October 2008

INFORMATION TECHNOLOGY

Management Improvements Needed on the Department of Homeland Security's Next Generation Information Sharing System

G A O

Accountability ★ Integrity ★ Reliability

INFORMATION TECHNOLOGY

Management Improvements Needed on the Department of Homeland Security's Next Generation Information Sharing System

Why GAO Did This Study

The Department of Homeland Security (DHS) is responsible for coordinating the federal government's homeland security communications with all levels of government. In support of this mission, DHS implemented, and has been enhancing, the Homeland Security Information Network (HSIN). It also has proposed a follow-on system, called Next Generation HSIN (HSIN Next Gen). GAO was asked to determine whether (1) DHS has stopped further improvements on HSIN and if so, the department's rationale for doing so and plans for acquiring its proposed follow-on system HSIN Next Gen and (2) the department is effectively managing the HSIN Next Gen acquisition. To accomplish this, GAO analyzed documentation, interviewed officials, and compared acquisition management processes and practices defined in industry best practices with those planned and underway by DHS.

What GAO Recommends

GAO recommends strengthening acquisition management controls before the department starts to migrate existing users to the new system by, among other things, staffing the program office appropriately, ensuring all user requirements are gathered, and identifying key risks surrounding the project. In written comments on this report, DHS described actions planned and underway to address GAO recommendations.

What GAO Found

DHS halted further improvements on the existing HSIN system in September 2007. Since then, the department has continued to operate and maintain the system while a replacement—HSIN Next Gen—is being planned and acquired. DHS decided in large part to pursue this replacement due to

- the existing system has security and information-sharing limitations that do not meet department and other users' needs, thus impeding the department's ability to effectively perform its mission; and
- the new system is to be a key part of a departmentwide consolidation effort to, among other things, reduce the number of systems within DHS that share sensitive but unclassified information.

DHS has developed an acquisition strategy for HSIN Next Gen, whereby the system is to be implemented in four phases, each providing for an increasing number of users to be transitioned to the system. For example, DHS plans to begin transitioning existing HSIN users beginning in May 2009. Further, in May 2008, DHS issued a task order engaging a contractor to acquire, deploy, operate, and maintain the new system. The total estimated value of the task order's initial year is $19 million; the order also includes 4 option years that if exercised, are estimated to be worth $62 million. DHS intends to continue to use the existing HSIN with the goal of terminating its use in September 2009 when HSIN Next Gen is to be fully completed. DHS estimates it will cost $3.1 million to operate and maintain HSIN between now and its planned September 2009 termination.

DHS is in the process of implementing key acquisition management controls for HSIN Next Gen, but has yet to implement the full set of controls essential to effectively managing information technology system projects in a rigorous and disciplined manner. Specifically, it has not fully implemented key process controls in the areas of

- project and acquisition planning,
- requirements development and management, and
- risk management.

DHS officials, including the Office of Operations Coordination and Planning's Chief Information Officer, who is responsible for managing the project, attribute the partial implementation of these key processes in large part to the aggressive schedule for acquiring and deploying HSIN Next Gen. The Chief Information Officer also stated the department plans to address these weaknesses by, for example, tasking its contractor to assist in the development and completion of the risk management process area, but had not yet established dates for when all of these activities will be completed. Until these weaknesses are effectively addressed and DHS implements and institutionalizes the full set of acquisition management controls, the project will be at increased risk of operating in an ad hoc and chaotic manner— potentially resulting in increased project costs, delayed schedules, and performance shortfalls.

_____ **United States Government Accountability Office**

Contents

Abbreviations

DHS	Department of Homeland Security
CIO	Chief Information Officer
HSIN	Homeland Security Information Network
HSIN Next Gen	Next Generation HSIN
IT	information technology
OPS	Office of Operations Coordination and Planning

United States Government Accountability Office
Washington, DC 20548

October 8, 2008

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and
    Governmental Affairs
United States Senate

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Department of Homeland Security (DHS) is responsible for coordinating the federal government's homeland security communications with all levels of government—including state and local. In support of this mission, the department deployed, and has been making improvements to, the Homeland Security Information Network (HSIN) as part of its goal to establish an infrastructure for sharing homeland security information. In 2005,[1] and more recently in January 2007,[2] we designated homeland security information sharing as a high-risk area. Consequently, it is important that federal networks and associated systems, applications, and data facilitate this vital information sharing, and do so in a manner that produces effective information sharing among and between the various levels of government. This is particularly crucial for DHS's HSIN, which is the department's primary information technology (IT) system for sharing terrorism and related information. Recently, DHS proposed a follow-on system to HSIN, which it refers to as Next Generation HSIN (HSIN Next Gen).

This report responds to your request that we determine whether (1) DHS has stopped further improvements on HSIN and if so, the department's rationale for doing so and plans for acquiring its proposed follow-on system HSIN Next Gen and (2) the department is effectively managing the HSIN Next Gen acquisition.

---

[1]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

[2]GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

On July 11, 2008, and July 17, 2008, we provided a briefing to staff of the House Homeland Security Committee and Senate Homeland Security and Governmental Affairs Committee, respectively. Prior to these staff briefings (on July 9, 2008), we provided the briefing to responsible DHS officials, who agreed in large part with our findings, conclusions, and recommendations. This report transmits (1) the slides that we used during the briefings and (2) the recommendations that we made to the Secretary of Homeland Security and the Director, Office of Operations Coordination and Planning, who is responsible for managing HSIN and HSIN Next Gen. The full briefing, including our scope and methodology, is reprinted as appendix I.

DHS Has Stopped Current HSIN System Improvements and Is in the Process of Acquiring a Replacement System

In September 2007, the department halted further improvements on the existing HSIN system. Since then, DHS has continued to operate and maintain the system while its replacement—HSIN Next Gen—is being planned and acquired. The department decided to pursue the replacement for two reasons. First, the existing system has security and information-sharing limitations that do not meet department and other users' needs. For example, with regard to security, the current HSIN does not support role-based access controls[3] and two-factor authentication.[4] These limitations hinder the department's ability to effectively perform its mission.

Second, the replacement system is to be used as a key part of a departmentwide consolidation effort aimed at reducing the number of multiple portals or Web-based systems within DHS by consolidating the systems across the department that are to share sensitive but unclassified information. In particular, HSIN Next Gen is to provide secure access to DHS sensitive but unclassified information and services for all department user communities, including those in the law enforcement, intelligence, immigration, and emergency and disaster management communities.

With regard to DHS plans to acquire HSIN Next Gen, the department has developed an acquisition strategy for the system and plans to have all users on the new system by September 2009. The system will be

---

[3]Role-based access controls limit system functions based on a user's designated role.

[4]Two-factor authentication is a way of verifying someone's identity by using two of the following: something the user knows (password), something the user has (badge), or something unique to the user (fingerprint).

implemented in four phases, each addressing a functional portion of the requirements and providing for an increasing number of users to be transitioned to the system. Specifically, during the first phase of implementation, the department plans to bring on board up to 20,000 new users from critical infrastructure sectors such as agriculture and food, and transportation systems. In addition, during the second phase (called Initial Operational Capability) and third phase (called Maturing Operational Capability), DHS plans to transition over 26,000 users that currently use the existing HSIN system; this transition of existing HSIN users is to begin in May 2009. To help carry out the strategy, DHS issued a task order in May 2008 engaging a contractor to acquire, deploy, operate, and maintain the new system. The total estimated value of the base year of this arrangement is $19 million, and the total estimated value, if each of the four options is exercised, is $62 million.

