



Testimony

Before the Subcommittee on Intelligence,  
Information Sharing and Terrorism Risk  
Assessment, Committee on Homeland  
Security, House of Representatives

---

For Release on Delivery  
Expected at 10 a.m. EDT  
Thursday, May 10, 2007

INFORMATION  
TECHNOLOGY

Homeland Security  
Information Network  
Needs to Be Better  
Coordinated with Key  
State and Local Initiatives

Statement of David A. Powner, Director  
Information Technology Management Issues



G A O

Accountability \* Integrity \* Reliability

---

---

---

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

---



Highlights of [GAO-07-822T](#), a report to Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, Homeland Security Committee, House of Representatives

## 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, the private sector, and the public. In support of its mission, the department has deployed a Web-based information-sharing application—the Homeland Security Information Network (HSIN)—and operates at least 11 homeland security networks. The department reported that in fiscal years 2005 and 2006, these investments cost \$611.8 million to develop, operate, and maintain.

In view of the significance of information sharing for protecting homeland security, GAO was asked to testify on the department's efforts to coordinate its development and use of HSIN with two key state and local initiatives under the Regional Information Sharing Systems—a nationwide information-sharing program operated and managed by state and local officials.

This testimony is based on a recent GAO report that addresses, among other things, DHS's homeland security networks and HSIN. In performing the work for that report, GAO analyzed documentation on HSIN and state and local initiatives, compared it against the requirements of the Homeland Security Act and federal guidance and best practices, and interviewed DHS officials and state and local officials.

[www.gao.gov/cgi-bin/getrpt?GAO-07-822T](http://www.gao.gov/cgi-bin/getrpt?GAO-07-822T).

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Powner at (202) 512-9286 or [pownerd@gao.gov](mailto:pownerd@gao.gov).

## INFORMATION TECHNOLOGY

# Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives

## What GAO Found

In developing HSIN, its key homeland security information-sharing application, DHS did not work effectively with two key Regional Information Sharing Systems program initiatives. This program, which is operated and managed by state and local officials nationwide, provides services to law enforcement, emergency responders, and other public safety officials. However, DHS did not coordinate with the program to fully develop joint strategies and policies, procedures, and other means to operate across agency boundaries, which are key practices for effective coordination and collaboration and a means to enhance information sharing and avoid duplication of effort. For example, DHS did not engage the program in ongoing dialogue to determine how resources could be leveraged to meet mutual needs.

A major factor contributing to this limited coordination was that the department rushed to deploy HSIN after the events of September 11, 2001. In its haste, it did not develop a comprehensive inventory of key state and local information-sharing initiatives, and it did not achieve a full understanding of the relevance of the Regional Information Sharing Systems program to homeland security information sharing.

As a result, DHS faces the risk that effective information sharing is not occurring and that HSIN may be duplicating state and local capabilities. Specifically, both HSIN and one of the Regional Information Sharing Systems initiatives target similar user groups, such as emergency management agencies, and all have similar features, such as electronic bulletin boards, "chat" tools, and document libraries.

The department has efforts planned and under way to improve coordination and collaboration, including developing an integration strategy to allow other applications and networks to connect with HSIN, so that organizations can continue to use their preferred information-sharing applications and networks. In addition, it has agreed to implement recommendations made by GAO to take specific steps to (1) improve coordination, including developing a comprehensive inventory of state and local initiatives, and (2) ensure that similar coordination and duplication issues do not arise with other federal homeland security networks, systems, and applications. Until DHS completes these efforts, including developing an inventory of key state and local initiatives and fully implementing and institutionalizing key practices for effective coordination and collaboration, the department will continue to be at risk that information is not being effectively shared and that the department is duplicating state and local capabilities.



---

Madame Chair and Members of the Subcommittee:

I appreciate the opportunity to be here today to discuss challenges facing the Department of Homeland Security (DHS) in coordinating efforts on its Homeland Security Information Network (HSIN) with state and local governments and other parties involved in the mission of keeping our nation secure. As you know, 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 developed HSIN as part of its goal to establish an infrastructure for sharing homeland security information.<sup>1</sup> Besides HSIN, an Internet-based application, DHS also operates at least 11 other networks in support of its homeland security mission. The department reported that in fiscal years 2005 and 2006, these investments cost \$611.8 million to develop, operate, and maintain.

