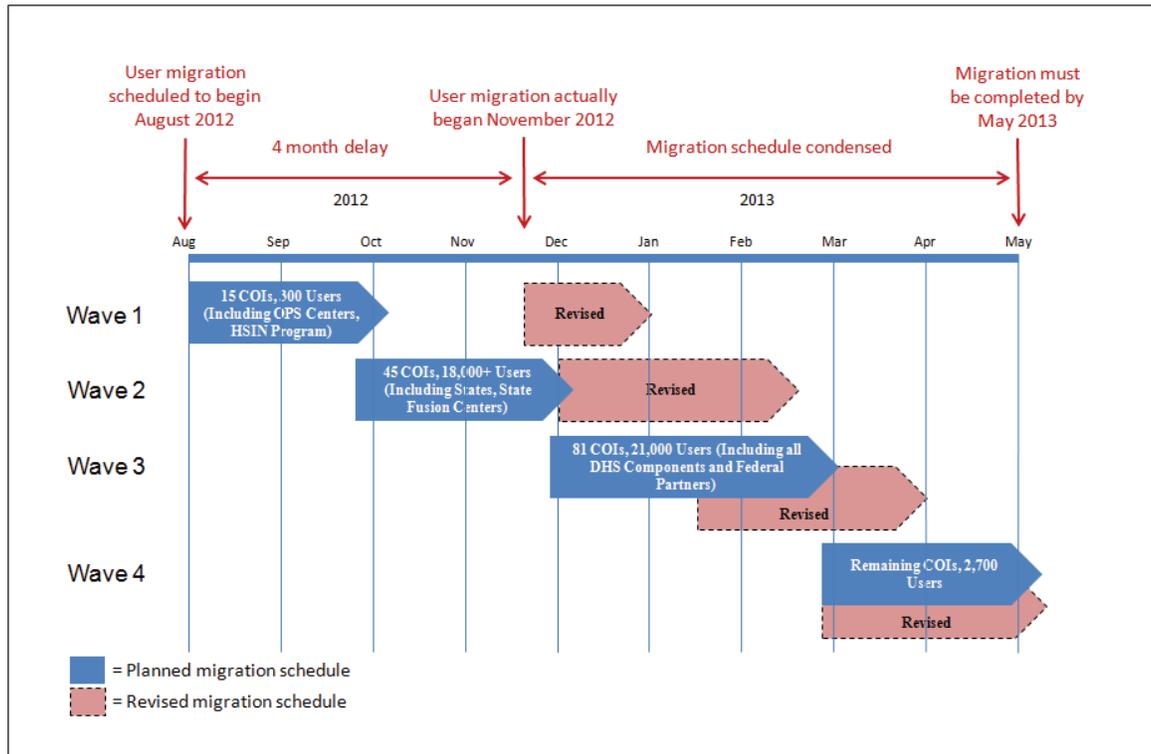
Figure 3. Delay in HSIN Release 3 Migration Schedule

Data Center and Technical Obstacles to Migration

HSIN Release 3 migration was behind schedule in part because of delays establishing the environments for system implementation at the DHS Data Center 2, located in Clarksville, Virginia.[7] Specifically, the award of the contract for establishing the environments needed to develop, test, and put the HSIN Release 3 system into production was delayed by 4 months. For the DHS data center to support HSIN Release 3, a new provision had to be added to the data center contract to address the unique software and security requirements of the system, which took time to work through. This delay reduced the time available to prepare these environments for system development activities from 6 months to just 2 months.

Once the contract was awarded, configuration of the environments took longer than anticipated because of technical issues. A contract was awarded for system development activities required for HSIN Release 3, including setting up the Identity and Access Management solution. The Identity and Access

---

[7] An environment is an operating system, program, or integrated suite of programs that provides all the facilities necessary for a particular application.