DHS intends to continue to use the existing HSIN with the goal of terminating its use in September 2009 when HSIN Next Gen is to be fully implemented. DHS estimates it will cost $3.13 million to operate and maintain HSIN between now and its planned September 2009 termination.

DHS Has Yet to Implement the Management Controls Essential to Effectively Manage the HSIN Next Gen Acquisition

As we have previously reported,[5] the success of critical projects such as HSIN depends on developing and implementing a full set of acquisition management controls to effectively manage the project. While DHS is in the process of implementing key acquisition management controls for HSIN Next Gen, it has yet to implement the full set of controls essential to managing HSIN Next Gen in a disciplined and rigorous manner. Specifically, it has not implemented key process controls in the areas of

- project and acquisition planning, which includes key processes, such as developing a program office and identifying staff roles and responsibilities;

- requirements development and management, which involves key processes, such as gathering, analyzing, and validating user requirements; and

---

[5]For example, GAO, *Information Technology: Management Improvements Needed on Immigration and Customs Enforcement's Infrastructure Modernization Program*, GAO-05-805 (Washington, D.C.: Sept. 7, 2005) and *Census Bureau: Important Activities for Improving Management of Key 2010 Decennial Acquisitions Remain to be Done*, GAO-06-444T (Washington, D.C.: Mar. 1, 2006).

- risk management, which includes key processes, such as identifying and analyzing risks and assigning responsibilities for managing risks.

With regard to project and acquisition planning, DHS has established a program office for HSIN Next Gen, including filling the position of project manager. However, it has not adequately staffed the HSIN Next Gen program office and identified staff roles and responsibilities.

In addition, in the area of requirements development and management, the department has gathered and analyzed requirements from critical infrastructure sector users. However, it has not gathered requirements from all other HSIN users and developed a change control process for managing change to requirements.

Further, regarding risk management, DHS has begun to develop a risk management plan that defines staff roles and responsibilities. However, it has yet to identify all key risks surrounding the project and develop risk mitigation plans and completion milestones.

DHS officials, including the Office of Operations Coordination and Planning's (OPS) Chief Information Officer (CIO), who is responsible for managing the project, attribute the partial implementation of these key processes in large part to the aggressive schedule for acquiring and deploying HSIN Next Gen. In our view, engaging a contractor and commencing work before implementing mature controls is not a recipe for success. Specifically, our research and experience at federal agencies have shown that the probability of success is low using this approach. The OPS CIO stated the department plans to address these weaknesses by, for example, tasking its contractor to assist in the development and completion of the risk management process area, but had not yet established dates for when all of these activities will be completed.

Consequently, until these weaknesses are effectively addressed and DHS implements and institutionalizes the full set of acquisition management controls, the project will be at increased risk of operating in an ad hoc and chaotic manner—potentially resulting in increased project costs, delayed schedules, and performance shortfalls.

Conclusions

DHS has been challenged in its ability to efficiently and effectively manage the department's existing primary information-sharing system. In particular, although DHS has invested upwards of $70 million on the system, it still does not fully meet user needs and as a result, has not been

fully utilized. DHS intends to address this performance shortfall by, among other things, acquiring a replacement system. A key challenge for DHS in this effort will be ensuring it develops an information-sharing system that effectively addresses its users' needs and in the process, does not waste or unwisely invest critical department resources.

To its credit, DHS has initiated some important steps in establishing sound and capable acquisition controls, but much remains to be accomplished before DHS management efforts can be considered effective and thereby minimize the risks associated with HSIN Next Gen delivering promised capabilities and benefits on time and within budget.

Investing money given the current state of management controls puts the project at risk. Given what is at stake, it is extremely important that DHS direct its attention to these management issues, and mitigate the associated risks as soon as possible.

Recommendations for Executive Action

To minimize risks to the HSIN Next Gen project, we are making six recommendations to the Secretary of Homeland Security aimed at strengthening management of the project. We recommend that the Secretary direct the Director, Office of Operations Coordination and Planning to strengthen program management controls by

- staffing the program office appropriately;

- identifying staff roles and responsibilities;

- ensuring all requirements are gathered, analyzed, and validated;

- developing and implementing a requirements change control process; and

- ensuring effective risk management by identifying all key risks surrounding the project and developing risk mitigation plans and completion milestones.

We also recommend that these controls be implemented before the department starts to migrate users to HSIN Next Gen's Initial Operational Capability.

Agency Comments and Our Evaluation

In written comments on a draft of this report, which were in a letter signed by DHS's Director of Operations Coordination and Planning and are reprinted in appendix II, the department described actions planned and underway to address our recommendations. These actions are consistent with those described by DHS in response to our July 9, 2008, briefing to the department in which it largely agreed with our findings, conclusions, and recommendations.

We are sending copies of this report to interested congressional committees and the Secretary of Homeland Security. We will also make copies available to others on request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

Should you or your staffs have any questions concerning this report, please contact me at 202-512-9286 or by e-mail at pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

David A. Powner
Director, Information Technology
Management Issues

Appendix I: Briefing Slides to Congressional Staff

GAO
Accountability * Integrity * Reliability

Information Technology: Management Improvements Needed on the Department of Homeland Security's Next Generation Information Sharing System

Briefing to the Staffs of the

Senate Committee on Homeland Security and Governmental Affairs
July 17, 2008

House Committee on Homeland Security
July 11, 2008

G A O
Accountability * Integrity * Reliability

Table of Contents

- Introduction

- Objectives, Scope, and Methodology

- Results in Brief

- Background

- Results

    o HSIN Is Currently Operational but Further Improvements Have Been Halted

    o Acquisition Management Controls Needed

- Conclusions

- Recommendations

- Agency Comments and Our Evaluation

- Attachment I: Scope and Methodology

2

G A O

Accountability * Integrity * Reliability

Introduction

The Department of Homeland Security (DHS) is responsible for coordinating the federal government's homeland security communications with all levels of government—including state and local. In support of this mission, the department implemented, and has been enhancing, the Homeland Security Information Network (HSIN) as part of its goal to establish an infrastructure for sharing homeland security information.[1] Recently, DHS proposed a follow-on system to HSIN, which it refers to as Next Generation HSIN (HSIN Next Gen).

In 2005,[2] and more recently in January 2007,[3] we designated homeland security information sharing as a high-risk area. Consequently, it is important that federal networks and associated systems, applications, and data facilitate this vital information sharing, and do so in a manner that produces effective information sharing among and between the various levels of government. This is particularly crucial for DHS's HSIN, which is the department's primary information technology (IT) system for sharing terrorism and related information.

---

[1]The Homeland Security Act of 2002 directed DHS to establish communications to share homeland security information with federal agencies, state and local governments, and other specified groups.
[2]GAO, *High-Risk Series: An Update,* GAO-05-207 (Washington, D.C.: January 2005).
[3]GAO, *High-Risk Series: An Update,* GAO-07-310 (Washington, D.C.: January 2007).