As agreed, in my remarks today I will discuss the department's efforts to coordinate its development and use of HSIN with key state and local information-sharing initiatives. These remarks are based on our recent report on homeland security networks and applications.<sup>2</sup> That report focused on two key initiatives under the Regional Information Sharing Systems program. This nationwide program, operated and managed by state and local officials, provides services (including information sharing) to support law enforcement and criminal justice agencies. Its information-sharing efforts also include emergency responders and public safety officials.

In performing the work for the report, we analyzed descriptive data (e.g., type of network, estimated costs) on major networks and Internet-based systems identified by DHS as supporting its

---

<sup>1</sup> 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.

<sup>2</sup> 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.: Apr. 16, 2007).

---

homeland security mission, including information sharing. We also reviewed documentation on HSIN and state and local initiatives; compared it against the requirements of the Homeland Security Act, federal guidance, and related best practices; and interviewed DHS officials and state and local officials. This work was performed in accordance with generally accepted government auditing standards.

---

## Results in Brief

In developing HSIN, DHS did not effectively coordinate with key state and local initiatives that are part of the Regional Information Sharing Systems program. Specifically, the department did not fully develop joint strategies and coordinated policies, procedures, and other means to operate across agency boundaries and meet mutual needs, which are key practices for effective coordination and collaboration and are a means to enhance information sharing and avoid duplication of effort. For example, DHS did not engage the program in ongoing dialogue to determine how resources could be leveraged to meet mutual needs or work through technical issues and differences in what each organization considers to be terrorism information.

A major factor contributing to the limited coordination was that after September 11, 2001, the department expedited its schedule for deploying HSIN. In its haste, it did not develop a comprehensive inventory of key state and local information-sharing initiatives.

Consequently, DHS faces the risk that effective information sharing is not occurring. It also faces the risk that the HSIN system may be duplicating state and local capabilities. Specifically, both HSIN and one of the key initiatives target similar user groups, such as emergency management agencies, and all have similar features, such as Web portals,<sup>3</sup> electronic bulletin boards, “chat” tools, and document libraries.

---

<sup>3</sup> A Web portal is generally a site that offers several resources or services, such as search engines, news articles, forums, and other tools.

---

The department has efforts planned and under way to improve coordination and collaboration. For example, it is forming an HSIN Mission Coordinating Committee and an HSIN Advisory Committee to help ensure that HSIN meets the information-sharing needs of DHS and other users. However, these activities have either just begun or are being planned, with implementation milestones yet to be defined. In addition to the planned improvements, DHS has agreed to implement our recommendations to take steps to ensure that HSIN is effectively coordinated with key state and local government information-sharing initiatives, which include identifying and inventorying such initiatives. We also recommended that DHS determine whether there are coordination and duplication issues with its other homeland security networks and associated systems and applications. Until DHS completes these activities, including developing an inventory of key state and local initiatives, and fully implementing and institutionalizing key practices and guidance for effective coordination and collaboration, it will continue to be at risk of not effectively sharing information with other key state and local information initiatives and duplicating state and local capabilities.

---

## 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,<sup>4</sup> 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.

---

<sup>4</sup> Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (Nov. 25, 2002).

As we have previously reported, DHS relies extensively on information technology (IT), such as networks and associated system applications, to carry out its mission.<sup>5</sup> Specifically, in our recent report, we reported that the department identified 11 major networks it uses to support its homeland security functions, including sharing information with state and local governments.<sup>6</sup> Examples of such DHS networks include the Homeland Secure Data Network, the Immigration and Customs Enforcement Network, and the Customs and Border Protection Network. In addition, the department has deployed HSIN, a homeland security information-sharing application that operates on the public Internet. As shown in table 1, of the 11 networks, 1 is categorized as Top Secret, 1 is Secret, 8 are Sensitive but Unclassified, and 1 is unclassified. HSIN is considered Sensitive but Unclassified.