Management tool was intended to improve the security of HSIN by requiring identity verification when new users register and two-factor authentication for logging onto the system.[8] Implementing the Identity and Access Management solution, however, was more technically complex than initially anticipated. The initial contract was awarded with the assumption that the Sun Microsystems' Identity and Access Management solution would be used. However, program management had to switch to using the Oracle Identity and Access Management solution after Oracle acquired Sun.[9]

The change to the Oracle solution caused unforeseen technical complications with integration between SharePoint and Oracle. Additional integration development was required, including a small amount of custom development to capture initial registration information in a user-friendly manner. In addition, the contractor had difficulty obtaining personnel with the skills required for the Oracle solution.

As a result of these technical challenges, the production environment was not completed until July 2012, only a month before migration was initially scheduled to begin. The time needed for system testing then pushed back the user migration schedule. Program personnel had planned to perform user acceptance testing during the development process. The environments needed for system testing, however, were not complete until after the initial development work was done. Program management did not consider HSIN Release 3 ready for user migration until November 2012, almost 4 months later than planned.

Impact of Delayed Implementation

As a result of HSIN Release 3 delays, there is increased risk that migration will not be completed by the May 2013 deadline to shut down the HSIN legacy environment. HSIN program management indicated that they may be able to extend the contract to maintain the HSIN legacy environment for 1 month without incurring additional costs. After that time, the program will incur additional operations and maintenance costs estimated at $480,000 per month.

Furthermore, delayed implementation of HSIN Release 3 has led some user communities to pursue other solutions for their information sharing needs. HSIN users have been promised a more secure and intuitive HSIN solution since

---

[8] Two-factor authentication requires the user to enter a user name and password as the first step for logging on and to receive and enter a soft token as the second step.
[9] Sun Microsystems was acquired by Oracle Corporation in January 2010.

February 2008, when HSIN NextGen was first proposed. Therefore, significant pressure remains on the program to deliver a solution that meets user expectations timely. One State has used DHS grant funds to build its own SharePoint site in anticipation that HSIN Release 3 will not deliver information sharing capabilities timely.

System Use

Although certain COIs within HSIN have used the system to share information successfully, HSIN is still not routinely or widely used to share information across the homeland security enterprise. Specifically, State-level COIs have been successful for some States where HSIN outreach personnel have effectively promoted system use. In addition, some nationwide COIs, including HSIN Critical Sectors and HSIN Emergency Management, have developed a modest size user base. As a result, these COIs have demonstrated how HSIN can support information sharing within their communities. However, HSIN is not routinely or widely used to share information across the homeland security enterprise. Despite areas of success, system use overall remains limited because of numerous challenges with system content and performance. As a result, HSIN has not fully met its mission of supporting information sharing across the homeland security enterprise, despite a significant investment in the system over the past decade.

State-Level Communities of Interest

HSIN has been used effectively by some States that have set up a State-level COI. All 50 States, as well as the District of Columbia, the Virgin Islands, Puerto Rico, and Guam, have HSIN COIs. Some States have developed robust State-level communities with a defined role in information sharing within that State. For example, Louisiana has several State-level portals with an estimated 1,000 user accounts. Oregon has an estimated 1,200 account holders, with more than 800 accounts within its State law enforcement portal. Georgia has more than 1,200 users on its State HSIN communities, with approximately 700 private sector users.

Not all States, however, have developed robust State-level communities on HSIN. The HSIN program did not track the number of account holders for each State COI, so the extent of State-level COI use on HSIN could not be accurately quantified. The HSIN program periodically reported on the combined number of State, local, and tribal users, as well as HSIN SLIC users. As of the end of May 2012, there were approximately 9,600 active State, local, and tribal users, including an estimated 2,200 HSIN SLIC users.

States in which HSIN provided the most value were often those served by an HSIN mission advocate who effectively promoted system use. HSIN mission advocates were deployed to regions throughout the country to work with stakeholders to expand their knowledge of the system and adapt HSIN to meet their specific needs. Personnel we met with from the States that had robust HSIN State-level portals credited the mission advocate they worked with for their success. For example, personnel from one State said that prior to the involvement of a mission advocate, HSIN was used in a limited way as a document repository. Subsequently, personnel from this State have worked with their mission advocate to integrate HSIN into their business processes, including the processes for managing special events and working with the State's terrorism liaison officers.