3

GAO
Accountability * Integrity * Reliability

Objectives, Scope, and Methodology

As agreed, our objectives were to determine whether

- DHS has stopped further improvements on HSIN and if so, the department's rationale for doing so and plans for acquiring its proposed follow-on system called HSIN Next Gen system, and

- the department is effectively managing the HSIN Next Gen acquisition.

For our first objective, we analyzed documentation and interviewed DHS officials from the office responsible for managing HSIN and HSIN Next Gen, the Office of Operations Coordination and Planning (OPS), to assess efforts planned and underway to implement HSIN system improvements and acquire HSIN Next Gen.

4

G A O
Accountability * Integrity * Reliability

Objectives, Scope, and Methodology

For our second objective, we compared processes and practices defined in the Software Engineering Institute's Capability Maturity Model® Integration for Acquisition (CMMI-ACQ)[4] and in our prior work analyzing best practices in industry and government[5] with those planned and underway by the department to determine the extent of implementation. In judging implementation, we used the following criteria: the processes were (1) *fully implemented* if all of the related guidance was addressed; (2) *partially implemented* if some, but not all, of the related guidance was addressed; and (3) *not implemented* if none of the related guidance was addressed.

Details of our scope and methodology are provided in attachment I. We conducted this performance audit from January 2008 to June 2008, 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.

_____

[4]Carnegie Mellon Software Engineering Institute, *Capability Maturity Model® Integration for Acquisition (CMMI-ACQ),* Version 1.2 (November 2007).
[5] For example, GAO, *Information Technology: Management Improvements Needed on Immigration and Customs Enforcement's Infrastructure Modernization Program,* GAO-05-805 (Washington, D.C.: Sept. 7, 2005) and *Census Bureau: Important Activities for Improving Management of Key 2010 Decennial Acquisitions Remain to be Done,* GAO-06-444T (Washington, D.C.: Mar. 1, 2006).

5

G A O
Accountability • Integrity • Reliability

Results In Brief

DHS halted further improvements on the existing HSIN system in September 2007. Since then, the department has continued to operate and maintain the system while a replacement—called HSIN Next Gen—is being planned and acquired. DHS decided to pursue this replacement for two reasons.

- First, the existing system has security and information sharing limitations that do not meet department and other users' needs, thus impeding the department's ability to effectively perform its mission.

- Second, the replacement system is to be used as a key part of a departmentwide consolidation effort to reduce the number of duplicative DHS Web-based systems.

DHS has developed an acquisition strategy for the system and plans to have all users on the new system by September 2009. DHS intends to continue to use the existing HSIN with the goal of retiring it once HSIN Next Gen has been completed. DHS estimates it will cost $3.13 million to operate and maintain HSIN between now and retirement.

6

G A O
Accountability * Integrity * Reliability

Results In Brief

DHS is in the process of implementing key acquisition management controls for HSIN Next Gen. For example, DHS has established a program office for HSIN Next Gen, including filling the position of project manager. In addition, DHS has begun to develop a risk management plan that defines staff roles and responsibilities. However, DHS has yet to implement the full set of controls essential to effectively managing IT system projects in a rigorous and disciplined manner. Specifically, it has not fully implemented key process controls in the areas of

- project and acquisition planning,

- requirements development and management, and

- risk management

DHS officials, including the OPS Chief Information Officer (CIO), who is responsible for managing the project, attribute the partial implementation of these key processes in large part to the aggressive schedule for acquiring and deploying HSIN Next Gen. DHS has activities planned and underway to address missing controls, but has not established dates for when all of these activities will be completed.

7

G A O
Accountability * Integrity * Reliability

Results in Brief

Until DHS has implemented these controls, there is increased risk of the project operating in an ad hoc and chaotic manner—potentially resulting in increased project costs, delayed schedules, and performance shortfalls. Accordingly, we are making recommendations to the Secretary of Homeland Security to (1) strengthen management controls, including project and acquisition planning, requirements development and management, and risk management; and (2) ensure that these controls be implemented before users are transitioned to HSIN Next Gen Initial Operational Capability.

In orally commenting on a draft of this briefing, DHS officials stated that they agreed with our findings and recommendations and described actions they have initiated to implement our recommendations. They also generally agreed with our conclusions. However, DHS officials stated that the risk raised in our conclusions was mitigated by their IT experience. While experience is important, key process controls, such as rigorous and disciplined requirements and risk management, are also essential to IT project success.

8

G A O
Accountability • Integrity • Reliability

Background

DHS is the lead department involved in securing our nation's homeland. Its mission includes, among other things, leading the unified national effort to secure the United States, preventing and deterring terrorist attacks, and protecting against and responding to threats and hazards to the nation.

As part of its mission and as required by the Homeland Security Act of 2002,[6] the department is also responsible for coordinating efforts across all levels of government and throughout the nation, including with federal, state, tribal, local, and private sector homeland security resources. This includes coordinating the federal government's networks and other communications systems with state and local governments.

In 2004, DHS developed and implemented HSIN as the department's primary IT system for sharing terrorism and related information with federal, state, and local agencies, among others. Specifically, this Web-based communication system is to provide a secure and trusted national IT system for sensitive but unclassified information sharing and collaboration among federal, state, local, tribal, territorial, private sector, and international partners engaged in preventing, protecting from, responding to, and recovering from all threats, hazards, and incidents within DHS's authority.

_____

[6]Homeland Security Act of 2002, Pub. L. No. 107-296 (Nov. 25, 2002).

9

G A O
Accountability • Integrity • Reliability

Background

HSIN offers both real-time chat and instant messaging capability, as well as a document library that contains reports from multiple federal, state, and local sources. Available through the system are suspicious incident and pre-incident information and analysis of terrorist threats, tactics, and weapons. Each community of interest has Web pages that are tailored for the community and contain general and community-specific news articles, links, and contact information.

HSIN is to support a number of homeland security-related mission areas that cover thousands of users across the United States. These mission areas include over 35 user groups, commonly referred to as communities of interest, including

- emergency management,

- law enforcement,

- counterterrorism,

- individual states, and

- private sector communities.

10

G A O
Accountability * Integrity * Reliability

Background

Other DHS component organizations, such as the Office of Infrastructure Protection, the Coast Guard, and Federal Emergency Management Agency, use HSIN as a tool to further their respective missions and therefore have assisted in the development, operations and maintenance, and enhancement of HSIN. For example, according to the Office of Infrastructure Protection, it works with the critical infrastructure sectors—that is, groups of similar private and government entities that operate and maintain systems and assets, whether physical or virtual, so vital to the nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters[7]—to gather user requirements and develop business processes in order to integrate HSIN into the critical sectors' information-sharing environment.

_____

[7] The critical infrastructure sectors include agriculture and food; banking and finance; chemical; commercial facilities; commercial nuclear reactors, materials, and waste; communications; critical manufacturing; dams; defense industrial base; drinking water and water treatment systems; emergency services; energy; government facilities; information technology; national monuments and icons; postal and shipping; public health and health care; and transportation systems.