**Table 1: DHS Information-Sharing Networks and HSIN Application**

Name	Categories	Users outside DHS	Reported cost per fiscal year (dollars in millions)		
			2005	2006	Total
C Local Area Network (C-LAN)	Top Secret	—	(a)	(a)	—
Homeland Secure Data Network (HSDN)	Secret	Other federal, state, local	\$46.2	\$32.6	\$78.8
Coast Guard Data Network Plus (CGDN+)	Sensitive but Unclassified	Other federal	15.0	15.0	30.0
Critical Infrastructure Warning Information Network (CWIN)	Sensitive but Unclassified	Other federal, state	12.1	12.0	24.1
Customs and Border Protection (CBP) Network	Sensitive but Unclassified	—	58.7	63.0	121.7
DHS Core Network (DCN)	Sensitive but Unclassified	—	13.4	10.3	23.7
Homeland Security Information Network (HSIN)	Sensitive but Unclassified	Other federal, state, local	11.9	20.5	32.4
Immigration and Customs Enforcement Network (ICENet)	Sensitive but Unclassified	Other federal, state, local	14.4	19.2	33.6
ONENet	Sensitive but Unclassified	—	34.6	40.0	74.6
Secret Service Wide Area Network (WAN)	Sensitive but Unclassified	—	2.8	3.1	5.9

<sup>5</sup> See, for example, GAO, *Information Technology: Major Federal Networks That Support Homeland Security Functions*, GAO-04-375 (Washington, D.C.: Sept. 17, 2004) and *Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments*, GAO-07-424 (Washington, D.C.: April 27, 2007).

<sup>6</sup> GAO-07-455.



Name	Categories	Users outside DHS	Reported cost per fiscal year (dollars in millions)		
			2005	2006	Total
Transportation Security Administration Network (TSANet)	Sensitive but Unclassified	Other federal	70.0	105.0	175.0
Federal Emergency Management Agency (FEMA) Switched Network	Unclassified	—	6.0	6.0	12.0
<b>Total<sup>a</sup></b>			<b>\$285.1</b>	<b>\$326.7</b>	<b>\$611.8</b>

Source: GAO analysis of agency data.

<sup>a</sup>Costs for C-LAN are not included, as the information is not publicly available.

As the table shows, some of these networks are used solely within DHS, while others are also used by other federal agencies, as well as state and local governments. In addition, the total cost to develop, operate, and maintain these networks and HSIN in fiscal years 2005 and 2006, as reported by DHS, was \$611.8 million. Of this total, the networks accounted for the vast majority of the cost: \$579.4 million.

## DHS Established HSIN to Provide Information-Sharing Capabilities

DHS considers HSIN to be its primary communication application for transmitting sensitive but unclassified information. According to DHS, this network is an encrypted, unclassified, Web-based communications application that serves as DHS's primary nationwide information-sharing and collaboration tool. It is intended to offer 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 application are suspicious incident and pre-incident information and analysis of terrorist threats, tactics, and weapons. The application is managed within DHS's Office of Operations Coordination.

HSIN includes over 35 communities of interest, such as emergency management, law enforcement, counterterrorism, individual states, and private sector communities. 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. The community Web pages also provide access to other resources, such as the following:

- *Document library.* Users can search the entire document library within the communities they have access to.

- 
- *Discussion threads.* HSIN has a discussion thread (or bulletin board) feature that allows users to post information that other users should know about and post requests for information that other users might have. Community administrators can also post and track tasks assigned to users during an incident.
  - *Chat tool.* HSIN's chat tool, known as Jabber, is similar to other instant message and chat tools—with the addition of security. Users can customize lists of their coworkers and send messages individually or set up chat rooms for more users. Other features include chat logs (which allow users to review conversations), timestamps, and user profiles.

---

## States and Local Governments Have Also Established Similar Initiatives

State and local governments have similar IT initiatives to carry out their homeland security missions, including sharing information. A key state and local-based initiative is the Regional Information Sharing Systems (RISS) program.

The RISS program helps state and local jurisdictions to, among other things, share information in support of their homeland security missions. This nationwide program, operated and managed by state and local officials, was established in 1974 to address crime that operates across jurisdictional lines. The program consists of six regional information analysis centers that serve as regional hubs across the country. These centers offer services to RISS members in their regions, including information sharing and research, analytical products, case investigation support, funding, equipment loans, and training. Funding for the RISS program is administered through a grant from the Department of Justice.

As part of its information-sharing efforts, the RISS program operates two key initiatives (among others): the RISS Secure Intranet (RISSNET) and the Automated Trusted Information Exchange<sup>7</sup> (RISS ATIX):

---

<sup>7</sup> Formerly called the Anti-Terrorism Information Exchange.