States that have implemented robust State-level HSIN communities have demonstrated how HSIN can effectively support information sharing. For example, in the Gulf Coast, HSIN was used for the lead-up and response to Hurricane Isaac in 2012. During this event, HSIN tools such as Connect and Jabber were used to communicate with and train emergency responders. HSIN was also used to provide timely information to local hospitals, fire departments, and law enforcement agencies.

In addition, the Georgia Information Sharing and Analysis Center used HSIN as a platform for a new tracking system, known as i-Track, for information on criminal leads. The i-Track system is housed within the Georgia law enforcement COI on HSIN, which allows it to function as a secure, Web-based solution accessible via any computer or smart phone with an Internet connection. Using HSIN for i-Track provided the ability to quickly add new users and to allow multiple people to view and update leads at the same time.

Critical Sectors and Emergency Management Communities of Interest

Certain nationwide COIs were being used to share information with a moderate number of system users. For example, HSIN Critical Sectors was the largest nationwide COI, with 13,300 users as of November 2012.[10] HSIN Emergency Management was the second largest nationwide COI, with 11,200 active users as of November 2012.

---

[10] The November 2012 total user number did not exclude inactive users. A May 2012 HSIN program report indicated approximately 14,000 total HSIN Critical Sector users; however, about 25 percent of these accounts were inactive.

These COIs achieved a moderate size because their COI leadership had taken steps to build user content and leverage collaborative tools such as Connect. For example, in fiscal year 2012 HSIN Critical Sectors hosted 1,408 Web conferences using Connect, with a total of 29,000 participants. HSIN Critical Sectors also reported approximately 550,000 page views in September 2012. In addition, during Hurricane Sandy, HSIN Emergency Management enabled multiple jurisdictions with incompatible emergency management systems to communicate with each other during the disaster response.

Incident Response and Special Events

HSIN has also been used effectively for large-scale and cross-State special events. For example, in 2010, the United States Coast Guard deployed HSIN as the main system for unclassified information sharing for thousands of personnel during the response to the Deepwater Horizon oil spill. HSIN provided response personnel from across the country access to daily briefings, reports, alerts, message board postings, and more.

Additionally, HSIN served as the primary intelligence threat and security information exchange system during the United States Olympic track and field trials in Eugene, Oregon, from June 21 through July 1, 2012. The trials featured more than 1,000 elite athletes and thousands of staff, media, spectators, and supporters. Users at the Federal, State, and local-level used HSIN to share information and communicate during the trials. HSIN was used for the twice-daily briefings, monitoring and manipulation of security cameras, and intelligence log maintenance. Agencies also employed HSIN to exchange safety plans, credentialing guidelines, traffic control plans, and emergency response plans.

Limited Overall System Use

Despite success within certain communities, HSIN has not been used to share information widely across the homeland security enterprise. Specifically, the number of HSIN account holders remained limited, and the extent to which those account holders were actively using the system was also limited. As of the end of October 2012, HSIN had 35,560 active account holders nationwide.[11] Although system planning documents identify the potential for HSIN to grow to more than 300,000 users in the long term, system growth since 2007 has been modest, from 25,511 accounts in 2007 to 35,560 accounts in 2012. In 2006,

---

[11] Active account holders are defined as having logged onto the system at least once over the period of a year.