11

G A O
Accountability • Integrity • Reliability

Background

The Office of Operations Coordination and Planning (OPS) CIO is responsible for ensuring that HSIN supports the needs of the department and its partners. This includes managing HSIN operations and maintenance, making necessary enhancements to the current system, and developing and acquiring HSIN Next Gen. The OPS CIO reports directly to the OPS Director who in turn reports directly to the DHS Secretary and Deputy Secretary.

Through fiscal year 2007, the department reports it has expended about $70 million on HSIN, and for fiscal year 2008, the department had budgeted about $21 million for operations, maintenance, and enhancement.

12

Background

In April 2007,[8] we reported that when coordinating efforts between HSIN and other state and local information-sharing initiatives, DHS did not fully adhere to key practices aimed at enhancing information sharing, collaboration, and avoiding duplication. For example, in developing the system, the department did not work with two key state and local initiatives, which are major parts of the Regional Information Sharing System program, to fully develop joint strategies to meet mutual needs.

In addition, it did not develop compatible policies, procedures, and other means to operate across organizational boundaries. DHS's limited use of these practices was attributable to a number of factors, including the department's expediting its schedule to deploy information-sharing capabilities after the events of September 11, 2001, and in doing so not developing a comprehensive inventory of key state and local information-sharing initiatives.

_____

[8]GAO, *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives*, GAO-07-455 (Washington, D.C.: April 16, 2007).

13

Background

Prior GAO Reviews Have Identified Opportunities for Improvement

As a result, we found there was increased risk that, among other things, effective information sharing is not occurring. Additionally, the department risked duplication of state and local capabilities. We recommended, among other things, that DHS

- identify and develop a comprehensive inventory of state and local initiatives;

- assess whether there are opportunities for HSIN to improve information sharing and avoid duplication of effort; and

- where there are opportunities, implement effective coordination and collaboration practices.

14

G A O
Accountability * Integrity * Reliability

Background

In response, DHS largely agreed with our recommendations and initiated actions to implement them. Examples include the following:

- In October 2007 and in February 2008, the HSIN Advisory Council—a HSIN user group composed of representatives from state, tribal, and local governments and the private sector—met to discuss HSIN information-sharing activities and provided strategic-level recommendations to the OPS Director.

- The HSIN Mission Coordinating Committee—a user group composed of representatives from DHS's components (e.g., the Office of Infrastructure Protection, the Coast Guard, and the Federal Emergency Management Agency)—has met five times over the past year to address their respective users' requirements for HSIN.

15

G A O
Accountability * Integrity * Reliability

Background

In July 2007,[9] we reported on challenges the department faced when using HSIN to share information with critical infrastructure sectors. Examples included:

- DHS officials responsible for leading the national effort to reduce critical infrastructure risk stated that although they encouraged critical sector entities to use HSIN, the system did not provide the capabilities that were promised, including providing the level of security expected by certain sectors.

- An internal DHS review of HSIN determined that the department had not clearly defined the purpose and scope of the system, and that the system had been developed without sufficient planning and project management.

_____

[9]GAO, *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve,* GAO-07-706R (Washington, D.C.: July 10, 2007).

16

Results: Objective 1

HSIN Is Currently Operational but Further Improvements Have Been Halted

DHS Has Stopped Current HSIN System Improvements and Is in the Process of Acquiring a Replacement System

The department halted further HSIN improvements in September 2007 but it continues to operate and maintain the system while its replacement—HSIN Next Gen—is being planned and acquired.

DHS decided to pursue a replacement system based on two reasons. First, the current system has security and information-sharing limitations that do not meet its users' needs and thus impedes the department's ability to effectively perform its mission. Second, the new system is to be used as part of a departmentwide effort—referred to as the portal consolidation program—to consolidate multiple portals or Web-based systems and improve sensitive but unclassified information-sharing capabilities within the department.

DHS has developed a HSIN Next Gen acquisition strategy and as part of the strategy, issued a May 2008 task order engaging a contractor to develop the system. DHS plans to have all users on the new system by September 2009. In the interim, DHS plans to continue to operate and maintain HSIN as the new system is acquired and deployed and users are transitioned to it. Once user transition is complete, the department intends to retire HSIN.

17

G A O
Accountability * Integrity * Reliability

Results: Objective 1
HSIN Improvements Halted Due to System Limitations

In September 2007, DHS executives, including the Undersecretary for Management, Chief Information Officer, Director of Operations Coordination and Planning, and key system user representatives (e.g., Office of Infrastructure Protection), met to discuss HSIN operations. Key representatives said HSIN was not meeting their needs due to system security and information-sharing limitations.

System security limitations cited included the system's inability to support

- role-based access controls, which limit system functions based on a user's designated role, and

- two-factor authentication, which is a way of verifying someone's identity by using two of the following: something the user knows (password), something the user has (badge), or something unique to the user (fingerprint).

18

G A O
Accountability ∗ Integrity ∗ Reliability

Results: Objective 1
HSIN Improvements Halted Due to System Limitations

Information-sharing limitations included the system's inability to

- enable users to access HSIN and systems outside of DHS (such as the state and local law enforcement's Regional Information Sharing System) using single sign capability (i.e., requiring only one user name and password);

- enable users to send alerts and notifications and receive alerts through e-mail or cell phones;

- support online meetings and presentations; and

- upload new users into the system in bulk.

19

G A O
Accountability * Integrity * Reliability

Results: Objective 1
HSIN Improvements Halted

According to user representatives, these limitations were hindering their ability to perform the mission of the department. For example, representatives from the Office of Infrastructure Protection (which is part of the National Protection and Programs Directorate) stated that without the security controls, private-sector officials from the critical infrastructure sectors were reluctant to share with DHS sensitive information about sector infrastructure that is essential to protecting the homeland, thus inhibiting the department's ability to adequately build trusted relationships with sector officials. In response, the Office of Infrastructure Protection initiated an effort to obtain requirements from HSIN critical infrastructure sectors users, augmenting the requirements the department had for the existing system.

Consequently, the executives at the September 2007 meeting (referenced above) decided the best way to implement the missing security and information-sharing capabilities was via a new system, rather than by enhancing the existing system. According to these officials, they based their decision largely on the view that the existing system could not be enhanced to provide these capabilities in a cost-effective manner. These officials also decided at this time to halt any further HSIN enhancements until the new system (HSIN Next Gen) was implemented, at which point they planned to retire the current HSIN system.

20

G A O
Accountability * Integrity * Reliability

Results: Objective 1
HSIN Next Gen's Goal Is to Also Eliminate Duplication

In addition, in October 2007 the Under Secretary for Management issued a memorandum detailing how HSIN Next Gen is to be used as an integral part of the department's portal consolidation program. According to the memorandum, the current DHS Web environment consists of more than 100 Web-based systems, which are mostly duplicative in capabilities. HSIN Next Gen is part of a departmentwide program aimed at reducing the number of duplicative Web-based systems within DHS by consolidating the systems across the department that are used to share sensitive but unclassified information, and by replacing portal technologies that limit its information-sharing capabilities.

In particular, according to the memorandum, HSIN Next Gen is to provide secure access to DHS information and services for all DHS user communities, including those in the law enforcement, intelligence, immigration, and emergency and disaster management communities.