- 
- Created in 1996, RISSNET is intended as a secure network serving member law enforcement agencies throughout the United States and other countries. Through this network, RISS offers services such as secure e-mail, document libraries, intelligence databases, Web pages, bulletin boards, and a chat tool.
  - RISS ATIX offers services similar to those offered by RISSNET to agencies beyond the law enforcement community, including executives and officials from governmental and nongovernmental agencies and organizations that have public safety responsibilities. RISS ATIX is partitioned into 39 communities of interest, such as critical infrastructure, emergency management, public health, and government officials. Members of each community of interest contribute information to be made available within each community.

According to RISS officials, the RISS ATIX application was developed in response to the events of September 11, 2001; it was initiated in 2002 as an application to provide tools for information sharing and collaboration among public safety stakeholders, such as first responders and schools. As of July 2006, RISS ATIX supported 1,922 users beyond the traditional users of RISSNET.

RISS ATIX uses the technology of RISSNET to offer services through its Web pages. The pages are tailored for each community of interest and contain community-specific news articles, links, and contact information. The pages also provide access to the following features:

- *Document library.* Participants can store and search relevant documents within their community of interest.
- *Bulletin board.* The RISS ATIX bulletin board allows users to post timely threat information in discussion forums and to view and respond to posted information. Users can post documents, images, and information related to terrorism and homeland security, as well as receive DHS information, advisories, and warnings. According to RISS officials, the bulletin boards are monitored by a RISS moderator to relay any information that might be useful for other communities of interest.

- 
- *Chat tool.* ATIXLive is an online, real-time, collaborative communications information-sharing tool for the exchange of information by community members. Through this tool, users can post timely threat information and view and respond to messages posted.
  - *Secure e-mail.* RISS ATIX participants have access to e-mail that can be used to provide alerts and related information. According to RISS, this is done in a secure environment.

---

## GAO Has Designated Information Sharing as High Risk

The need to improve information sharing as part of a national effort to improve homeland security and preparedness has been widely recognized, not only to improve our ability to anticipate and respond to threats and emergencies, but to avoid unnecessary expenditure of scarce resources. In January 2005,<sup>8</sup> and more recently in January 2007,<sup>9</sup> we identified establishing appropriate and effective information-sharing mechanisms to improve homeland security as a high-risk area. The Office of Management and Budget (OMB) has also issued guidance that stresses the importance of information sharing and avoiding duplication of effort.<sup>10</sup> Nonetheless, although this area has received increased attention, the federal government faces formidable challenges in sharing information among stakeholders in an appropriate and timely manner.

As we concluded in October 2005, agencies can help address these challenges by adopting and implementing key practices, related to OMB's guidance, to improve collaboration, such as establishing joint strategies and addressing needs by leveraging resources and developing compatible policies, procedures, and other means to operate across agency boundaries.<sup>11</sup> Based on our research and

---

<sup>8</sup> GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

<sup>9</sup> GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

<sup>10</sup> For example, Office of Management and Budget, *Management of Federal Information Resources*, Circular A-130 (Washington, D.C.: Nov. 30, 2000) and *Preparation, Submission, and Execution of the Budget*, Circular A-11 (Washington, D.C.: June 30, 2006).

<sup>11</sup> GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: October 2005).

---

experience, these practices are also relevant for collaboration between federal agencies and other levels of government (e.g., state, local). Until these coordination and collaboration practices are implemented, agencies face the risk that effective information sharing will not occur.

Congress and the Administration have made several efforts to address the challenges associated with information sharing. In particular, as we reported in March 2006, the President initiated an effort to establish an Information Sharing Environment that is to combine policies, procedures, and networks and other technologies that link people, systems, and information among all appropriate federal, state, local, and tribal entities and the private sector.<sup>12</sup> In November 2006, in response to congressional direction, the Administration issued a plan for implementing this environment and described actions that the federal government intends—in coordination with state, local, tribal, private sector, and foreign partners—to carry out over the next 3 years.