HSIN program management identified a metric of increasing user accounts by 5,000 accounts annually, with a goal of reaching 55,000 accounts by fiscal year 2012. This goal has not been achieved. Further, OMB required HSIN to reach 130,000 active users by 2015. To achieve this goal would require an unprecedented growth rate over the next 3 years. Figure 4 shows the number of accounts from 2007 to 2012 and OMB's growth target for 2015.
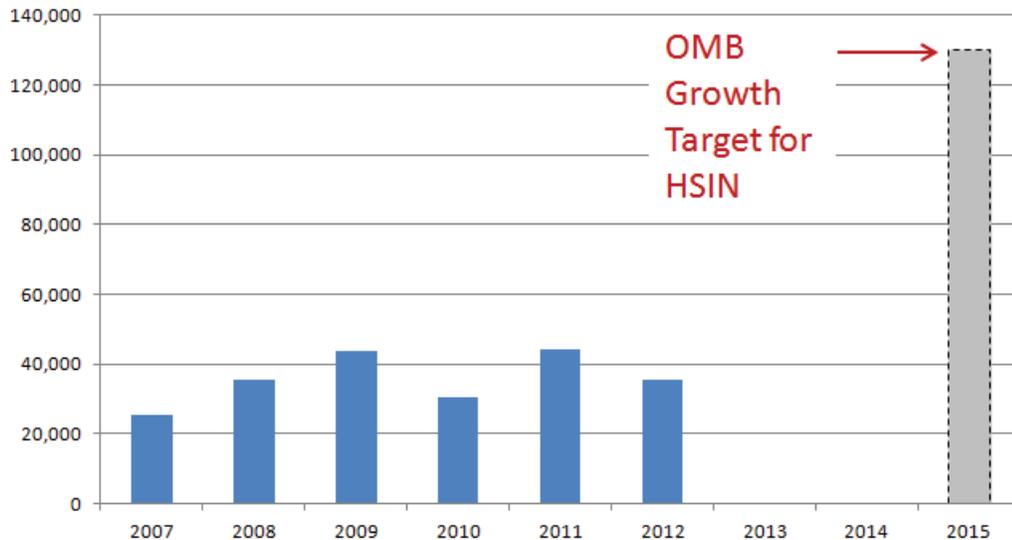

Figure 4. Total HSIN Accounts from 2007 to 2012 and OMB 2015 Target

It has also been a challenge for HSIN to maintain active account holders. In February 2010, HSIN program personnel disabled all accounts that had been inactive for more than a year as part of a user cleanup initiative to enhance system security and cost effectiveness. As a result, the number of HSIN accounts dropped from 44,846 to 19,150, a loss of 25,696 accounts, which amounted to 57 percent of all accounts. In May 2012, HSIN program personnel began to regularly track account activity and found that only 34,225 of the 45,489 accounts were active.

Further, the level of use of HSIN as measured by how often account holders logged onto the system was low. Figure 5 shows logon rates of 4 percent daily, 12 percent weekly, 28 percent monthly, and 49 percent over a 90-day period. Conversely, more than half of HSIN account holders did not log on to HSIN over a 90-day period.
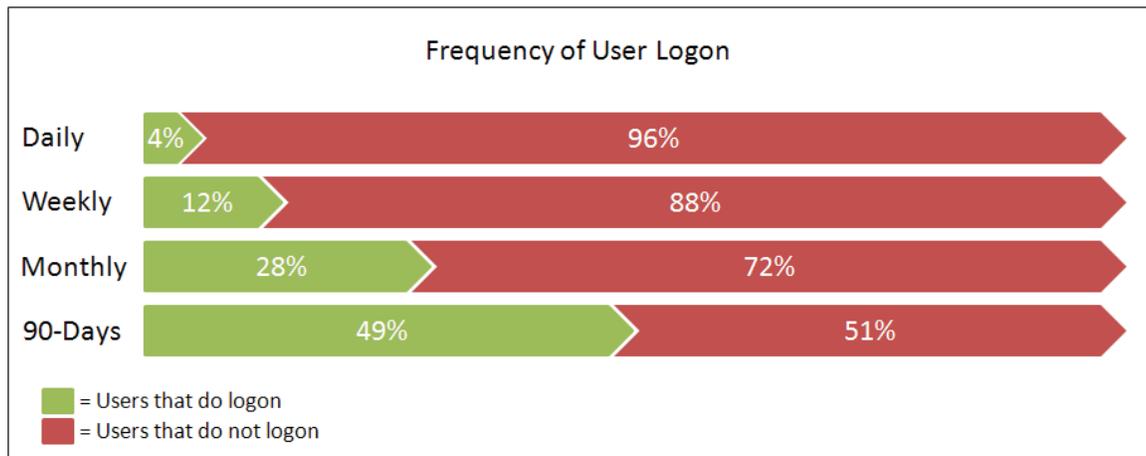
Figure 5. Frequency of User Logon[12]