21

G A O
Accountability * Integrity * Reliability

Results: Objective 1
Homeland Security Information Network Next Generation

As part of the system acquisition and implementation strategy, DHS plans to continue operating and maintaining HSIN until September 2009. The department estimates the cost to operate and maintain the current system through September 2009 will be $3.13 million. DHS reports it will have spent a total of $91 million on HSIN by the end of fiscal year 2008.

In parallel, the department plans to begin developing and implementing HSIN Next Gen in four phases; the phases—along with a brief description of their functional purpose—are as follows.

- Phase one, referred to as Spiral 1, is to establish an operational platform for the HSIN critical sector users' requirements.
- The second phase, Initial Operational Capability, is to (1) deliver requirements currently supported by HSIN, as well as provide additional security controls and (2) begin migrating users of the current system to HSIN Next Gen.
- Phase three, Maturing Operational Capability, is to migrate all remaining users of the current system to HSIN Next Gen.
- The fourth phase, called the Final Operational Capability, is to provide for improved content management; better information discovery and delivery; and improved alert, notification, and public announcement functions.

22

Each phase is intended to, among other things, address a functional portion of the requirements and provide for an increasing number of users to be transitioned to the system. In addition, DHS plans to draw upon the existing HSIN system and capabilities, rather than developing a complete infrastructure replacement. Specifically, where possible, it plans to re-use existing HSIN hardware and software. The department plans to use the contractor (discussed in detail below) to help them do this. However, it has yet to set a date for when this is to be completed.

Further, in terms of users, during the first phase of implementation, the department plans to bring on board up to 20,000 critical sector users. In addition, over the second and third phases, DHS plans to transition over 26,000 users that currently use the existing HSIN system.

In May 2008, the department issued a task order to a contractor[10] to acquire, deploy, operate, and maintain the new system. The total estimated value of the base year of this arrangement is $19 million, and the total estimated value, if each of the four options is exercised, is $62 million.

_____

[10] The department issued a cost-plus-fixed-fee task order under the Enterprise Acquisition Gateway for Leading Edge Solutions (EAGLE). EAGLE is a DHS multiple award indefinite-delivery/indefinite-quantity contract, under which DHS conducted a competition for the HSIN Next Gen task order.

23

G A O
Accountability * Integrity * Reliability

Results: Objective 1
Homeland Security Information Network Next Generation

Each of the HSIN Next Gen phases, the timing of their implementation, the percentage of users to be transitioned, and the date the contractor was issued the task order are depicted in figure 1.

24

G A O
Accountability * Integrity * Reliability

Results: Objective 1
Homeland Security Information Network Next Generation

Figure 1: HSIN Next Generation Phases and Associated Milestones
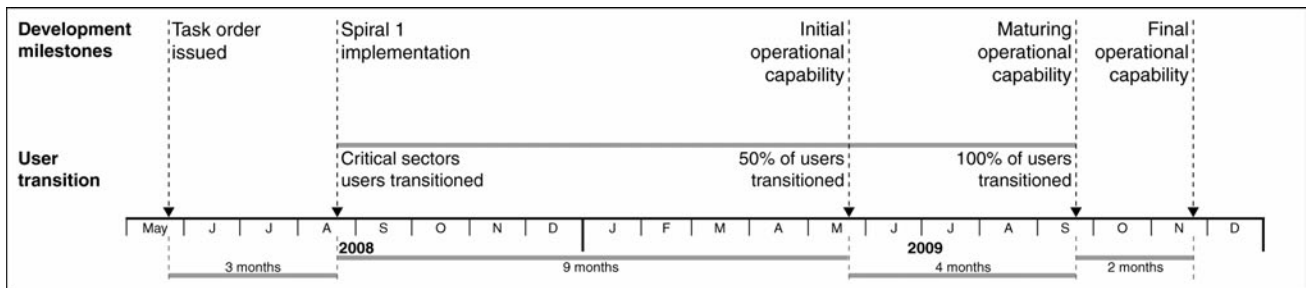
Source: GAO analysis of DHS data.

Key dates are:

- May 2008 – issued task order to contractor for HSIN Next Gen.
- August 2008 – implement Spiral 1 with the goal of supporting up to 20,000 critical sectors users.
- May 2009 – complete Initial Operational Capability with 13,000 current users scheduled to transition.
- September 2009 – implement Maturing Operational Capability with the transition of the remaining 13,000 users.
- November 2009 – complete Final Operational Capability by delivering new functionality to users.

25

G A O

Accountability * Integrity * Reliability

Results: Objective 2
Acquisition Management Controls Needed

DHS Has Yet to Implement the Management Controls Essential to Effectively Manage the HSIN Next Gen Acquisition

DHS is in the process of implementing key acquisition management controls, but it has yet to implement the full set of controls essential to managing HSIN Next Gen in a disciplined and rigorous manner. Specifically, it has not implemented key process controls in the areas of

- project and acquisition planning,

- requirements development and management, and

- risk management.

Until DHS has fully implemented these controls, it increases the risk of the project operating in an ad hoc and chaotic manner—potentially resulting in increased project costs, delayed schedules, and performance shortfalls.

26

G A O
Accountability * Integrity * Reliability

Results: Objective 2
Acquisition Management Controls Needed

As we have previously reported,[11] the success of critical projects such as HSIN depends on developing and implementing a full set of acquisition management controls to effectively manage the project. Leading organizations, such as the Software Engineering Institute and the Chief Information Officer's Council, and our research and experience at federal agencies have shown that such process controls are significant in successful system acquisition and development projects. In particular, the CMMI-ACQ[12] has defined a suite of key acquisition process control areas that are necessary to manage system acquisitions in a rigorous and disciplined fashion. These process areas include

- project and acquisition planning,

- requirements development and management, and

- risk management.

The following table provides a list of key processes within each process area.

---

[11] For example, GAO-05-805 and GAO-06-444T.
[12] Carnegie Mellon Software Engineering Institute, *Capability Maturity Model® Integration for Acquisition (CMMI-ACQ),* Version 1.2 (November 2007).

27

G A O
Accountability * Integrity * Reliability

Results: Objective 2
Acquisition Management Controls Needed

Table 1: Key Processes for Effectively Managing IT Projects

Process area	Key processes
Project and acquisition planning	- developing a program office - obtaining appropriate staff, and ensuring that staff have the skills and knowledge needed to manage the project - identifying staff roles and responsibilities - identifying key deliverables and milestones for the project and acquisition
Requirements development and management	- gathering user requirements - analyzing and validating user requirements - managing any changes to the requirements in collaboration with stakeholders
Risk management	- identifying and analyzing risks - assigning responsibilities for managing risks - developing mitigation plans and completion milestones for identified risks

Source: GAO summary of leading practices, including practices identified by the Software Engineering Institute, the Chief Information Officer's Council, and the Office of Management and Budget.

28

G A O
Accountability * Integrity * Reliability

Results: Objective 2
Acquisition Management Controls Needed

DHS is currently implementing key acquisition controls for the HSIN Next Gen but it has yet to implement the full set of controls essential to effectively managing the project.

Table 2 provides a summary of the status of the project relative to each of the key process areas.

29

G A O
Accountability * Integrity * Reliability

Results: Objective 2
Acquisition Management Controls Needed

Table 2: Summary of the Status of HSIN Next Gen Acquisition Management Controls as of June 2008

Process area	Key processes	Status
Project and acquisition planning	• Establish a program office	●
	• Obtain appropriate staff	○
	• Identify staff roles and responsibilities	○
	• Identify key deliverables and milestones for project and acquisition	●
Requirement development and management	• Gather user requirements	◐
	• Analyze and validate user requirements	◐
	• Manage change to requirements	○
Risk management	• Identify and analyze risks	◐
	• Assign responsibilities for managing risks	●
	• Develop mitigation plans and completion milestones for identified risks	○

Source: GAO analysis of agency data.

● Key process area implemented   ◐ Key process area partially implemented   ○ Key process area not implemented

30

G A O
Accountability · Integrity · Reliability

Results: Objective 2
Acquisition Management Controls Needed

With regard to project and acquisition planning, DHS has implemented two of the four key processes. Specifically, it has

- established a program office for HSIN Next Gen, including filling the position of the project manager, and developed an April 2008 mission needs statement for HSIN Next Gen; and

- developed a project schedule, identifying key deliverables and milestones, for the HSIN Next Gen project and acquisition.

However, having already issued a task order to the contractor for HSIN Next Gen, the department has not filled two positions that it identified it needed to appropriately staff the program office. According to DHS officials, including the OPS CIO, they are in the process of hiring two full-time employees by the end of fiscal year 2008. In addition, the department is in the process of identifying staff roles and responsibilities, but has yet to finalize the effort.

Until the program office is adequately staffed and roles and responsibilities have been defined, DHS will be challenged in its ability to manage the HSIN Next Gen acquisition and project, including overseeing the contractor tasked to develop the system.

31

G A O
Accountability * Integrity * Reliability

Results: Objective 2
Acquisition Management Controls Needed

With regard to requirements development and management, DHS has partially implemented two of the three key processes, and has yet to implement the remaining process. Specifically, for Spiral 1, DHS has

- gathered user requirements from the critical infrastructure sector users, and

- analyzed these requirements through the OPS CIO, HSIN stakeholders, and the HSIN Mission Coordinating Committee.

The department used these user requirements, the existing HSIN requirements, and pending change requests for the current system to create the Functional Requirements Document dated March 2008. This document defines and outlines the known user requirements for HSIN Next Gen. The Functional Requirements Document was included as part of the HSIN Next Gen solicitation documentation (i.e., request for proposals) used to award the contractor in May 2008. However, while DHS has gathered and analyzed user requirements from critical infrastructure sector users, it has not gathered requirements from all other HSIN users. Moreover, DHS has yet to validate the requirements.

32

G A O
Accountability * Integrity * Reliability

Results: Objective 2
Acquisition Management Controls Needed

In addition, DHS has not developed a change control process for managing change to requirements in collaboration with stakeholders, including developing criteria for evaluation and acceptance of requirements.

DHS has efforts planned and underway to address these weaknesses. For example, the department is in the process of establishing an initiative (called the HSIN Mission Integration Effort) to improve its ability to gather user requirements by having a formal outreach process to communicate with HSIN users. According to the OPS CIO, this is part of the department's effort to improve its capability to gather requirements from HSIN users. In addition, DHS plans to validate requirements for each HSIN Next Gen phase before they are completed, which is to be by August 2008 for Spiral 1. Further, DHS plans to establish a change control board to manage HSIN Next Generation requirements by September 2008.

While these are steps in the right direction, until they are completed and DHS has fully gathered, analyzed, and validated all user requirements and implemented effective change management, it faces the risk that HSIN Next Gen will not meet user and mission needs, which is a problem it faced with the existing HSIN and why it is currently working on a replacement system.

33

G A O
Accountability * Integrity * Reliability

Results: Objective 2
Acquisition Management Controls Needed

With regard to risk management, DHS has implemented one of the key processes and part of another, and has yet to implement the remaining process. Specifically, DHS's HSIN Next Gen Acquisition Plan (dated February 2008)

- assigns responsibility for managing the risks; and

- partially identifies a list of primary risks both internal and external to the department, such as

  o insufficient funding to execute future development,

  o insufficient government staff to execute the project, and

  o changes in HSIN user requirements that could negatively impact cost and schedule.

In addition to these efforts, DHS has begun to develop a risk management plan that defines staff roles and responsibilities, including procedures for identifying and tracking risks and assessing the probability and impact of individual risks.

34

GAO
Accountability * Integrity * Reliability

Results: Objective 2
Acquisition Management Controls Needed

However, the department has yet to develop risk mitigation plans and completion milestones, which includes recommended courses of action for each critical risk. The department intends to develop such plans, which are to provide risk mitigation strategies with alternatives and mitigation project plans, including activities, schedules, and resource requirements. However, the department has yet to establish a date for when this is to be completed.

In addition, the list of primary risks prepared did not include all key risks. For example, HSIN Next Gen's schedule, which has been identified by the OPS CIO as being aggressive, has not been identified as a risk.

Until DHS fully implements and institutionalizes risk management, there is increased probability that unanticipated risks may occur that could have a critical impact on HSIN Next Gen's cost, schedule, and performance.

35

G A O
Accountability * Integrity * Reliability

Results: Objective 2
Acquisition Management Controls Needed

The OPS CIO stated that the reason for the partial implementation of these key processes is attributable in large part to an aggressive schedule for acquiring and deploying HSIN Next Gen.

In our view, engaging a contractor and commencing work before implementing mature controls is not a recipe for success. Specifically, our research and experience at federal agencies have shown that the probability of success is low using this approach. A case in fact is the existing HSIN system which was acquired and deployed via an overly aggressive schedule with the result being it did not meet all users' needs, necessitating in part the need for the HSIN Next Gen replacement.

The OPS CIO stated the department plans to address these weaknesses by, for example, tasking its contractor to assist in the development and completion of the risk management process area. However, until the processes have been implemented and institutionalized, and the full set of acquisition management controls are implemented, the project will be at increased risk of operating in an ad hoc and chaotic manner—potentially resulting in increased project costs, delayed schedules, and performance shortfalls.

36

GAO
Accountability * Integrity * Reliability

Conclusions

DHS has been challenged in its ability to efficiently and effectively manage the department's existing primary information-sharing system. In particular, although DHS has invested upwards of $70 million on the system, it still does not fully meet user needs and as a result, has not been fully utilized. DHS intends to address this performance shortfall by, among other things, acquiring a replacement system. A key challenge for DHS in this effort will be ensuring it develops an information-sharing system that effectively addresses its users' needs and in the process, does not waste or unwisely invest critical department resources.

To its credit, DHS has initiated some important steps in establishing sound and capable acquisition controls, but much remains to be accomplished before DHS management efforts can be considered effective and thereby minimize the risks associated with HSIN Next Gen delivering promised capabilities and benefits on time and within budget.

Investing money given the current state of management controls puts the project at risk. Given what is at stake, it is extremely important that DHS direct its attention to these management issues, and mitigate the associated risks as soon as possible.

37

G A O
Accountability * Integrity * Reliability

Recommendations for Executive Action

To minimize risks to the HSIN Next Gen project, we are making six recommendations to the Secretary of Homeland Security aimed at strengthening management of the project. We recommend that the Secretary direct the Director, Office of Operations Coordination and Planning to strengthen program management controls by

- staffing the program office appropriately;

- identifying staff roles and responsibilities;

- ensuring all requirements are gathered, analyzed, and validated;

- developing and implementing a requirements change control process; and

- ensuring effective risk management by identifying all key risks surrounding the project and developing risk mitigation plans and completion milestones.

We also recommend that these controls be implemented before the department starts to migrate users to HSIN Next Gen's Initial Operational Capability.

38

G A O
Accountability • Integrity • Reliability

Agency Comments and Our Evaluation

In oral comments on a draft of this briefing, DHS officials agreed with our findings and recommendations and described actions that they have underway to address our recommendations. In particular, the OPS CIO stated that they have engaged a contractor to help them organize the HSIN program office, which includes identifying staff roles and responsibilities.

DHS officials also generally agreed with our conclusions. However, they took exception with the statement in our conclusions that investing money given the current state of management controls puts the project at risk. According to DHS officials, including the OPS CIO, they believe the risks to the project are mitigated by the IT experience of the HSIN staff, including the knowledge it has gained over the past 4 years in operating, maintaining, and enhancing HSIN. While we agree that IT experience is important, our research and experience at federal agencies have shown that, in addition to people, key processes, such as rigorous and disciplined requirements and risk management, are essential to IT project success.

DHS officials also provided technical comments, which we have incorporated into the briefing as appropriate.

39

G A O
Accountability * Integrity * Reliability

To address our first objective, we

- assessed department efforts to stop HSIN system improvements by analyzing agency documentation and then discussing with agency officials via interviews. For example, we
    - reviewed executive-level correspondence, memos, strategies, and related documentation describing the department's plans for the current system, including ceasing system improvements and the reasons for doing this;
    - reviewed cost estimates to determine the planned costs of the operations and maintenance, and discussed the costs of enhancing the current system with OPS officials; and
    - interviewed OPS officials to clarify our understanding of the documentation and the department's rationale for choosing to develop the follow-on system.

- analyzed DHS plans for the proposed follow-on system. Specifically, we
    - evaluated the HSIN Next Gen acquisition plan, requirements document, request for proposals, and related documentation to determine what activities were planned and when they were to be accomplished; and
    - reviewed independent cost estimates to determine the planned costs for the development, operations, and maintenance of the new system.

40

G A O
Accountability • Integrity • Reliability

To address our second objective, we assessed the extent to which the department was managing the acquisition of HSIN Next Gen based on the processes defined in the Software Engineering Institute's Capability Maturity Model® Integration for Acquisition (CMMI-ACQ).[13] In particular, we analyzed the department's efforts in acquisition planning, requirements development and management, and risk management. In doing so, we

- assessed HSIN Next Gen acquisition and project planning documentation and interviewed OPS officials to obtain key milestones;
- reviewed the HSIN Next Gen system requirements and interviewed officials from OPS and the Office of Infrastructure Protection, and representatives from HSIN governance bodies in order to understand how requirements were gathered and managed; and
- evaluated the HSIN Next Gen risks and risk management plan, and interviewed OPS officials to understand how risks were identified and are to be managed.

---

[13]Carnegie Mellon Software Engineering Institute, *Capability Maturity Model® Integration for Acquisition (CMMI-ACQ),* Version 1.2 (November 2007).

41

G A O
Accountability • Integrity • Reliability

Attachment I
Scope and Methodology

In making these judgments, we used the following criteria: processes were
- *fully implemented* if all of the related guidance was addressed;
- *partially implemented* if some, but not all, of the related guidance was addressed; and
- *not implemented* if none of the related guidance was addressed.

We conducted our work at DHS headquarters offices in Washington, D.C., and the Office of Infrastructure Protection in Arlington, Virginia. We conducted this performance audit from January 2008 to June 2008, 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.

42

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

September 19, 2008

David A. Powner
Director, Information Technology Management Issues
U.S. Government Accountability Office

Dear Mr. Powner:

The Office of Operations Coordination and Planning (OPS) appreciates the opportunity to comment on the Government Accountability Office (GAO) report, "Information Technology: Management Improvements Needed on the Department of Homeland Security's Next Generation Information Sharing System." OPS in coordination with the DHS Office of the Chief Information Officer (OCIO) are working to establish a secure and trusted information sharing and collaboration environment for Sensitive but Unclassified (SBU) information for use by DHS and non-DHS partners engaged in preventing, protecting from, responding to, and recovering from all threats, hazards, and incidents within the authority of DHS.

The decision to upgrade the Homeland Security Information Network (HSIN) technology platform meets the growing needs of HSIN users. The current technology platform does not provide the necessary capabilities required to provide the necessary trust and interoperability. Upgrading HSIN technology addresses current user needs and provides a robust and trusted foundation adjustable over time to meet arising end user information sharing requirements. The project to upgrade the HSIN technology platform is called HSIN NextGen. It is important to understand that HSIN Next Generation (NextGen) is primarily a software upgrade to the current HSIN technology platform rather than an acquisition of a replacement system. The HSIN NextGen project, along with operations and maintenance of the current HSIN platform, is being done within the existing HSIN investment profile and does not require additional money.

The HSIN NextGen project will follow a phased implementation approach based on industry best practices. This approach allows the Department to effectively and efficiently move all current HSIN users onto an enhanced platform, constituting initial operating capability (IOC), by October, 2009. The current HSIN technology platform will remain operational throughout the phased implementation to ensure continued service for all users. Phase 1 of the HSIN NextGen project, driven by the HSIN Critical Sectors (HSIN-CS) priority requirements, was achieved on August 25, 2008.

Page 1 of 5

The following responses address the recommendations within the report:

Recommendation: Staffing the program office appropriately

OPS has advertised for a HSIN Program Requirements Manager and is working with the DHS Office of the Chief Human Capital Officer to fill this position within 60 days. Two GS-15 leadership and technical positions have been advertised and we anticipate having personnel onboard within 60 to 90 days. The HSIN Program Manager is assisted by an experienced team of professional contracting firms. The roles filled by the contractors include cost, earned value management, schedule, performance, architecture, change process, and other support functions that are typical of a program management office.

The OPS CIO plans to fill ten additional billets beginning in Fiscal Year 2009 (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.

The HSIN program is not currently staffed to support simultaneous, significant outreach initiatives to our partners. To meet this demand, DHS plans to increase overall OPS CIO Division staffing in FY09 and FY10, subject to Congressional approval of existing budget requests. 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 and focused on our Federal, State, local, and private sector partners.

Recommendation: Identifying staff roles and responsibilities

In April 2008, the OPS CIO initiated an effort by an outside team to analyze the current OPS CIO Division, which includes HSIN Program Management. This effort provided recommendations for transforming the OPS CIO Division and enable DHS to more effectively meet its complex, integrated mission requirements, both within DHS and across the larger homeland security community. The team conducted extensive research and performed over thirty-five interviews with OPS CIO staff, OPS stakeholders, and DHS-wide leaders. Then, the team applied proven analytical methods to form strategic and tactical views of organization, examining the CIO functions and capabilities it requires for the future. In addition, the team conducted a detailed, bottom-up assessment of existing capabilities and supporting activities.
Four key areas were analyzed:

- **Process**: Develop an understanding of the existing and future processes including functions, tasks and activities needed to perform the mission of the OPS CIO Division
- **People**: Develop an understanding of the existing and future staff and expertise needed to support the mission and processes of the OPS CIO Division

Page 2 of 5

- **Technology**: Develop an understanding of the existing and future technologies including applications, data and technology standards needed to perform the mission of the OPS CIO Division
- **Physical Infrastructure**: Develop an understanding of the existing, future facilities and working environment needed to perform the mission of the OPS CIO Division

The recommendation for the future state of the OPS CIO Division includes a detailed description of the organization model, including the processes, people, technology and infrastructure required, to implement the recommended organization.

Recommendation: Ensuring all requirements are gathered, analyzed, and validated

User requirements were the primary driver of the decision to upgrade the HSIN environment. These are not the only driver of the process. Initial phases will not meet every user requirement. The prioritization of certain user requirements is necessary. The Department must set timeline milestones in addition to identifying user requirements. This ensures that the awarded task order is completed in a timely manner, while initially ensuring that the Department meets the most urgent system requirements. Phases 1 through 3 of the HSIN NextGen project address the user needs to provide a secure and trusted information sharing and collaboration platform.

The Department determined that the HSIN NextGen project must first address the security and trust requirements identified through HSIN Community of Interest (COI) owners' input. Based upon input from many of the HSIN Community of Interest (COI) owners, the Department determined that the HSIN NextGen project must first address the security and trust requirements identified by all COIs. State, local and tribal first responders have reached out to the Department by requesting changes and sending requirements through the HSIN Helpdesk and/ or through the HSIN Mission Advocates. These change requests and requirements were recorded in the HSIN Change Request Tracking System (CHARTS). Many change requests were made by HSIN-CS and State, local, or tribal users. All change requests and requirements were examined and where possible incorporated into the HSIN NextGen Functional Requirements Document (FRD). The operational user requirements, which include policy, business process, and governance, will be gathered through identified DHS business leads and the HSIN Outreach Team.

Using a best practices approach, the HSIN Mission Integration Effort will gather user requirements and establish on-the-ground relationships through HSIN representatives (Mission Advocates). 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 further the understanding of the Commonwealth's information sharing needs and aid to support the Department partners' homeland security mission. In the future, the Department will engage with more partners to further examine the needs of our State, local, tribal and Federal partners.

The Department further determined that the most time sensitive and pressing needs of the existing HSIN COIs were those of the HSIN Critical Sectors (HSIN-CS). HSIN-CS provides a common environment for the critical infrastructure/key resource (CI/KR) stakeholder partners. NPPD has gathered and validated necessary user requirements for this phase from their

Page 3 of 5

stakeholders over a two year period. The critical infrastructure/key resource community is a well governed and defined community. The National Protection and Programs Directorate, Office of Infrastructure Protection (NPPD/IP), has determined that implementing the HSIN-CS priority requirements at the earliest moment was an absolute necessity to avoid mission degradation and loss of the voluntary participation of the 18 infrastructure sectors.

Recommendation: Developing and Implementing a requirements change control process

There must be one overarching requirements process that brings business, functional and technical architecture products into alignment. This is a complex undertaking, given the necessity for interoperability, as well as the depth, breadth, and volunteer nature of potential HSIN user groups. The phased approach to migrating communities onto the upgraded HSIN environment mitigates many risks.

The HSIN NextGen project will make the HSIN environment responsive and flexible to user requirements through a single, well-designed requirements process. The diversity of customer requirements and the need for a more standards-based platform, responsive to changing user requirements, is a driver for the HSIN NextGen project. The use of the maturing governance structure will ensure customer needs are met. The Information Sharing Governance Board (ISGB), along with the Information Sharing Coordinating Council (ISCC) and other mission coordination bodies, will work with the HSIN Program Manager to make certain that the requirements are captured, reviewed, and, if appropriate, implemented into the HSIN program change management process. DHS will adapt its tactics and timeline as needed using the phased deployment strategy and a segment architecture approach.

Future phases of HSIN NextGen will create improved versions based upon continued input from HSIN users. Currently, and moving forward in future phases, improvements to HSIN have been and will continue to be driven by the input of Federal, State, local, private sector, and tribal users with each phase improving upon the last. We anticipate that once HSIN users have a chance to understand and use the upgraded HSIN capabilities, they will suggest additional improvements or enhancements. These requests will translate into requirements to be submitted into the HSIN change management process and then incorporated into subsequent phases of the HSIN NextGen project.

To ensure success, a governance structure was initiated that integrated a larger segment architecture framework and the phased implementation approach. This structure continues to evolve to ensure that all stakeholders are involved and end user requirements are accurately captured, vetted, managed, and implemented. Key program activities and decisions are guided by DHS policies, processes, and procedures for consistency, repeatability, and compliance. The HSIN governance structure allows HSIN program resources to engage with mission leaders from all segments to determine whether HSIN is an appropriate solution for that target segment. If so, the governance structure allows us to identify mission requirements of that segment community and determine whether HSIN can meet those requirements in a timely, cost effective manner. The Department will move forward with the implementation of additional capabilities for new or existing mission areas based on whether HSIN can meet those requirements in a timely, cost

Page 4 of 5

effective manner. Once that determination is made, additional capabilities will be designed, developed, and validated with participation from stakeholders.

Recommendation: Ensuring effective risk management by identifying all key risks surrounding the project and developing risk mitigation plans and completion milestones

The HSIN Program Team exercises a proactive approach to risk. OPS identifies and mitigate risks before they manifest as schedule slippage, cost overruns, and unsatisfied requirements. Our risk management approach incorporates a continuing, closed-loop review and analysis of technical, programmatic, cost, and schedule risks throughout the entire program lifecycle. OPS uses proven management toolsets for detailed documentation and tracking of all identified risks/problems from point of discovery through risk resolution (e.g. web portals to facilitate user entry, tracking, reporting and maintenance of a centralized repository for all deliverables and product information). Our risk management approach monitors overall program health to ensure goals are being met. The Risk Management Plan consists of the following key areas:

- **Risk Identification:** Project managers are responsible for proactively identifying and documenting potential problems, issues, risks and dependencies at every program level
- **Risk Reporting:** Project managers conduct regular issue/risk review meetings to ensure risks are reported appropriately and in a timely manner. Prior to the internal program review (IPR), probability-of-occurrence and consequence-of-failure analyses are conducted to quantify and rank all identified risks
- **Risk Mitigation Strategy:** In addition to routine risk reporting, project manager are responsible for mitigation strategies for every risk that is identified. Impacted areas and/or systems, resources and skills required, as well as potential level of effort to provide resolution, are captured in the strategy
- **Risk Escalation:** Risks ranked high and medium may require special attention and/or action plans for mitigation, thus the overall Risk Management plans include an escalation path based on risk category and impacted area

I look forward to working with you to ensure that user communities that depend upon HSIN are able to accomplish their missions. If I may be of further assistance, please contact my office.

Sincerely,

Roger T. Rufe, Jr.

Page 5 of 5

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

David A. Powner, (202) 512-9286 or pownerd@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff also made key contributions to this report: Gary Mountjoy, Assistant Director; Barbara Collier; Kaelin Kuhn; Rebecca LaPaze; and Lori Martinez.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548