---

## Efforts to Coordinate HSIN with Key State and Local Information-Sharing Initiatives Have Been Limited

DHS did not fully adhere to the previously mentioned key practices in coordinating its efforts on HSIN with key state and local information-sharing initiatives. The department's limited use of these practices is attributable to a number of factors: in particular, after the events of September 11, 2001, the department expedited its schedule to deploy HSIN capabilities, and in doing so, it did not develop an inventory of key state and local information initiatives. Until the department fully implements key coordination and collaboration practices and guidance, it faces, among other things, the risk that effective information sharing is not occurring. DHS has efforts planned and under way to improve coordination and

---

<sup>12</sup> GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: March 2006).

---

collaboration, including implementing the recommendations in our recent report.<sup>13</sup>

---

## Key Practices Were Not Effectively Implemented

In developing HSIN, DHS did not fully adhere to the practices related to OMB's guidance. First, although DHS officials met with RISS program officials to discuss exchanging terrorism-related documents, joint strategies for meeting mutual needs by leveraging resources have not been fully developed. DHS did not engage the RISS program to determine how resources could be leveraged to meet mutual needs. According to RISS program officials, they met with DHS twice (on September 25, 2003, and January 7, 2004) to demonstrate that their RISS ATIX application could be used by DHS for sharing homeland security information. However, communication from DHS on this topic stopped after these meetings, without explanation. According to DHS officials, they did not remember the meetings, which they attributed to the departure from DHS of the staff who had attended.

In addition, although DHS initially pursued a limited strategy of exchanging selected terrorism-related documents with the RISS program, the strategy was impeded by technical issues and by differences in what each organization considers to be terrorism information. For example, the exchange of documents between HSIN and the RISS program stopped on August 1, 2006, because of technical problems with HSIN's upgrade to a new infrastructure. As of May 3, 2007, the exchange of terrorism-related documents had not yet resumed, according to HSIN's program manager. This official also stated that the program is currently working to fix the issue with the goal of having it resolved by June 2007.

Finally, DHS has yet to fully develop coordination policies, procedures, and other means to operate across agency boundaries with the RISS program. DHS has not fully developed such means to operate with the RISS program and leverage its available technological resources. Although an operating agreement was

---

<sup>13</sup> GAO-07-455.

---

established to govern the exchange of terrorism-related documents, according to RISS officials, it did not cover the full range of information available through the RISS program.

---

### DHS's Expedited Schedule Was Major Cause for Limited Coordination, Increasing the Risk of Ineffective Information Sharing and Duplication

The extent of DHS's adherence to key practices (and the resulting limited coordination) is attributable to DHS's expedited schedule to deploy an information-sharing application that could be used across the federal government in the wake of the September 11 attacks; in its haste, DHS did not develop a complete inventory of key state and local information initiatives. According to DHS officials, they still do not have a complete inventory of key state and local information-sharing initiatives. DHS's Office of Inspector General also reported that DHS developed HSIN in a rapid and ad hoc manner, and among other things, did not adequately identify existing federal, state, and local resources, such as RISSNET, that it could have leveraged.<sup>14</sup>

Further, DHS did not fully understand the RISS program. Specifically, DHS officials did not acknowledge the RISS program as a state and local based program with which to partner, but instead considered it to be one of many vendors providing a tool for information sharing. In addition, DHS officials believed that the RISS program was solely focused on law enforcement information and did not capture the broader terrorism-related or other information of interest to the department.

Because of this limited coordination and collaboration, DHS is at increased risk that effective information sharing is not occurring. The department also faces the risk that it is developing and deploying capabilities on HSIN that duplicate those being established by state and local agencies. There is evidence that this has occurred with respect to the RISS program. Specifically:

---

<sup>14</sup> Department of Homeland Security Office of Inspector General, Office of Information Technology, *HSIN Could Support Information Sharing More Effectively*, DHS/OIG-06-38 (Washington, D.C.: June 2006).

- 
- HSIN and RISS ATIX currently target similar user groups. DHS and the RISS program are independently striving to make their applications available to user communities involved in the prevention of, response to, mitigation of, and recovery from terrorism and disasters across the country. For example, HSIN and RISS ATIX are being used and marketed for use at state fusion centers<sup>15</sup> and other state organizations, such as emergency management agencies across the country.
  - HSIN and RISS applications have similar approaches for sharing information with their users. For example, on each application, users from a particular community—such as emergency management—have access to a portal or community area tailored to the user’s information needs. The community-based portals have similar features focused on user communities. Both applications provide each community with the following features:<sup>16</sup>
    - *Web pages.* Tailored for communities of interest (e.g., law enforcement, emergency management, critical infrastructure sectors), these pages contain general and community-specific news articles, links, and contact information.
    - *Bulletin boards.* Participants can post and discuss information.
    - *Chat tool.* Each community has its own online, real-time, interactive collaboration application.
    - *Document library.* Participants can store and search relevant documents.