System Content

According to State and local personnel we interviewed, HSIN use remained limited in part because the system content was not useful.[13] Specifically, several State and local HSIN users said that HSIN did not provide sufficient access to information from DHS components such as the Transportation Security Administration, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement. Although the NOC posted some component information to HSIN in summary documents, DHS component use of HSIN was limited. State and local personnel said that access to DHS component databases and intelligence reports would make HSIN uniquely valuable. Several State and local personnel said that they did not see a reason to use HSIN if DHS was not actively using and contributing to the system.

To improve DHS component buy-in and use of HSIN, program management has sought to identify other information sharing portals owned and operated by DHS components that could be moved onto HSIN. Seven DHS component portals have already been moved onto HSIN, and another 10 have been identified for future consolidation. For example, the National Protection and Programs Directorate moved three of its portals onto HSIN, including its Fire Services portal with 3,700 users. Several portals targeted for future consolidation have a large number of users, such as the Coast Guard HomePort portal with

---

[12] Daily, weekly, and monthly logon frequency is based on the average from January 2012 to the end of October 2012. The 90-day logon frequency is based on the average from May 2012, when the HSIN program started tracking this information, to the end of October 2012.
[13] The HSIN program is responsible for the system platform; however, each COI is responsible for the content available to system users.

approximately 25,000 users. The portal consolidation plan identifies approximately 63,000 DHS users that would be added to HSIN when the consolidation is completed.

In addition, personnel rely on systems other than HSIN to obtain information. There were numerous other information sharing systems that State and local users were more accustomed to, or found easier to use to obtain law enforcement, critical infrastructure, and emergency management information. For example, in 2006 we reported that the relationship of HSIN to existing Federal law enforcement information sharing systems, such as the Regional Information Sharing Systems Network and Law Enforcement Online, was not clearly defined. HSIN program management has pursued, but not achieved, a common logon capability with those systems since our 2006 report. As a result, the HSIN Law Enforcement COI has remained small, with approximately 2,000 active users. Several HSIN Law Enforcement users said that they only log on to HSIN in order to keep their account active.

Similarly, critical infrastructure protection personnel obtained information from other sources that provided the same kind of information as HSIN. Specifically, private sector personnel we spoke with said that HSIN Critical Sectors and the Federal Bureau of Investigation's InfraGard system have similar information. InfraGard is intended to share information between the Federal Bureau of Investigation and its private sector partners. Further, at one location, private sector personnel said that a State-level critical infrastructure information email list service also provided them with much of the same information they received on HSIN and InfraGard.

State and local personnel have also relied on the DHS intelligence officers deployed to their respective fusion centers to obtain information rather than on HSIN. Specifically, fusion center personnel we spoke to said that if they needed to request information from DHS, they asked the DHS intelligence officer deployed to their fusion center. Similarly, if they needed to receive critical information from DHS, they relied on their intelligence office to share that information with them. Further, DHS intelligence officers said that they often did not use HSIN and instead relied on their points of contact within DHS for information. Consequently, HSIN SLIC, which is intended to be the COI for sharing intelligence information between DHS and State and local intelligence personnel, remained small, with approximately 2,200 active users.

System Usability

HSIN use was also limited in part because account holders did not find the system user-friendly. Specifically, numerous system users we spoke with said that they could not easily locate information on HSIN. For example, users found browsing through the folders in the document library confusing and unhelpful for discovering new information that might be useful to them. Users said that old content was not archived, so a folder in the document library that looked relevant might not in fact be relevant because it contained old information. One user said that while browsing for information on chemical security, he found a folder that contained documents that were 4 years old.

In addition, users said that they could not easily find information on HSIN using the search functionality. Search results often did not contain the specific documents that users were looking for, which they had previously seen on HSIN. For example, one user tried to find an ecoterrorism document 6 months after it was initially posted, and had to go through folders document by document to find the specific document. Users also said that search results contained too many documents to look through that were not relevant to the search. For example, one user said that a search for a particular document returned 400 results, 350 of which referred to the same product.

The large number of HSIN COIs also sometimes made it difficult for users to find and share information. There were more than 1,300 COIs as of October 2012, making it difficult for users to know if they had access to the right COIs, or if there were other useful COIs that they did not know about. System users in one State said that they find it easier to call their points of contact in other States for information requests because of the large number of COIs. These users, however, said that this process makes them concerned that they might miss information, which could lead to an inability to "connect the dots" in a serious situation. Further, system users could not post information to multiple COIs at once; instead, users had to post information to each COI separately. System users we met with said that they did not have the time to post information multiple times, resulting in information being shared less broadly. HSIN program management had developed a plan to reduce the number of COIs and enable users to post documents to multiple COIs as part of the HSIN Release 3 upgrade. Until these changes are implemented, however, finding and sharing information across COIs on HSIN remains difficult at times.

Communication

The HSIN program has made progress communicating the role of the system to State and local personnel through the use of mission advocates; however, cuts to the mission advocate program threaten this progress. In 2006, we reported that the HSIN program had not clearly communicated the role of HSIN to State and local personnel, resulting in limited system buy-in. In 2008, we reported that limited resources continued to hinder communication and coordination with system stakeholders, resulting in ongoing challenges in meeting information sharing requirements. Since these reports, HSIN program management has deployed mission advocates to improve communication with system stakeholders and build the user community. Although mission advocates have demonstrated success building State-level COIs in some regions, the mission advocate program had been cut significantly, from 22 mission advocates to 8, because of budget constraints. This reduction in the number of mission advocates will likely have a direct effect on the support provided to field users and undermine a critical element for growing the user community.

Conclusion

HSIN's mission to facilitate information sharing across the homeland security enterprise has not been fully achieved. Some HSIN COIs were being used to share information; however, the overall size of the user community and the level of system use indicated that further progress was needed. DHS has invested an estimated $231 million in HSIN over 9 years but has not yet achieved the information sharing capability envisioned. HSIN program management has implemented plans and strategies to reorient HSIN through the HSIN Release 3 upgrade that may, once completed, improve HSIN. Information sharing with homeland security partners across Federal, State, local, tribal, and the private sector is a critical DHS mission, and the HSIN system could be a critical tool for supporting this mission if implemented effectively.

Recommendations

We recommend that the Director of Operations Coordination and Planning work with the Information Sharing and Safeguarding Governance Board and affiliated DHS components to:

Recommendation #1: Develop and implement a plan to increase DHS components' adoption of HSIN as their Sensitive but Unclassified information sharing portal.

Recommendation #2: Identify and develop a plan to meet user requirements for effective content organization, reliable search functionality, and efficient organization of COIs in HSIN Release 3.

We recommend that the Director of Operations Coordination and Planning work with the Undersecretary of Intelligence and Analysis to:

Recommendation #3: Develop and implement a plan to improve communication and collaboration with State and local stakeholders to expand exposure to HSIN and the capabilities the system can provide.

Management Comment and OIG Analysis

We obtained written comments on a draft of this report from the Director of the Office of Operations Coordination and Planning. We have included a copy of these comments in their entirety in appendix B.

In the comments, the Director concurred with our recommendations and provided details on steps being taken to address specific findings and recommendations in the report. We have reviewed management's comments and provided an evaluation of the issues described in the comments below. These recommendations are considered open and unresolved until we receive and evaluate the Director's corrective action plans.