---

<sup>15</sup> A fusion center is defined as a “collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.”

<sup>16</sup> Beyond the collaboration tools listed, RISSNET also provides access to other law enforcement resources, such as analytical criminal data-visualization tools and criminal intelligence databases.



---

---

## DHS Has Improvements Planned and Under Way, Including Implementing Our Recent Recommendations

According to DHS officials, including the HSIN program manager, the department has efforts planned and under way to improve coordination. For example, the department is in the process of developing an integration strategy that is to include enhancing HSIN so that other applications and networks can interact with it. This would promote integration by allowing other federal agencies and state and local governments to use their preferred applications and networks—such as RISSNET and RISS ATIX—while allowing DHS to continue to use HSIN.

Other examples of improvements either begun or planned include the following:

- The formation of an HSIN Mission Coordinating Committee, whose roles and responsibilities are to be defined in a management directive. It is expected to ensure that all HSIN users are coordinated in information-sharing relationships of mutual value.
- The recent development of engagement, communications, and feedback strategies for better coordination and communication with HSIN, including, for example, enhancing user awareness of applicable HSIN contact points and changes to the system.
- The reorganization of the HSIN program management office to help the department better meet user needs. According to the program manager, this reorganization has included the use of integrated process teams to better support DHS's operational mission priorities as well as the establishment of a strategic framework and implementation plan for meeting the office's key activities and vision.
- The establishment of a HSIN Advisory Committee to advise the department on how the HSIN program can better meet user needs, examine DHS's processes for deploying HSIN to the states, assess state resources, and determine how HSIN can coordinate with these resources.

---

In addition to these planned improvements, DHS has agreed to implement the recommendations in our recent report. Specifically, we recommended that the department ensure that HSIN is effectively coordinated with key state and local government information-sharing initiatives. We also recommended that this include (1) identifying and inventorying such initiatives to determine whether there are opportunities to improve information sharing and avoid duplication, (2) adopting and institutionalizing key practices related to OMB's guidance on enhancing and sustaining agency coordination and collaboration, and (3) ensuring that the department's coordination efforts are consistent with the Administration's recently issued Information Sharing Environment plan.<sup>17</sup> In response to these recommendations, DHS described actions it was taking to implement them. (The full recommendations and DHS's written response to them are in report.)

---

In closing, DHS has not effectively coordinated its primary information-sharing system with two key state and local initiatives. Largely because of the department's hasty approach to delivering needed information-sharing capabilities, it did not follow key coordination and collaboration practices and guidance or invest the time to inventory and fully understand how it could leverage state and local approaches. Consequently, the department faces the risk that effective information sharing is not occurring and that its HSIN application may be duplicating existing state and local capabilities. This also raises the issue of whether similar coordination and duplication issues exist with the other federal homeland security networks and associated systems and applications under the department's purview.

DHS recognizes these risks and has improvements planned and under way to address them, including stated plans to implement our recommendations. These are positive steps and should help address

---

<sup>17</sup> As mentioned earlier, this plan is aimed at establishing, in 3 years, the networks and other technologies that link people, systems, and information among all appropriate federal state, local, and tribal entities and the private sector.

---

shortfalls in the department's coordination practices on HSIN. However, these actions have either just begun or are planned, with milestones for implementation yet to be defined. Until all the key coordination and collaboration practices are fully implemented and institutionalized, DHS will continue to be at risk that the effectiveness of its information sharing is not where it needs to be to adequately protect the homeland and that its efforts are unnecessarily duplicating state and local initiatives.

Madame Chair, this concludes my testimony today. I would be happy to answer any questions you or other members of the subcommittee may have.

---

## Contacts and Acknowledgements

If you have any questions concerning this testimony, please contact David Powner, Director, Information Technology Management Issues, at (202) 512-9286 or [pownerd@gao.gov](mailto:pownerd@gao.gov). Other individuals who made key contributions include Gary Mountjoy, Assistant Director, Barbara Collier; Joseph Cruz; Matthew Grote; and Lori Martinez.