In response to recommendation one, the Director concurred and indicated that the HSIN program has made incremental progress on user adoption and portal consolidation since the Secretary designated HSIN as the Department's Sensitive but Unclassified information sharing portal in 2006. The Director also indicated that partnering with the Information Sharing and Safeguarding Governance Board will allow the program to garner much needed support to achieve the user adoption and portal consolidation goals of the Department. Finally, the Director stated that the HSIN program will work with the Information Sharing and Safeguarding Governance Board and the Information Sharing Coordinating Council to develop and implement a plan to promote greater adoption of HSIN as the Department's target Sensitive but Unclassified portal. We recognize this action as a positive step toward addressing this recommendation and look forward to learning more about continued progress in the future.

Responding to recommendation two, the Director concurred and stated that the HSIN program continues to develop and implement plans for meeting user requirements around effective content organization, reliable search

functionality, and efficient organization of COIs in HSIN Release 3. The Director also indicated that the program plans to deliver increased search functionality and improved content organization in FY 2014. Further, the Director stated that the program will leverage the Information Sharing and Safeguarding Governance Board and the HSIN Executive Steering Committee to validate user requirements gathered by the HSIN program and verified by the HSIN User Working Group. We believe that such efforts are good steps toward addressing our recommendation and look forward to learning more about continued progress in this regard.

In response to recommendation three, the Director concurred and said that the HSIN program will work with the Under Secretary for Intelligence and Analysis, as well as other DHS offices, as appropriate, to develop and implement communications plans that will increase the use of HSIN and expand exposure to HSIN and its capabilities. We recognize this action as a positive step toward addressing this recommendation.

Appendix A
Objectives, Scope, and Methodology

The 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.

As part of our ongoing responsibilities to assess the efficiency, effectiveness, and economy of departmental programs and operations, we conducted an audit to determine the effectiveness of HSIN in supporting information sharing among select stakeholders as well as progress made with HSIN since our October 2008 report, *DHS' Efforts to Improve the Homeland Security Information Network (OIG-09-07)*.

We researched and reviewed Federal laws, Department management and acquisition directives, and other executive guidance related to IT systems, planning, management, and governance. We reviewed recent Government Accountability Office (GAO) and OIG reports to determine prior challenges, findings, and recommendations. Additionally, we searched the Internet to obtain and review documents and news articles pertaining to HSIN and information sharing. Furthermore, we evaluated documents that DHS OPS provided in July 2009 on activities to address and close our October 2008 report recommendations. We also obtained access to select HSIN COIs to view information sharing via the system. Using this information; we designed a data collection approach consisting of focused interviews, documentation analysis, site visits, and HSIN system demonstrations to conduct our followup review.

We conducted our audit fieldwork from August to November 2012 at HSIN Program Office headquarters in Washington, DC. We met with key Department officials responsible for HSIN's planning, implementation, program management, and governance to obtain information on the progress made to resolve challenges identified in our prior reports, assess the current status of information sharing among select HSIN stakeholders, and determine challenges to the planning and implementation of the HSIN system. These officials included members of the DHS OCIO, OPS, I&A, and other components. Additionally, we met with members of the HSIN Executive Steering Committee, mission advocates, and leaders of stakeholder communities.

We also met with stakeholders at the following fusion centers: Sacramento, California; Salem, Oregon; Atlanta, Georgia; Tallahassee, Florida; Phoenix, Arizona; Austin, Texas; and Baton Rouge, Louisiana. Additionally, we met with United States Coast Guard

stakeholders in New Orleans, Louisiana, and emergency management stakeholders in Austin, Texas, and Gleneden Beach, Oregon.

At field locations, we met with fusion center directors, intelligence analysts and officers, security specialists, antiterrorism coordinators, private sector stakeholders, tribal stakeholders, HSIN administrators, and other HSIN users to understand HSIN user requirements and system use in the field. We discussed legacy HSIN and the extent to which it meets mission information sharing needs, user involvement, communication with headquarters, and the upcoming implementation of HSIN Release 3. We also discussed the use of HSIN during special events and major HSIN success stories. Where possible, we obtained documentation to support the information provided during the meetings.

We conducted this performance audit between August 2012 and January 2013 pursuant to the *Inspector General Act of 1978*, as amended, and according to 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon 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 of Information Management. Major OIG contributors to the audit are identified in appendix C.

Appendix B
Management Comments to the Draft Report

*Office of Operations Coordination
and Planning*
U.S. Department of Homeland Security
Washington, DC 20528

**Homeland
Security**

MAY **1 7 2013**

MEMORANDUM FOR: Charles K. Edwards
Acting Inspector General

FROM: Richard Chávez
Director, Office of Operations Coordination and Planning
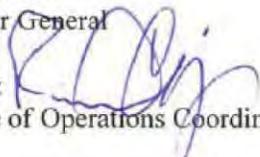
SUBJECT: DHS Office of Inspector General Draft Report: "Homeland
Security Information Network Improvements and Challenges"

Purpose

The Office of Operations Coordination and Planning (OPS) appreciates the work of the Office of
Inspector General (OIG) in conducting this review of the Homeland Security Information
Network (HSIN). Below are responses to each of the recommendations.

Discussion

OIG Recommendation #1: We recommend that the DHS Director of Operations Coordination
and Planning work with the Information Sharing and Safeguarding Governance Board and
affiliated Components to: Develop and implement a plan to increase DHS components' adoption
of HSIN as their Sensitive but Unclassified information sharing portal.

OPS Response: Concur. The Secretary of Homeland Security identified HSIN as the
Department's Sensitive but Unclassified (SBU) information sharing portal in 2006, and since
then, the program has made incremental progress on user adoption and portal consolidation.
Partnering with the Information Sharing and Safeguarding Governance Board (ISSGB) will
allow the program to garner much needed support to continue to achieve the user adoption and
portal consolidation goals of the Department. The HSIN program will work with the ISSGB and
its subordinate council, the Information Sharing Coordinating Council (ISCC), to develop and
implement a plan to promote greater adoption of HSIN as the Department's target SBU portal.

OIG Recommendation #2: We recommend that the DHS Director of Operations Coordination
and Planning work with the Information Sharing and Safeguarding Governance Board and
affiliated Components to: Identify and develop a plan to meet user requirements for effective
content organization, reliable search functionality, and efficient organization of COIs in HSIN
Release 3.

OPS Response: Concur. The HSIN program continues to develop and implement plans for meeting user requirements around effective content organization, reliable search functionality, and efficient organization of Communities of Interest (COIs) in HSIN Release 3 (R3). Currently, the HSIN program is migrating users to a new release of the platform called HSIN R3 which has a much better organizational structure designed for more efficient information sharing. The program is currently working to deliver increased search functionality and improved content organization in Fiscal Year 14. The program will leverage the ISSGB and the HSIN Executive Steering Committee to validate that the plans meet the user requirements gathered by the HSIN program and verified by the HSIN User Working Group.

OIG Recommendation #3: We recommend that the DHS Director of Operations Coordination and Planning work with the Undersecretary of Intelligence and Analysis-to: Develop and implement a plan to improve communication and collaboration with State and local stakeholders to expand exposure to HSIN and the capabilities the system can provide.

OPS Response: Concur. The HSIN program will work with the Undersecretary of Intelligence and Analysis, and, as appropriate, other DHS offices with State and local equities, to develop and implement communications plans that will increase the use of HSIN and expand exposure to HSIN and its capabilities.

Appendix C
Major Contributors to This Report

Richard Harsche, Division Director
Steven Staats, Auditor Manager
Erin Dunham, Auditor
Anna Hamlin, Auditor
Kevin Mullinix, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary, Office of Intelligence and Analysis
Chief Information Officer, DHS Office of the Chief Information Officer
OIG Liaison, Office of Operations Planning and Coordination
OIG Liaison, Office of Intelligence and Analysis
OIG Liaison, Office of the Chief Information Officer
Director of Local Affairs, Office of Intergovernmental Affairs
Acting Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate