United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2012

INFORMATION SHARING

DHS Has Demonstrated Leadership and Progress, but Additional Actions Could Help Sustain and Strengthen Efforts

GAO-12-809

GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-12-809, a report to congressional requesters

September 2012

INFORMATION SHARING

DHS Has Demonstrated Leadership and Progress, but Additional Actions Could Help Sustain and Strengthen Efforts

Why GAO Did This Study

Recent planned and attempted acts of terrorism on U.S. soil underscore the importance of the need to ensure that terrorism-related information is shared with stakeholders across all levels of government in an effective and timely manner. DHS, through its Office of Intelligence and Analysis, has responsibility for sharing this information and has established an information-sharing vision for 2015—which includes ensuring that the right information gets to the right people at the right time. GAO was asked to examine the extent to which DHS (1) has made progress in achieving its information-sharing mission, and (2) tracks and assesses information-sharing improvements. GAO analyzed relevant DHS documents, such as strategic planning documents and those related to DHS's governance structure, among others, and interviewed DHS officials.

What GAO Recommends

GAO recommends that DHS revise its policies and guidance to include processes for identifying information-sharing gaps, analyzing root causes of those gaps, and identifying, assessing, and mitigating risks of removing incomplete initiatives from its list; better track and assess the progress of key information-sharing initiatives; and establish the level of capabilities programs must implement to meet its vision for 2015. DHS agreed with these recommendations and identified actions taken or planned to implement them.

View GAO-12-809. For more information, contact Eileen Larence at (202) 512-6510 or larencee@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) has made progress in achieving its information-sharing mission, but could take additional steps to improve its efforts. Specifically, DHS has demonstrated leadership commitment by establishing a governance board to serve as the decision-making body for DHS information-sharing issues. The board has enhanced collaboration among DHS components and identified a list of key information-sharing initiatives. The board has also developed and documented a process to prioritize some of the initiatives for additional oversight and support. However, because DHS has not revised its policies and guidance to include processes for identifying information-sharing gaps and the results; analyzing root causes of those gaps; and identifying, assessing, and mitigating risks of removing incomplete initiatives from its list, it does not have an institutional record that would help it replicate and sustain those information-sharing efforts. Overall, DHS's key information-sharing initiatives have progressed, and most have met interim milestones. However, progress has slowed for half of the 18 key initiatives, in part because of funding constraints. For example, 5 of DHS's top 8 priority information-sharing initiatives currently face funding shortfalls. The board has not been able to secure additional funds for these initiatives because they ultimately compete for funding within the budgets of individual components, but DHS officials noted that the board's involvement has kept some initiatives from experiencing funding cuts. DHS is also developing plans that will be important in managing its information-sharing efforts, such as a revised strategy for information sharing and a related implementation plan.

DHS has taken steps to track its information-sharing efforts, but has not yet fully assessed how they have improved sharing. Specifically, DHS is tracking the implementation progress of key information-sharing initiatives, but the department does not maintain completion dates and does not fully assess the impact initiatives are having on sharing. Determining and documenting initiative completion dates and how initiatives affect sharing, where feasible, would help the board better track progress in implementing the initiatives and make any necessary course corrections if completion dates are delayed. Further, DHS has begun to assess the extent to which its technology programs, systems, and initiatives—which include the key information-sharing initiatives—have implemented critical information-sharing capabilities, such as secure user access authorization. However, DHS has not yet determined the specific capabilities each particular program must implement for DHS to conclude that it has improved information sharing enough to achieve its information-sharing vision for 2015. Establishing the level of capabilities programs must implement could help DHS prioritize programs, and track and assess progress toward its vision. In addition, DHS is in the process of implementing customer feedback measures on the usefulness of information provided and has taken steps to assess customers' information needs. DHS has not yet developed measures that determine the impact of its information-sharing efforts on homeland security, but plans to develop ways to assess information-sharing results toward achieving its 2015 vision. DHS's time frames for completing this effort are to be included in forthcoming plans currently being developed.

Contents

Table

Figures

Abbreviations

AWN	Alerts, Warnings, and Notifications
CBP	Customs and Border Protection
CHISE	Controlled Homeland Information Sharing Environment
CIO	Chief Information Officer
DHS	Department of Homeland Security
DOJ	Department of Justice
EA	enterprise architecture
FBI	Federal Bureau of Investigation
HSIN	Homeland Security Information Network
I&A	Office of Intelligence and Analysis
ICE	Immigration and Customs Enforcement
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISE	Information Sharing Environment
LEISI	Law Enforcement Information Sharing Initiative
NCTC	National Counterterrorism Center
QHSR	*Quadrennial Homeland Security Review*
SAR	Suspicious Activity Reporting

G A O
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 18, 2012

Congressional Requesters

Recent planned and attempted acts of terrorism on U.S. soil underscore the importance of ensuring that terrorism-related information is shared with stakeholders across all levels of government, the private sector, and foreign countries in an effective and timely manner.[1] Consistent with the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) and the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act), among other statutes, the Department of Homeland Security (DHS) has responsibility for sharing terrorism-related information with federal, state, local, tribal, territorial, international, and private sector partners.[2] DHS is also one of five key agencies tasked with responsibilities related to establishing the Information Sharing Environment (ISE)—a statutorily mandated governmentwide approach to facilitate the sharing of terrorism-related information.

We have designated terrorism-related information sharing as high risk because the government faces formidable challenges in analyzing and disseminating this information in a timely, accurate, and useful manner.[3] Our work on this high-risk area has primarily focused on the government's efforts to implement the ISE. As part of the ISE, DHS has been working to improve its sharing of terrorism-related information. In a September 2010 letter to DHS, we identified steps that the department could take to

[1] For purposes of this report, terrorism-related information encompasses terrorism information, which includes weapons of mass destruction information, and homeland security information consistent with section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, as well as law enforcement information relating to terrorism or the security of the homeland. See Pub. L. No. 108-458, § 1016(a), 118 Stat. 3638, 3664-65 (2004) (codified as amended at 6 U.S.C. § 485(a)). See also Pub. L. No. 107-296, § 892(f), 116 Stat. 2135 (2002) (codified at 6 U.S.C. § 482(f)).

[2] See generally Pub. L. No. 110-53, 121 Stat. 266 (2007), Pub. L. No. 108-458, 121 Stat. 3638 (2004). See also, generally, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[3] Terrorism-related information sharing remained a high-risk area for our February 2011 update. See GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: Feb. 16, 2011) for the most recent update. See also *Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP (Washington, D.C.: Nov. 1, 2000).

improve its sharing, which, among other things, included the development of a strategy for how DHS will achieve its information-sharing mission, demonstration of the existence of a clear governance structure for information sharing, and demonstration that DHS is making progress in providing terrorism-related information to its customers. DHS in turn identified related actions it was taking and provided us periodic updates on its progress, which are discussed later in this report. In response to your request, this report addresses the extent to which DHS (1) has made progress since 2010 in achieving its information-sharing mission, and what related challenges exist, if any, and (2) tracks and assesses information-sharing improvements.[4]

To address the first objective, we analyzed relevant strategic planning documents, as well as documents related to DHS's governance structure, plans and initiatives, and budget and technology framework for information sharing.[5] We also interviewed program officials within DHS's Office of Intelligence and Analysis (I&A), as well as officials from DHS's Office of the Chief Information Officer (CIO) to obtain information on the department's efforts to improve information sharing and related challenges. We selected one DHS information-sharing initiative—the Law Enforcement Information Sharing Initiative (LEISI) led by U.S Immigration and Customs Enforcement (ICE)—to analyze as a case study example of DHS's actions related to information-sharing initiatives, and discussed it with ICE officials.[6] We selected LEISI because it is one of DHS's information-sharing priorities and an established program. We assessed DHS's efforts against *Standards for Internal Control in the Federal*

[4] Although the high-risk area focuses on sharing terrorism-related information, many of the programs and efforts discussed in this report relate to DHS's efforts to share types of information beyond terrorism-related information.

[5] DHS has made recent efforts to also improve the safeguarding of information—in response to the release of classified and diplomatic documents by the website Wikileaks in 2010—but this was outside the scope of our review and therefore is not addressed in this report.

[6] LEISI was 1 of DHS's 18 key information-sharing initiatives as of September 2012.

Government and criteria that we use in assessing high-risk issues.[7] We also reviewed DHS's efforts related to its Segment Architecture against our prior report and federal guidance on defining architecture content.[8]

To address the second objective, we analyzed documentation and examples of DHS's mechanisms for tracking and assessing the progress and results from its information-sharing efforts, including documentation and data on DHS's performance measures for customer feedback and customer information needs, among other areas, for fiscal years 2011 and 2012. We assessed the reliability of these data by, for example, analyzing performance measurement documentation, and determined that they were sufficiently reliable for the purposes of this report. We also interviewed program officials within I&A and from DHS's Office of the CIO. In addition, we obtained information from customers of DHS's information sharing, including 10 of 77 fusion centers, where states and major urban areas collaborate with federal agencies to improve information sharing; 1 of 7 DHS operational components who participate in the DHS Intelligence Enterprise, ICE; and 2 of DHS's 16 intelligence community customers, the Office of the Director of National Intelligence (ODNI) and the Federal Bureau of Investigation (FBI).[9] We selected fusion centers based on, among other things, geographic dispersion and variation in risk based on the Department of Justice's (DOJ) 25 Cities

[7] See GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1, 1999). We have also established five criteria to assess when the government has made sufficient progress so that an issue no longer poses significant risk and can be removed as a high-risk area: demonstrated top leadership commitment to reduce risks; capacity, such as funding and other resources to reduce risks; a corrective action plan to identify and address root causes of risks; mechanisms to monitor effectiveness of corrective measures; and demonstrated progress in implementing corrective measures. See GAO-01-159SP. Because DHS is one of five key agencies responsible for establishing the ISE, its efforts to improve information sharing will not, on their own, result in removing the issue as a high-risk area.

[8] A segment architecture defines a road map to enhance business operations and achieve measurable performance improvements for a portion, or segment, of the enterprise. See GAO, *Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investments*, GAO-11-455 (Washington, D.C.: July 21, 2011). See also Federal Segment Architecture Working Group, *Federal Segment Architecture Methodology Version 1.0,* December 2008.

[9] According to the Under Secretary for Intelligence and Analysis, departmental intelligence programs, projects, activities, and personnel—including the intelligence elements of key operational components, as well as I&A—make up the DHS Intelligence Enterprise.

Project.[10] We selected ICE, ODNI, and the FBI because they are key customers of DHS's intelligence products or partner with I&A to create these products. ICE is a DHS component that shares terrorism-related information and leads two of DHS's key information-sharing initiatives. ODNI and the FBI are federal agencies that have key roles in analyzing terrorism threats to the United States and jointly issue products with DHS. The FBI also has the primary role in carrying out investigations within the United States of threats to national security. Because we selected a nonprobability sample of customers to contact, the information we obtained from these customers may not be generalized to all customers nationwide, but it provided us with a general understanding of the perspectives about DHS's information sharing held by different customer types nationwide. We assessed DHS's efforts for tracking and assessing information-sharing improvements against criteria for practices in program management.[11]

We conducted this performance audit from November 2011 through September 2012 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. Additional details on our scope and methodology are contained in appendix I.

[10] The 25 Cities Project refers to the High-Risk Metropolitan Area Interoperability Assistance Project, a DOJ Wireless Management Office grant program that identified the top 25 metropolitan areas that were considered likely targets for terrorist attack and provided communication solutions to federal and local authorities such as fire, police, and emergency medical services. Projects differ from city to city.

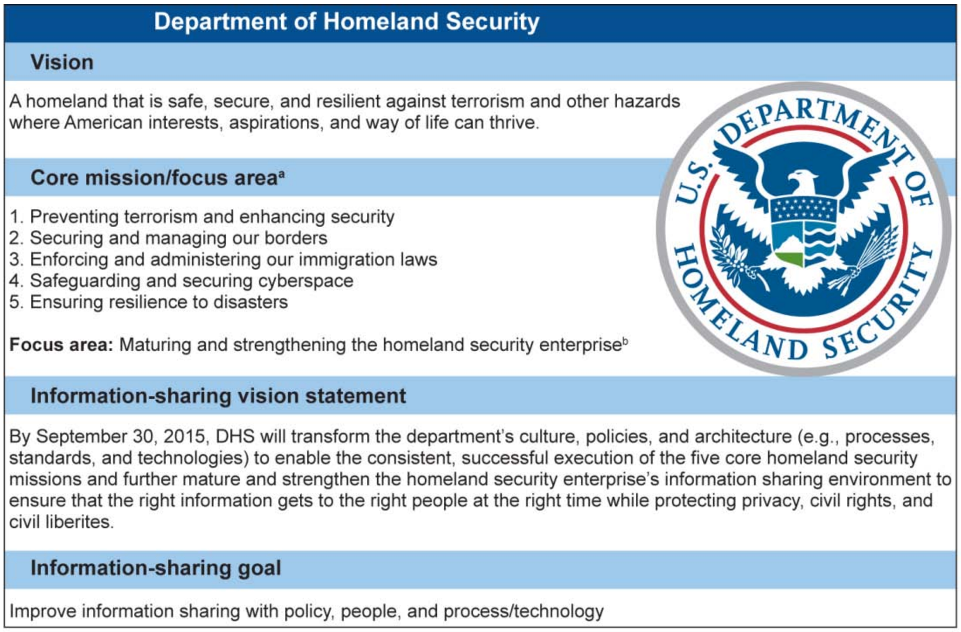
[11] For example, see Project Management Institute, *The Standard for Program Management®* (Newtown Square, PA: 2006); GAO, *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making*, GAO-05-927 (Washington, D.C.: Sept. 9, 2005), and *Program Evaluation: Studies Helped Agencies Measure or Explain Program Performance*, GAO/GGD-00-204 (Washington, D.C.: Sept. 29, 2000).

Background

Overview of DHS Roles and Responsibilities and the Information Sharing Environment

Figure 1 shows DHS's homeland security and information-sharing visions, missions, and goal.[12]

Figure 1: DHS's Visions, Missions, and Goal



U.S. DEPARTMENT OF HOMELAND SECURITY

Department of Homeland Security

Vision

A homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.

Core mission/focus area[a]

1. Preventing terrorism and enhancing security
2. Securing and managing our borders
3. Enforcing and administering our immigration laws
4. Safeguarding and securing cyberspace
5. Ensuring resilience to disasters

Focus area: Maturing and strengthening the homeland security enterprise[b]

Information-sharing vision statement

By September 30, 2015, DHS will transform the department's culture, policies, and architecture (e.g., processes, standards, and technologies) to enable the consistent, successful execution of the five core homeland security missions and further mature and strengthen the homeland security enterprise's information sharing environment to ensure that the right information gets to the right people at the right time while protecting privacy, civil rights, and civil liberites.

Information-sharing goal

Improve information sharing with policy, people, and process/technology

Source: GAO analysis of DHS information; seal courtesy of DHS.

[a] According to DHS officials, information sharing is a cross-cutting capability for all mission areas.

[b] According to DHS documentation, the homeland security enterprise is composed of the federal, state, local, tribal, territorial, nongovernmental, and private sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of the United States.

I&A is the lead DHS component with responsibilities for sharing terrorism-related information with all levels of government and the private sector. I&A performs a variety of functions related to information sharing, including gathering customer information needs, developing and

[12] According to DHS officials, DHS's information-sharing vision statement and goal will be updated when DHS publishes its *Fiscal Year 2012-2017 DHS Information Sharing and Safeguarding Strategy*.

distributing intelligence reports, and gathering customer feedback on the information I&A provides. I&A, along with the Office of the CIO, also has a key role in the overall governance structure DHS has created to manage information sharing throughout the department, which is discussed more fully later in this report. I&A is headed by the Under Secretary for Intelligence and Analysis who has responsibilities for, among other things, providing homeland security intelligence and information to the Secretary of Homeland Security; other federal officials and agencies, such as members of the intelligence community; Members of Congress; departmental component agencies; and the department's state, local, tribal, territorial, and private sector partners, such as fusion centers. In addition to I&A, multiple other DHS components—such as ICE, U.S. Customs and Border Protection (CBP), and the Transportation Security Administration (TSA)—share information within and outside DHS on threats more specific to their mission areas, such as travel information. Among other things, these agencies develop and distribute intelligence reports about these areas to customers, such as the intelligence community.

DHS is one of five key agencies responsible for establishing the ISE.[13] Section 1016 of the Intelligence Reform Act, as amended by the 9/11 Commission Act, requires the President to take action to facilitate the sharing of terrorism-related information through the creation of the ISE.[14] In April 2005, the President designated a Program Manager—within the Office of the Director of National Intelligence—to, among other things, plan for, oversee implementation of, and manage the ISE. In July 2011, we recommended that in defining a road map for the ISE, the Program Manager ensure that relevant initiatives individual agencies were implementing are leveraged across the government, among other

[13] In total, there are 15 ISE departments and agencies. In addition to the 5 key agencies (DHS, the Department of Justice, the Department of State, the Department of Defense, and the Office of the Director of National Intelligence), the other departments and agencies include the Central Intelligence Agency, the Department of Commerce, the Department of Energy, the Department of Health and Human Services, the Department of the Interior, the Department of Transportation, the Department of the Treasury, the FBI, and the National Counterterrorism Center, as well as the Joint Chiefs of Staff. See, e.g., appendix A of the July 2010 *ISE Annual Report to the Congress*.

[14] See 6 U.S.C. § 485.

things.[15] The Program Manager generally agreed with our recommendations and has actions under way to address them. DHS noted that the department remained committed to continuing its work with the Program Manager and relevant stakeholders to further define and implement a fully functioning ISE.

DHS's Office of the CIO is responsible for the department's information technology management and is developing the department's enterprise architecture (EA), which is designed to establish an agencywide road map to achieve its mission. An EA can be viewed as a reference or "blueprint" for guiding an organization's transition to its future environment that includes maximizing information sharing within and across organizational boundaries. Along with I&A, the Office of the CIO is responsible for overseeing this transition.

Federal Statutes and Strategies Governing Information Sharing

Since the terrorist attacks of September 11, 2001, several statutes have been enacted into law that relate to enhancing the sharing of terrorism-related information among federal, state, and local agencies as well as other stakeholders, and the federal government has developed related strategies and guidelines to meet its statutory obligations. Pursuant to the Homeland Security Act, as amended, I&A has responsibility for, among other things, assessing, receiving, and analyzing law enforcement, intelligence, and other information in order to (1) identify and assess the nature and scope of terrorist threats to the homeland, (2) detect and identify threats of terrorism against the United States, and (3) understand such threats in light of actual and potential vulnerabilities to the homeland.[16] Further, pursuant to the 9/11 Commission Act, the Secretary of Homeland Security—through the Under Secretary for I&A—shall

[15] GAO-11-455. In this report, we made recommendations at the national level to the Program Manager for the ISE and did not make any recommendations to DHS or other individual key agencies that support the ISE.

[16] See 6 U.S.C. § 121.The Homeland Security Act established a Directorate of Information Analysis and Infrastructure Protection, within which the Assistant Secretary for Information Analysis carried out the department's primary intelligence functions. See Pub. L. No. 107-296, § 201, 116 Stat. at 2145-49. The 9/11 Commission Act subsequently eliminated the directorate and established separate offices for Intelligence and Analysis, headed by an Under Secretary, and for Infrastructure Protection, headed by an Assistant Secretary. See Pub. L. No. 110-53, § 531, 121 Stat. at 332-35.

integrate the information and standardize the format of the terrorism-related products of the department's intelligence components.[17]

In October 2007, the President issued the *National Strategy for Information Sharing*, which identifies the federal government's information-sharing responsibilities. The strategy calls for authorities at all levels of government to work together to obtain a common understanding of the information needed to prevent, deter, and respond to terrorist attacks. On the basis of the National Strategy, DHS developed a strategy in 2008 to direct the department's information-sharing efforts and is drafting a *Fiscal Year 2012-2017 DHS Information Sharing and Safeguarding Strategy*. DHS plans to finalize and release this new strategy after the Executive Office of the President issues a new *National Strategy for Information Sharing and Safeguarding*, and DHS then plans to release an implementation plan that is to describe in more detail how the department will implement its strategy along with related milestones.[18] DHS's new strategy is intended to update the 2008 strategy to reflect the department's growing and increasingly complex mission and include information safeguarding—in response to the release of classified and diplomatic documents by the website Wikileaks in 2010—as well as information sharing.

DHS Has Made Progress in Advancing Key Information-Sharing Initiatives, but Additional Steps Could Help Sustain Such Efforts

DHS has established a decision-making body—the Information Sharing and Safeguarding Governance Board (the board)—that demonstrates senior executive-level commitment to improving information sharing. The board has identified information-sharing gaps and developed a list of key initiatives to help address those gaps, but additional steps could help DHS sustain these efforts. Board and department attention has helped achieve progress on many of the key initiatives, but funding challenges have slowed some efforts. DHS has also made progress in developing and implementing DHS's Information Sharing Segment Architecture, but has not yet fully developed this architecture. The board plans to update the *DHS Information Sharing Strategy* and develop a related implementation plan, which will be important in managing information-sharing efforts.

[17] See 6 U.S.C. § 124a(a).

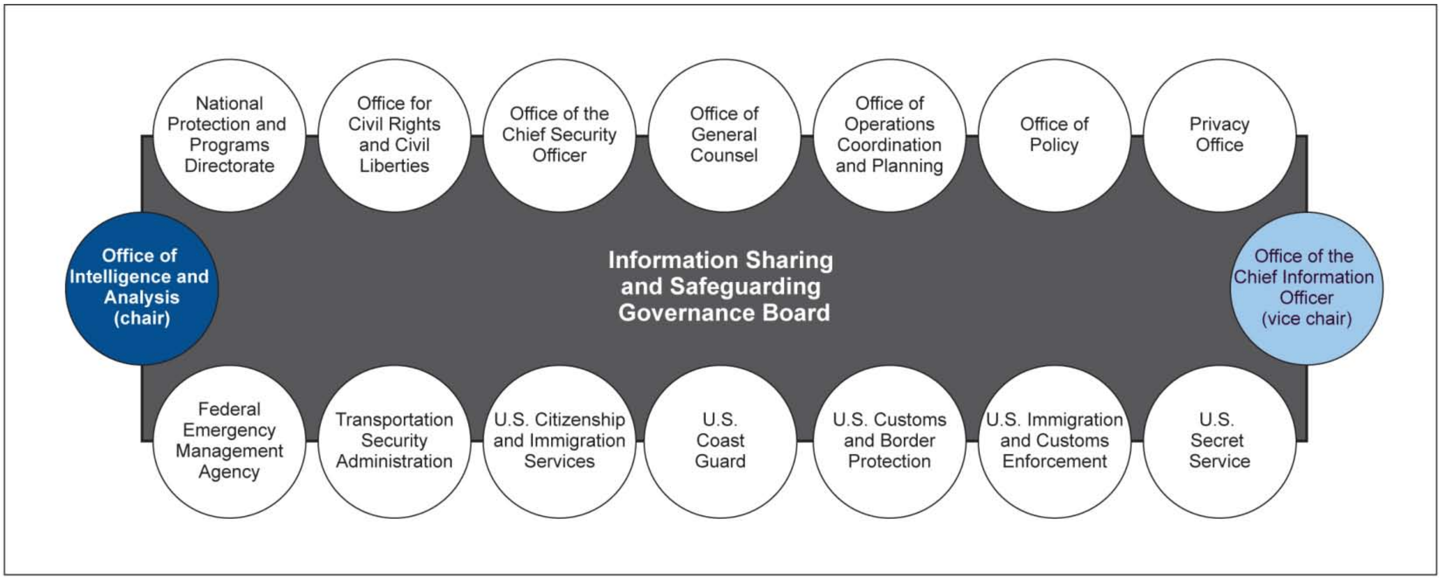
[18] As of early September 2012, the new *National Strategy for Information Sharing and Safeguarding* had not been released.

The Governance Board Demonstrates Leadership Commitment to Improving Information Sharing

The Information Sharing and Safeguarding Governance Board serves as DHS's senior executive-level decision-making body for information-sharing issues. According to the board's charter, DHS established the board in 2007 to serve as the "arbiter of data access denials or delays that cannot be resolved at the component level" and to work with DHS operational components to monitor their information management processes and ensure respect for legal protections. In the aftermath of the release of classified and diplomatic documents by the website Wikileaks, in 2011 DHS revised the board's charter to reflect its responsibility to govern both information sharing and safeguarding and expanded the board's membership to incorporate components with information-safeguarding responsibilities.[19] The board includes senior executive-level representation from almost every DHS component, as shown in figure 2.

[19] According to the board's charter, as revised, the President, through the August 2, 2011, memorandum entitled FY 2013 Programmatic Guidance for the Information Sharing Environment, directed departments and agencies in the Information Sharing Environment to strengthen governance processes for the sharing and safeguarding of critical information, both classified and unclassified, and to improve capabilities at the agency level to address and mitigate vulnerabilities. The revised charter also provides that pursuant to Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, issued on October 7, 2011, all federal departments and agencies must, among other things, institute a governance mechanism that synchronizes information sharing and safeguarding. See 76 Fed. Reg. 63,811 (Oct. 13, 2011).

Figure 2: Composition of the Information Sharing and Safeguarding Governance Board


National Protection and Programs Directorate
Office for Civil Rights and Civil Liberties
Office of the Chief Security Officer
Office of General Counsel
Office of Operations Coordination and Planning
Office of Policy
Privacy Office
Office of Intelligence and Analysis (chair)
Information Sharing and Safeguarding Governance Board
Office of the Chief Information Officer (vice chair)
Federal Emergency Management Agency
Transportation Security Administration
U.S. Citizenship and Immigration Services
U.S. Coast Guard
U.S. Customs and Border Protection
U.S. Immigration and Customs Enforcement
U.S. Secret Service

Source: GAO analysis of DHS information.

The Under Secretary for Intelligence and Analysis serves as the board's chair. According to DHS officials, as the DHS representative to the interagency policy committee for information sharing, the Under Secretary brings knowledge of governmentwide information-sharing efforts.[20] The DHS Chief Information Officer serves as the board's vice chair, also bringing knowledge as the authority over DHS's technology-related information-sharing projects. Board minutes show that senior-level officials attend the board's quarterly meetings, demonstrating DHS leadership commitment to the board's work. The board is responsible for approving the department's information-sharing and -safeguarding vision and strategy, establishing information-sharing goals and priorities, and overseeing implementation across DHS components. According to DHS

[20] For example, the Under Secretary for I&A participates in the Information Sharing and Access Interagency Policy Committee (ISA IPC). In July 2009, the administration established the ISA IPC within the Executive Office of the President to, among other things, identify information-sharing priorities going forward. The ISA IPC assumed the functions and responsibilities of the former White House Information Sharing Council, which had been established pursuant to section 1016(g) of the Intelligence Reform Act. See 6 U.S.C. § 485(g). The committee—with representation of participating ISE agencies and communities—is intended to provide oversight and guidance to the ISE.

officials, the board periodically reports its results to the Secretary of Homeland Security. The Information Sharing Coordinating Council serves as an advisory body to the board and supports it by recommending policies and procedures for information sharing, preparing for board meetings, and helping to track information-sharing initiatives.[21]

The board has advanced DHS information sharing in several ways. First, the board has raised visibility—that is, has increased awareness of—information-sharing initiatives. Both the Office of the CIO and ICE officials noted that visibility improves stakeholder coordination across initiatives and facilitates access to high-level officials who can help initiatives overcome roadblocks. For example, ICE officials said that the board has increased the visibility of LEISI—DHS's main initiative for sharing law enforcement information with state and local partners—and that other DHS components are now more likely to coordinate with LEISI in their law enforcement information-sharing activities. An official from the Office of the CIO also noted that the board provides information-sharing initiatives with organizational support at higher levels across DHS, which can remove roadblocks within or across components. For example, the official noted that one information-sharing initiative—the Homeland Security Information Network (HSIN), which DHS uses to share information with federal, state, and local partners—cannot succeed without this visibility and now has better stakeholder coordination than ever before.

Second, according to DHS officials, the board has helped to reduce redundancies across DHS components. For example, through board activities, members recognized that DHS components were independently developing over 20 systems to collect, share, and display the information that components and other stakeholders need to plan for and respond to threats and hazards, known as Common Operating Picture systems. The board worked with the components involved to examine each component's Common Operating Picture systems and identify opportunities for cooperation, thereby reducing redundancies and saving funds.

[21] The board has two additional subordinate bodies—the Law Enforcement Shared Mission Community, which serves as an advisory board on law enforcement information-sharing issues, and the Information Safeguarding and Risk Management Council, which serves as an advisory board on information-safeguarding issues.

In February 2012, the board also established an Information Sharing Environment Coordination Activity—with staff from I&A and the Office of the CIO—to facilitate decision making related to DHS's Information Sharing Segment Architecture transition plans. The group's responsibilities include developing recommendations and advising on policy development, resource allocation, acquisition management, and program management processes. In addition, the group is responsible for assessing whether departmental investments in new and existing technology programs include critical information-sharing capabilities, and whether investments present opportunities to deploy capabilities as enterprise services, such as computer-to-computer mechanisms to deliver information between systems. We discuss this group's role in several information-sharing efforts later in this report. Because the group is relatively new, it was too early for us to determine its impact. DHS's actions to establish an information-sharing governance structure and related activities demonstrate DHS leadership's commitment to improving information sharing.

DHS Has Identified Key Information-Sharing Initiatives to Fill Gaps, but Additional Steps Could Help Sustain this Process

Key Information-Sharing Initiatives

DHS has identified a list of initiatives that it determined are key to advancing information sharing within the department and with its customers, which DHS refers to as its Information Sharing Roadmap. According to DHS officials, to develop this list, the board hosted a series of meetings from April 2010 through December 2011 with relevant components in each of its five mission areas.[22] According to I&A officials,

[22] The Quadrennial Homeland Security Review is a DHS strategic framework that includes DHS's vision for a secure homeland, specifies key mission priorities, and outlines goals for each DHS mission area. As part of this review, DHS identified five homeland security missions and assessed DHS efforts to mature and strengthen the homeland security enterprise itself. See DHS, "Quadrennial Homeland Security Review Report," February 2010. According to DHS officials, information sharing is not a mission unto itself, but a "force multiplier" that enables the department to achieve its mission objectives faster and at reduced risk and cost. DHS structured the discussions for each mission area to identify gaps related to (1) people and cultural issues, (2) policy and legal issues, and (3) technology issues.

these meetings included in-depth conversations with DHS and component executives about their information-sharing activities and gaps, and presentations from subject matter experts on these issues. The board selected a list of 22 initiatives that it determined represented DHS's greatest opportunities to improve information sharing. Some of these initiatives were information-sharing programs that components were already implementing as part of their mission activities, while others were new projects designed to address specific information-sharing gaps. According to DHS officials, the process of identifying departmental information-sharing gaps evolved progressively over the course of 2 years as the board continually sought to improve its methods.

According to DHS officials, in July 2011, the board's chair requested that board members prioritize the list of initiatives and select a smaller and more manageable list to receive additional support in the DHS budget process. Using a weighted scoring and voting system, each board member selected 5 top-priority initiatives based on four criteria: cross-departmental impact, linkage to mission areas, enterprisewide information-sharing enabler, and level of DHS component support. After compiling these rankings across members, the board determined that 8 initiatives were clustered near the top of the list and established these initiatives as its priority efforts, as shown in table 1.

Table 1: DHS's Eight Priority Information-Sharing Initiatives, as of September 2012

Initiative	Responsible component(s)[a]	Function
Controlled Homeland Information Sharing Environment (CHISE)	I&A, Office of the CIO, and Screening Coordination Office	Developing an integrated, searchable index to consolidate and streamline access to intelligence, law enforcement, and other information across DHS.
Information Sharing Segment Architecture (Segment Architecture) Transition	I&A and Office of the CIO	Overseeing the Segment Architecture Transition Plan—that is, the actionable steps and milestones needed to implement the key capabilities required for the DHS information sharing environment.
Law Enforcement Information Sharing Initiative	ICE	Sharing law enforcement information with state and local partners. This initiative includes formulating uniform law enforcement information-sharing policies for DHS, expanding and enhancing information technology to support information sharing, simplifying customer access to federal law enforcement and homeland security information, and ensuring that DHS law enforcement officers and analysts have the systems needed to access information from federal, state, and local partners.
Common Operating Picture/User-Defined Operating Picture	Office of Operations Coordination and Planning and Office of the CIO	Developing an application that collects, shares, and displays the information DHS components need to plan for and respond to threats and hazards.

Initiative	Responsible component(s)[a]	Function
TECS Modernization	CBP and ICE	Modernizing the infrastructure of TECS—a key system for border enforcement and the sharing of information about people who are inadmissible to the United States under the law or pose a potential threat.
Private Sector Information Sharing Work Plan	Private Sector Office and National Protection and Programs Directorate	Developing better engagement tools, processes, and methods to encourage and promote two-way information sharing with private sector partners.
Homeland Secure Data Network	I&A and Office of the CIO	Developing a secure network that gives DHS the ability to collect, disseminate, and exchange information with federal, state, and local partners up to the secret level.
Homeland Security Information Network	I&A and Office of the CIO	Developing a secure, web-based sensitive but unclassified network for information sharing and collaboration with federal, state, local, tribal, territorial, private sector, and international partners.

Source: GAO analysis of DHS documents.

[a] The Screening Coordination Office within the DHS Office of Policy was established to integrate, where appropriate, the wide range of DHS screening and credentialing activities to enhance DHS missions of keeping dangerous people and things out of the United States and securing critical infrastructure. The Office of Operations Coordination and Planning is responsible for monitoring the security of the United States on a daily basis and coordinating activities within DHS and with governors and law enforcement partners, among others. The Private Sector Office, within the Office of Policy, is responsible for, among other things, promoting public-private partnerships and best practices to improve homeland security. The National Protection and Programs Directorate has responsibility for advancing DHS's risk reduction mission by addressing various physical and virtual threats.

To improve the process it used to select the priority initiatives, DHS formed the Criteria Working Group in 2011. According to the working group's briefing materials, the group developed new criteria for selecting priority initiatives—such as mission criticality and feasibility—that it will use in future prioritization efforts and a new process for integrating component input on which initiatives to choose as priorities.

According to DHS officials, the board also recognized the need to periodically add and remove initiatives from the broader list of key information-sharing initiatives and developed and documented processes to do so. Therefore, in December 2011, the board elected to begin reviewing the list of initiatives on a semiannual basis, evaluating the initiatives for continued relevancy and considering newly emerging requirements. According to I&A officials, the board could remove an initiative from the list because (1) the initiative has "graduated"—that is, it has achieved all of its information-sharing goals or (2) the initiative has languished because components have not provided needed funding or DHS did not have a lead component to manage the initiative. These latter initiatives would be removed from the list and set aside for potential reevaluation if a component agrees to lead the initiative at a later date. In

May 2012, DHS issued the *Information Sharing and Safeguarding Roadmap Implementation Guide* to document and describe goals and elements of the list of key initiatives and provide guidance for development, management, and oversight of the list.[23]

In 2012, the board added 5 new initiatives to the list in order to reflect the board's new emphasis on information safeguarding.[24] The board also consolidated 3 initiatives into a single initiative, split 1 initiative into 2 separate initiatives, and removed 3 from the list because, according to I&A officials, they were better handled by other entities and no longer required board involvement. As of September 2012, DHS had 18 key information-sharing initiatives and 5 safeguarding initiatives on its list of key initiatives.

Steps to Sustain Efforts

DHS's efforts to identify information-sharing gaps and select initiatives to address them have advanced information-sharing efforts, but additional steps could help DHS sustain these efforts. First, DHS has not documented its process for identifying information-sharing gaps in each of its mission areas or the list of gaps it identified. Documenting this process and its results could help DHS replicate and sustain this process in the future. Federal internal control standards require agencies to clearly document significant activities.[25] DHS officials noted the board did not document the process because its efforts were in early stages and the process was revised as the board learned from experience. Processes for selecting key information-sharing initiatives are documented in DHS's *Roadmap Implementation Guide*—the department's policies and procedures for managing key initiatives. However, because DHS's assessment of gaps drives the selection of key information-sharing initiatives, documenting the process for identifying gaps and the results of that process in the *Roadmap Implementation Guide* or other related policies and procedures would provide DHS with an institutional record to better replicate, and therefore sustain, a key step in its efforts to improve information sharing.

[23] DHS, *Information Sharing and Safeguarding Roadmap Implementation Guide,* May 2012.

[24] DHS's five safeguarding priorities in the 2012 list of initiatives are Address the Insider Threat, Improve Access Control, Improve Enterprise Audit, Reduce Removable Media Use, and Reduce User Anonymity.

[25] GAO/AIMD-00-21.3.1.

Second, DHS did not analyze the root causes of information-sharing gaps to ensure that its key initiatives target the correct problems. According to DHS officials, DHS did not do this because the root causes of DHS's information-sharing problems—such as challenges in incorporating diverse agencies into a single department—are well known and have been discussed at high levels within the executive branch, in the context of the formation of DHS, in the 9/11 Commission Report, and through subsequently enacted laws.[26] These broad, overarching issues help inform DHS's efforts to improve information sharing, but documenting and implementing a process for analyzing the specific causes of DHS's information-sharing gaps within each mission area would help DHS ensure that it invests in the correct information-sharing solutions. For example, diagnosing whether specific gaps are caused by DHS's own funding decisions and constraints, by its organizational structure, or by technological limitations would allow DHS to better choose appropriate solutions. Furthermore, our work on high-risk programs has shown that analyzing root causes of program gaps or limitations can help in designing effective solutions to reduce risks.[27]

Third, DHS has not established and documented a process for identifying and assessing the risks of removing an initiative from the list when the initiative does not have funding or component support, and does not have a documented process for mitigating the risk of removing incomplete initiatives. Given that DHS selects key information-sharing initiatives based on identified information-sharing gaps, it is important to assess the risks of removing an initiative and determine whether alternative solutions are needed to mitigate these risks in order to address information-sharing gaps. Internal control standards also require agencies to comprehensively identify risks and decide how to manage them.[28] The board's deliberations on updates to its strategy recognize the need to institutionalize risk management into daily mission operations for information sharing. However, officials stated that the board has not accounted for the risk of removing items to date because (1) the processes for developing the list of initiatives are relatively new and (2) the only items DHS has removed so far are ones that continue to be

[26] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, D.C.: July 2004).

[27] GAO-01-159SP.

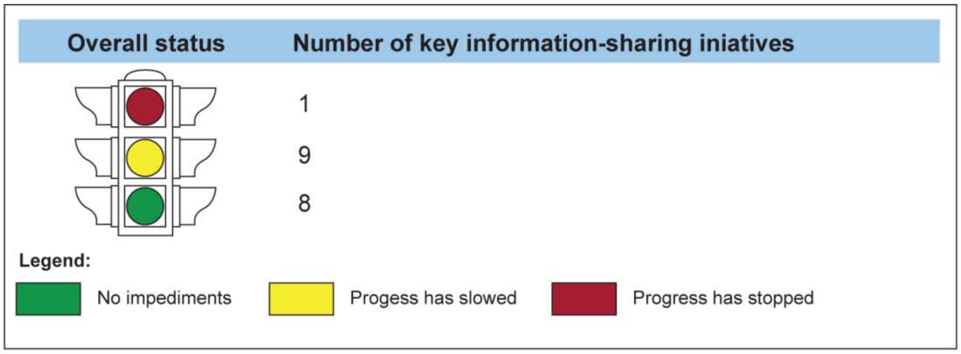
[28] GAO/AIMD-00-21.3.1.

managed by another entity within the department, which mitigated the risk of removal. Nevertheless, as we describe in the following section, funding and other constraints may require DHS to remove items from the list in the future, and establishing and documenting processes for potential future use could help guide these decisions. DHS officials stated that such processes could improve information-sharing efforts. By establishing and documenting processes for identifying and assessing the risks of removing an incomplete initiative from its list and working to mitigate that risk, DHS could be better positioned to identify the effects that removal may have on its information-sharing efforts and sustain these efforts.

DHS Has Advanced Key Information-Sharing Initiatives, but Progress Has Slowed for Half of Them in Part because of Funding Constraints

Since DHS developed its list of key information-sharing initiatives, many of those initiatives have proceeded and met interim program milestones. As of June 2012, 15 of the 18 key information-sharing initiatives met at least one interim milestone, and DHS fully completed 1 initiative—developing a training course designed to improve and increase sharing of terrorism information by promoting a culture of awareness. However, as shown in figure 3, progress has slowed or stopped for 10 of the 18 key information-sharing initiatives presented to the board in June 2012.

Figure 3: Summary of Overall Status of DHS Key Information-Sharing Initiatives, as of June 2012



Overall status	Number of key information-sharing iniatives
🟥	1
🟨	9
🟩	8

Legend:

🟩 No impediments 🟨 Progess has slowed 🟥 Progress has stopped

Source: GAO analysis of DHS information.

Funding constraints are a primary reason why progress has slowed or stopped for some initiatives. For example, among the 8 priority information-sharing initiatives, 5 faced risks as of June 2012 because of lack of funding, and DHS has had to delay or scale back at least 4 of them. More specifically, according to ICE documents, LEISI has met milestones related to several activities—including developing a strategic plan, implementing a performance metrics tracking system, and expanding information sharing with federal, state, and local partners—but inadequate funding threatens the ability of ICE to further expand the LEISI user base and share additional data, among other things. Also, DHS's top information-sharing priority (CHISE)—an initiative to develop an integrated, searchable index to consolidate and streamline access to intelligence, law enforcement, and other information across DHS—has not been fully funded, but efforts to explore possible funding options continue, according to DHS officials. The officials noted that CHISE is intended to streamline access to terrorism-related information and help analysts synthesize this information. The officials added that until CHISE is developed, analysts will continue to separately access numerous data sets from across the department, which requires a larger number of analysts, is more time consuming, and may result in missing connections among data in different data sets.

According to I&A officials, for the fiscal year 2012 budget, the board made a concerted effort to advocate for additional funding to support priority initiatives and emphasize information sharing during the DHS planning and budgeting process. According to I&A officials, the board was not able to obtain increased funding for the initiatives but plans to continue its efforts. The officials noted that the board does not have budget authority within the department, and therefore does not have the authority or resources to fund the priority initiatives. They explained that under the DHS budget process, the initiatives are considered integral to, and not separate from, an agency's fundamental mission activities and are funded through the DHS components responsible for each initiative. Thus, according to the officials, in a constrained budget environment, components are faced with difficult decisions in deciding whether to fund mission activities or information-sharing activities. However, DHS officials stated that the board's involvement has kept some of these initiatives from experiencing funding cuts. In addition, as we reported in July 2012, the board serves as the portfolio governance board for information sharing, which provides guidance and investment recommendations for future year planning, programming, and budgeting.[29] According to DHS officials, as the department's information technology governance process matures, the board will have a more formal role and processes for affecting funding decisions.

[29] GAO, *Information Technology: DHS Needs to Further Define and Implement Its New Governance Process*, GAO-12-818 (Washington, D.C.: July 25, 2012).

Moving forward, DHS plans to collect and publish data on the annual and long-term funding the department budgets and spends on its information-sharing and -safeguarding programs and activities.[30] According to DHS officials, the ability for the department to generate reliable cost estimates for these sharing and safeguarding programs and activities will lower the risk to the public and minimize overruns, missed deadlines, and performance shortfalls. The officials added that cost estimates will also allow decision makers to prioritize future investments and demonstrate a continued commitment to support the capability and capacity of DHS components to share and safeguard information. These cost estimates could also allow us to determine the extent to which DHS has the capacity to implement its plans. We will continue to monitor DHS's implementation of these plans and its ability to address funding shortfalls for key initiatives, particularly in a challenging budget environment.

DHS Has Made Important Progress, but Has Yet to Fully Implement Its Information-Sharing Architecture

DHS has developed architecture guidance to support the implementation of its target DHS information sharing environment.[31] Specifically, in May 2009, DHS published version 2.1 of its Information Sharing Segment Architecture. In July 2011, we reported that the Segment Architecture did not include key architecture content, such as a transition plan for moving to the target DHS information sharing environment and a conceptual solution architecture that provides an integrated view of proposed systems and services.[32] In response, DHS has made important progress in addressing the missing architecture content. For example, in January 2012, DHS updated its Segment Architecture to include a transition plan that provides a conceptual road map to implement the key capabilities needed to achieve the target DHS information sharing environment.

[30] According to DHS officials, this effort and related milestones will be discussed in the implementation plan for the forthcoming *DHS Information Sharing and Safeguarding Strategy*. As noted earlier in this report, DHS officials stated that they are waiting to release this strategy until after the new *National Information Sharing and Safeguarding Strategy* is released.

[31] The target DHS information sharing environment contains four technology layers (information access, information presentation, information discovery, and information delivery), which represent the functional groupings of information processes necessary to realize the target information sharing environment.

[32] GAO-11-455. In this report, we made ISE recommendations at the national level to the Program Manager for the ISE and did not make any recommendations to the individual key agencies, including DHS, that support the ISE.

DHS has also taken actions to identify and define its key business and information requirements, an initial important step in building an effective architecture to determine technology solutions it will need to achieve its information-sharing goals. According to guidance issued by the Program Manager for the ISE, agencies should create an inventory of assets to effectively share terrorism-related information.[33] According to the executive director of the DHS Information Sharing Environment Office, DHS has completed an inventory of the data assets (e.g., databases containing terrorism-related information) that each of the components across the department owns, such as border-crossing records. More specifically, DHS has cataloged more than 800 data assets across the department and identified the basic information available in each asset. Also according to the executive director, the Information Sharing Environment Coordination Activity will then determine with what other stakeholders DHS needs to share these data assets. DHS has determined that 80 of the data assets contain information with potential value in counterterrorism efforts. Of those 80, DHS identified the top 20 most valuable data assets and included them in the CHISE initiative, which is to organize these data assets into searchable indices to facilitate fast information retrieval. Since 2008, we have reported on the importance of agencies taking an inventory of what information they own as the first step to then determining who needs to have this information and how agencies will share it with key partners.[34] DHS's inventory efforts should help it to more systematically determine where it has gaps in sharing or additional opportunities to use the information it owns to protect the homeland.

DHS has also developed a conceptual solution architecture, which, according to the guidance issued by the Program Manager for the ISE, is to provide an integrated view of the combined systems, services, and technology for the target ISE, as well as the interfaces between them. This conceptual solution architecture provides an integrated view of

[33] Program Manager for the ISE, Information Sharing Environment Profile and Architecture Implementation Strategy version 2.0, June 2009.

[34] GAO, *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GAO-08-492 (Washington, D.C.: June 25, 2008).

systems, such as Homeland Secure Data Network,[35] and services, such as Enterprise Service Bus message services,[36] which allow information to flow among disparate applications across multiple hardware and software platforms. This is important since it defines specific technology resources for implementing DHS's information sharing environment. In addition, DHS officials stated the department is using its shared space to share terrorism-related information with other agencies.[37] For example, the officials stated DHS plans to use its Suspicious Activity Reporting (SAR) shared space to share SAR data with the Department of Justice.[38]

DHS has made important progress, but issues remain to effectively implement its information-sharing architecture. According to the guidance issued by the Program Manager for the ISE, agencies should align data assets with the ISE business mission processes. DHS stated that it has aligned its data assets with the ISE SAR business process and made progress in aligning data assets with the ISE Terrorist Watchlist mission business process.[39] However, it has not aligned data assets with the ISE Alerts, Warnings, and Notifications (AWN) mission business process.[40] DHS stated that it will document the AWN data assets' alignment after the

[35] Homeland Secure Data Network is a classified wide-area network for DHS that serves as a consolidated backbone that brings together multiple, legacy secret-level classified networks across DHS and provides interconnections to intelligence community and federal law enforcement resources.

[36] Enterprise Service Bus is an integration technology that provides the capability to bridge disparate information technology networks and platforms.

[37] Shared spaces are repositories used to make standardized terrorism-related information, applications, and services accessible to all ISE agencies and other relevant entities.

[38] The Nationwide Suspicious Activity Reporting Initiative is to establish a national capacity for gathering, documenting, processing, analyzing, and sharing reports of suspicious activity that is potentially terrorism-related.

[39] The ISE Terrorist Watchlist mission business process is a component of the identification and screening mission process and encompasses the receiving and sharing of reported information and the nomination, export, screening, encounter, redress, and updates to the Terrorist Screening Database. The FBI's Terrorist Screening Center maintains this database of known or suspected terrorists, which is used during security-related and other screening processes.

[40] Alerts, Warnings, and Notifications refers to an ISE mission business process that supports the preparation of and ensures timely dissemination and handling of terrorism alerts and warnings among ISE participants, at appropriate security levels.

Program Manager for the ISE issues a national-level standard that describes business context and information exchanges for AWN. According to the Deputy Program Manager for the ISE, the Office of the Program Manager plans to work with DHS and other agencies on the development of standard information exchanges for AWN in fiscal year 2013. The alignment of DHS data assets with the ISE mission business processes is important because it would support better discovery and sharing of relevant terrorism-related information.

In addition, while DHS has developed a conceptual solution architecture, it has not yet determined how well its current systems and technology environment support target business and information requirements. According to guidance from the Program Manager for the ISE, ISE agencies should assess the systems and technology environment for alignment with business and information requirements. According to DHS officials, from April through July 2012, the DHS Information Sharing Environment Coordination Activity conducted an initial baseline assessment of major programs to determine whether current systems and technologies can satisfy target architecture requirements, such as business and data requirements. Also according to DHS, it will review other segment architectures (e.g., screening) being developed to assess alignment with information-sharing capabilities described in the information-sharing architecture. By taking these actions, DHS could achieve cost avoidance and cost savings in implementing the DHS information sharing environment.[41]

Upcoming Information Sharing Strategy and Implementation Plan Will Be Important in Managing Information-Sharing Efforts

DHS's activities to assess gaps, select initiatives, and ensure that information-sharing programs have the capabilities needed to promote sharing are in the early development and implementation phases. As a result, DHS is taking steps to institutionalize some of its policies and practices, including developing key strategies and plans, that will be important in planning and managing its information-sharing efforts. In our September 2010 letter to DHS, we stated that DHS should develop a strategy and commensurate plans to achieve its information-sharing mission, among other things. According to DHS officials, the department is taking steps to update and develop other strategies and related plans in

[41] Additional information on the status of the Information Sharing Environment Coordination Activity's efforts is discussed later in this report.

addition to its list of key information-sharing initiatives that could address steps we have identified for DHS to take in information sharing. For example, as discussed earlier in this report, DHS is working to update the *DHS Information Sharing Strategy*, in part to be consistent with governmentwide efforts to update the related National Strategy. DHS officials stated that they expect to issue the updated strategy after the National Strategy is released, although the date of this latter action is uncertain. In deliberating on the updates, DHS is working to ensure that the DHS strategy outlines its information-sharing vision and mission, and addresses important components, such as goals and objectives on sharing and safeguarding information, methods it plans to achieve key outcomes as well as manage any potential risks, and steps it plans to take to ensure efforts receive the resources they need. Subsequent to releasing its strategy, DHS plans to release the *Information Sharing and Safeguarding Implementation Plan* within 90 days that is to describe in more detail how DHS will implement its strategy and include related milestones for the efforts described in the plan. We will continue to monitor implementation of these strategies and plans for taking corrective actions to improve information sharing.

DHS Has Taken Steps to Track Information-Sharing Efforts, but Has Not Yet Fully Assessed How They Have Improved Sharing

DHS is tracking the progress key information-sharing initiatives are making toward interim milestones but the department generally does not track when the initiatives will be completed, so as to make course corrections if completion dates are delayed, or assess what impact they are having on achieving needed sharing. DHS also has taken several steps to implement the information-sharing capabilities it needs to share information but has not yet defined the level of capabilities that initiatives and other programs must have in place to help it achieve the department's information-sharing vision. Customer feedback can help assess information sharing by indicating how useful customers find the products DHS disseminates; DHS has taken steps to survey its customers to determine their satisfaction as well as assess their needs. DHS has not yet developed measures that determine the impact of sharing on its homeland security efforts, but plans to develop more meaningful ways to assess information-sharing results and progress toward achieving its vision.

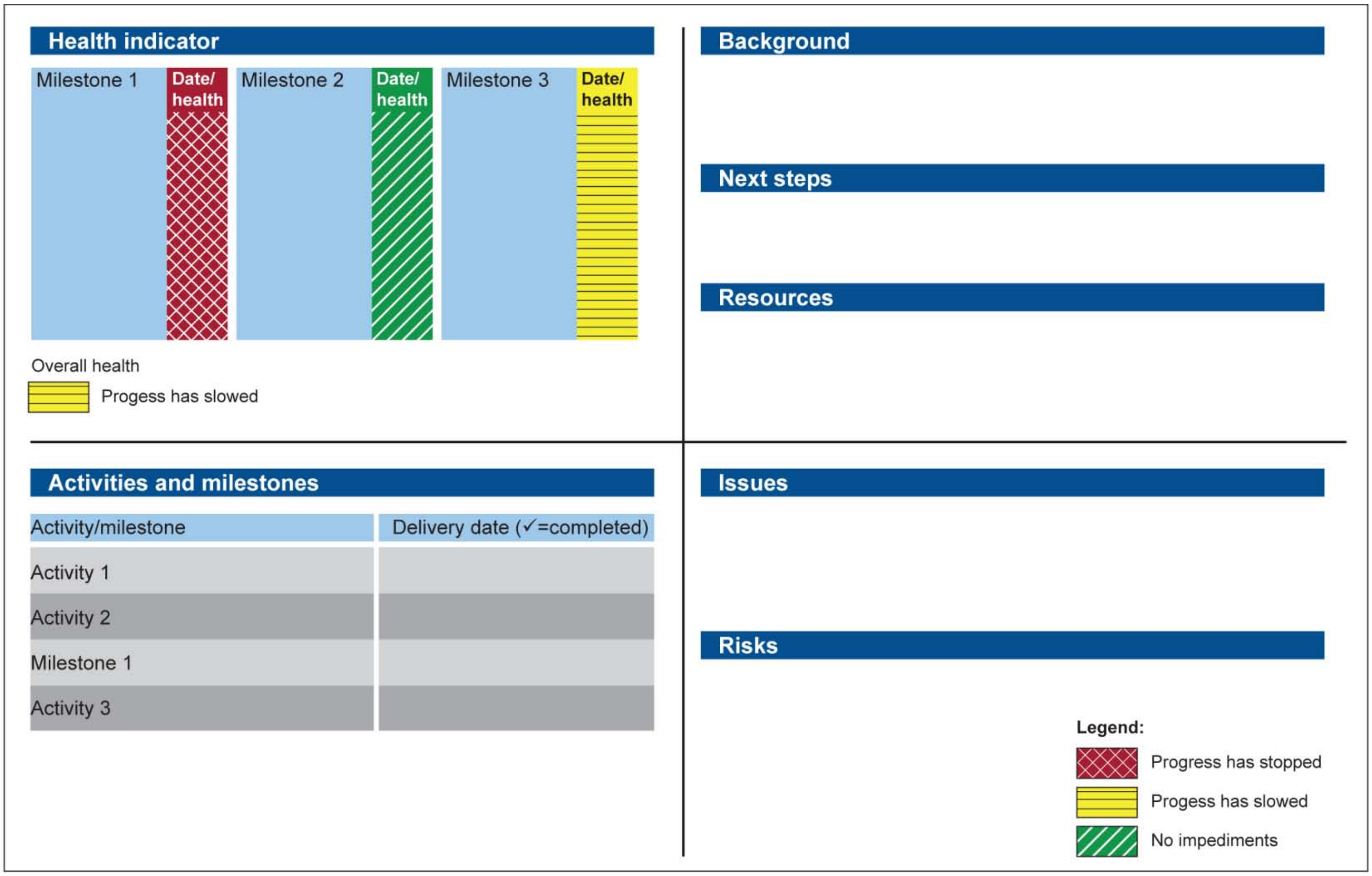
DHS Is Tracking Progress of Key Initiatives but Does Not Track Completion Dates or Assess Impacts on Information Sharing

Our work has shown that being able to track the progress of initiatives that address program barriers as well as assess the effectiveness of initiatives, or the results they achieve, can help agencies minimize the risks in key programs such as information sharing.[42] DHS is tracking the implementation progress of key information-sharing initiatives, but the department does not track how close the initiatives are to completion and could better assess how the initiatives are improving information sharing or helping DHS achieve its 2015 vision, which includes ensuring that the right information gets to the right people at the right time.

DHS has developed a tool to track implementation of key information-sharing initiatives, referred to as Roadmap Quad Charts, but it does not include information on how close the initiatives are to completion. According to I&A documents, the purpose of the charts is to report an initiative's implementation progress to the board. Components are responsible for providing the information tracked in the charts and submitting monthly updates to I&A. The tool contains an overall health indicator, key milestones, risks, and other data, as shown in figure 4.

[42] GAO-01-159SP.

Figure 4: Generic Quad Chart for Key Information-Sharing Initiatives



Health indicator

Milestone 1	Date/ health	Milestone 2	Date/ health	Milestone 3	Date/ health
	🟥		🟩		🟨

Overall health

🟨 Progess has slowed

Background

Next steps

Resources

Activities and milestones

Activity/milestone	Delivery date (✓=completed)
Activity 1	
Activity 2	
Milestone 1	
Activity 3	

Issues

Risks

Legend:

🟥	Progress has stopped
🟨	Progess has slowed
🟩	No impediments

Source: GAO analysis of I&A quad charts.

The left quadrants of the chart define interim activities and milestones, and track progress toward both. Components categorize the health of each initiative as having no impediments (green), or that its progress has slowed (yellow) or stopped (red). The right quadrants contain narrative information, including issues facing the initiative—such as inadequate funding or technological or legal difficulties encountered—and risks to progress, such as the impact of an initiative's inability to meet time frames.[43]

The board reviews the Quad Charts on a quarterly basis to track and oversee progress, and can question components on the initiatives and the status of milestones. For example, one initiative (Common Operating Picture/User-Defined Operating Picture Integrated Project Team) experienced challenges in setting milestones, which was reflected in its chart. Subsequently, the board pushed the relevant components to set more aggressive milestones, and, as a result, DHS expects to begin transitioning components from over 20 different common operating pictures to about 5 common operating pictures in March 2013, which, according to DHS officials, is earlier than would have been possible without the board's involvement. When the transition has been completed, DHS will have streamlined the applications that collect, share, and display the information components need to plan for and respond to threats and hazards, which will increase efficiencies, according to DHS officials.

The Quad Charts track progress that initiatives are making toward interim activities and milestones, but do not include information regarding completion dates or what difference the initiatives are making in improving information sharing. For example, a LEISI program official said that LEISI identifies milestones for the charts that can be accomplished each year, but the LEISI chart does not show how much closer that year's targets will advance the initiative toward completing its information-sharing functions. Including completion dates in the charts could help the board better understand the overall progress initiatives made, make more informed decisions on which initiatives it will advocate should receive additional funding, and generally provide better oversight by holding components accountable for these completion dates. In addition, the charts do not provide information on how effective initiatives have been. For example, the charts do not provide a sense of any improvements in how ICE shares law enforcement information with key stakeholders as a

[43] The charts only track progress on the information-sharing portions of component programs and not the overall programs. For example, CBP and ICE are updating the system they use to track and manage cases involving decisions about whether individuals planning to enter the United States are admissible or pose a security threat (TECS Modernization). While CBP and ICE are responsible for managing the overall program, the board uses the Quad Chart to track progress on efforts to share information from the system with internal and external customers.

result of implementing LEISI, such as how many more data sets are available to share or the increase in the number of users with access to these data sets. Including such information in the Quad Chart could help the board assess how initiatives improve DHS information sharing, including the impact of any risks identified in the chart. According to DHS officials, the lower left quadrant of the chart is intended to show longer-term activities and milestones leading toward completion, but our review shows that 15 of the 18 initiatives did not have completion milestones as of June 2012. DHS officials stated that it will not be possible to identify completion dates for some initiatives, such as for CHISE, because they are in the early planning stages and responsible components cannot yet estimate their completion. Moreover, other initiatives, such as the Nationwide Suspicious Activity Reporting Initiative, are secretarial priorities that DHS will not remove from the list of key initiatives because they are ongoing initiatives with no date for completion.

DHS officials recognize they need to better track the progress of key initiatives and assess how they affect sharing with customers, but related efforts are just beginning and DHS did not have further details on what changes they will make. Program management practices note the importance of establishing a timeline for program milestones and deliverables, including when a program is complete, which helps lay the groundwork for the program and position it for successful execution. These practices also note that it is important to track intermediate and final results of a program as well as the benefits a program delivers, which helps ensure the organization will realize and sustain the benefits from its investment.[44] We recognize that completion dates cannot be provided in each case. However, determining and documenting initiative completion dates and assessing how initiatives affect sharing, where feasible, would help the board better track progress in implementing the initiatives, make any necessary course corrections if completion dates are delayed, and demonstrate how initiatives enhance information sharing and homeland security.

[44] Project Management Institute, *The Standard for Program Management®*.

DHS Is Assessing Technology and Fusion Center Capabilities Needed to Share Information, but Could Better Determine How Technology Capabilities Are Helping Achieve 2015 Vision

In addition to identifying and tracking key information-sharing initiatives it needs to implement, DHS has also taken several steps to assess the capabilities that programs need so that key partners can access and share information the department owns. First, DHS has begun to assess the extent to which its technology programs have implemented critical information-sharing capabilities. DHS officials stated that from April through July 2012, the Information Sharing Environment Coordination Activity conducted initial baseline assessments of approximately 160 technology programs, systems, and initiatives—which include the key information-sharing initiatives—to determine the extent to which they have critical information-sharing capabilities in place. Capabilities include, for example, ways to determine that a user who is trying to access DHS information is authorized to access it and the ability to subsequently audit or track who has accessed this information.[45] DHS officials noted that the Office of the CIO and board plan to track the progress that individual information-sharing programs and initiatives achieve in implementing these capabilities, as applicable, and develop a mechanism to provide DHS better visibility over the capabilities that programs have implemented and still need to implement. DHS officials stated that they plan to introduce this capability-tracking mechanism in early 2013.

DHS's planned capability-tracking mechanism may not include an important step to help DHS determine its progress toward its 2015 information-sharing vision. The *Information Sharing Segment Architecture Transition Plan* discusses major milestones and time frames for implementing the critical capabilities in order for DHS to achieve its information-sharing vision by 2015. However, this plan does not detail—and DHS officials said that they have not determined—the specific capabilities each particular program must implement for DHS to conclude that it has improved information sharing enough to achieve the 2015 information-sharing vision. For example, the transition plan notes that DHS is to have begun developing the framework for establishing how to

[45] The seven critical capabilities are (1) information sharing environment governance and implementation; (2) service-oriented architecture, which is to help the department move away from manual data exchanges and more quickly exchange information; (3) identity, credential, and access management; (4) electronic directory services, which allow users to find the location of people, organizations, and data across security domains within DHS and with partners; (5) discovery service, which provides a repository for information-sharing agreements, among other things; (6) delivery service; and (7) user presentation/interface. According to DHS officials, not all programs will need to implement all of the capabilities.

authorize user access by the end of fiscal year 2012, but it does not include which programs this capability is relevant for, and how many of them must implement this capability for DHS to be able to conclude that it has made meaningful progress in that capability by 2015. DHS officials recognize the importance of measuring progress toward the 2015 vision, but the department's efforts to define critical capabilities are new and it has not yet taken this step. Including this step in the department's efforts to develop its capability-tracking mechanism would help DHS better understand which programs to prioritize to improve information sharing.

Our past work and the experience of leading organizations have demonstrated that measuring performance allows organizations to track progress they are making toward intended results—including goals, objectives, and targets they expect to achieve—and gives managers critical information on which to base decisions for improving their programs.[46] The Information Sharing Environment Coordination Activity charter also notes that this group is to provide the board with the ability to prioritize and oversee steps DHS is taking to achieve its information-sharing vision. Determining the specific capabilities certain programs must implement in order for DHS to achieve its 2015 vision and subsequently tracking annual progress could help DHS prioritize programs and track and assess progress toward ensuring that the right information is getting to the right people at the right time to meet their homeland security responsibilities.

Second, in addition to tracking the capabilities of its own programs, DHS, in conjunction with the Department of Justice, is collecting information on the extent to which fusion centers are putting in place certain capabilities that the two agencies and other federal interagency partners have determined are critical for ensuring these centers can effectively operate in a national information-sharing network. States and major urban areas originally created fusion centers to provide information about threats within the centers' jurisdictions. The federal government, particularly through DHS, has been leveraging such centers to further disseminate federal information on threats and to collect information on threats and pass it on to federal agencies, among other things. I&A collaborated with the fusion center directors and their interagency partners to design and

[46] For example, see GAO-05-927, and *Program Evaluation: Studies Helped Agencies Measure or Explain Program Performance*, GAO/GGD-00-204 (Washington, D.C.: Sept. 29, 2000).

implement the 2011 Fusion Center Assessment, which is to help DHS track the progress of fusion centers in achieving key capabilities. These include the capability to receive, analyze, and further disseminate information on terrorist threats and crimes that can be precursors to terrorism. DHS completed its initial assessment in October 2011 and issued a report on its results in June 2012.[47] The assessment found that overall capability scores for the 72 fusion centers that participated ranged from 29 to 97 out of 100, with an average score of 77. The report stated that the national network is a long-term investment and made recommendations on how DHS and its federal interagency partners can help fusion centers fill gaps over the next 4 years. DHS officials said that they will look at trends in individual fusion center scores to identify what capability gaps exist across the National Network of Fusion Centers and work with centers to focus any federal resources they receive on filling these gaps. DHS plans to monitor the improvements that centers make over time in filling capability gaps as an indicator of the effectiveness of fusion centers.

Third, as part of its continued efforts to integrate the various components that were folded into DHS when it was created, I&A led an effort to review all of the legacy information-sharing agreements that different components had in place to help ensure components had the capability to share information seamlessly with each other. To track the progress of this effort, DHS developed a performance measure on the percentage of existing external information-sharing and access agreements that allow for sharing of information with all DHS components that have an authorized purpose for that information.[48] For example, if ICE had an agreement with a foreign country to share law enforcement information, other DHS components that have an authorized purpose for that information would also have access to that information. DHS increased the percentage of agreements that provided for sharing across all of DHS from less than 3 percent in fiscal year 2009 to 97 percent in fiscal year 2012, which exceeded the fiscal year 2012 target of 85 percent. As a result, DHS officials stated that the department plans to retire this performance measure and replace it with one that measures the

[47] DHS, 2011 National Network of Fusion Centers: Final Report (Washington D.C.: May 2012).

[48] Information-sharing and access agreements are vehicles used by DHS to exchange, receive, and share information from external (non-DHS) parties.

outcomes of executing these agreements. Specifically, DHS plans to assess customer satisfaction of the recipients of multiple data sets received through these agreements beginning in October 2012.

Customer Feedback Can Provide Perspectives on the Usefulness of Information Shared

DHS's key initiatives and capabilities should help to increase the department's ability to make components' information available to important customers, and to disseminate components' products and reports created for these customers.[49] However, determining whether the right people have the right information at the right time requires obtaining views from customers about the accuracy, usefulness, and timeliness of information provided and shared. DHS components are in the process of implementing customer feedback mechanisms that should help to provide customers' perspectives of how well DHS is meeting its 2015 vision.

Information and Intelligence Products

DHS has taken steps to survey customers to measure how satisfied they are with the information and intelligence products that DHS components disseminate, such as homeland security assessments and homeland information notes.[50] Such customer satisfaction data are important measures that help to gauge the usefulness of the information provided. DHS recognizes that there is a potential for bias in survey results, but DHS is taking steps to obtain feedback in additional ways, such as meeting with its customers to assess their needs, as a means to improve intelligence products.

DHS measures customer satisfaction by attaching surveys to information and intelligence products or sending surveys separately to customers following the dissemination of a product. I&A and TSA have developed and implemented surveys that gauge customer satisfaction with the usefulness of information in these products and other DHS intelligence

[49] For the purposes of this report, DHS customers are entities that consume DHS intelligence products. These entities include federal, state, local, tribal, territorial, and private sector partners. In addition, DHS components consume intelligence products developed and distributed by other DHS components, such as I&A.

[50] Homeland security assessments provide in-depth analysis based on detailed research. Homeland security notes provide information or analysis on a recent or current event or development of interest to DHS customers.

components are following suit.[51] Component surveys include a common question that asks customers to rate satisfaction on a five-point scale—very satisfied, somewhat satisfied, neither satisfied nor dissatisfied, somewhat dissatisfied, or very dissatisfied—and DHS customer satisfaction performance measures report the percentage of intelligence products rated somewhat satisfied or very satisfied. DHS plans to aggregate survey results on this question from across the DHS Intelligence Enterprise components, use the data as a gauge on how the information provided contributed to success in achieving goals for missions areas—such as preventing terrorist attacks—and publish the results in the department's *Annual Performance Report* as performance measures, beginning in 2013. For example, TSA disseminated about 11,000 incident reports that pertain to preventing terrorist attacks during the first two quarters of 2012 and received about 5,800 responses. Over the same time period, I&A distributed 41 reports pertaining to preventing terrorist attacks and received over 700 responses.[52] These data show that customers who responded to the surveys said that they were generally satisfied with the reports they reviewed during that time frame. I&A data for fiscal year 2011 also show that customers said they were generally satisfied with products disseminated that year. These customer feedback mechanisms should help to provide customers' perspectives of how well DHS is meeting its 2015 vision.

However, I&A recognizes that the survey results may not be representative of the entire population of customers that received those products because customers voluntarily choose whether or not to provide feedback. In internal documents and external reports on customer feedback, such as the I&A annual report to Congress, I&A cautions readers that survey results are subject to bias that prevents the organization from drawing conclusions about the entire I&A customer

[51] As of June 2012, U.S. Citizenship and Immigration Services—the agency responsible for overseeing lawful immigration to the United States—and ICE have also implemented a survey but have not received any feedback to support the associated performance measures. Ultimately, the survey will also be used by the Coast Guard and CBP.

[52] According to DHS officials, it is not possible to calculate a response rate because they do not know how many customers have read the reports.

population.[53] For example, a bias is created by the requirement that a customer read a product in order to take the survey—meaning that the feedback of those who read the product and chose to provide feedback may not be representative of those customers that decided not to read an I&A product. Given this potential for bias in I&A data, any performance measures drawn from that data will carry that bias, providing DHS, Congress, and taxpayers with a potentially incomplete account of progress made in improving information sharing. According to DHS officials, because of technological limitations in tracking the dissemination of products, I&A does not know the number of recipients or readers of each product, which prevents I&A from knowing the full impact of this bias.

I&A has taken a number of steps to obtain feedback in other ways and help ensure it provides customers with the right information at the right time. For example, according to I&A officials, I&A has initiated a core customer study designed to establish a common definition of core customers, allowing I&A to identify and directly survey representative samples of customers from across each segment on their satisfaction with I&A's intelligence support. However, the study is in the beginning phases; thus I&A has not yet established a completion date and it is too early to evaluate the results. In addition, I&A has established a Customer Feedback Working Group to analyze feedback-related issues and devise ways to improve products. For example, on the basis of feedback that I&A products did not contain enough relevant local content, the group has begun a project to improve the regional content in intelligence products, according to I&A officials. Further, I&A conducts targeted surveys on high-interest topical issues to assess its performance on sharing terrorism-related intelligence and information.

Our discussions with various DHS customers indicate varying levels of satisfaction with terrorism-related information from DHS and its components, including I&A and TSA. According to DHS officials, the department has prioritized its customers, and the department funds

[53] See I&A, *Voluntary Feedback from State, Local, Tribal, and Private Sector Consumers, 2010 Report to Congress* (November 8, 2010). Pursuant to the Homeland Security Act of 2002, as amended, the Secretary of DHS is to submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives an annual report describing consumer feedback it obtains and, if applicable, how DHS adjusts its production of intelligence products in response to such consumer feedback. See 6 U.S.C. § 124h(g).

information-sharing initiatives according to these priorities. This, in turn, can affect how relevant some of the customers find DHS and its components' information to their mission. For example, fusion centers are higher-priority customers than customers in the intelligence community, such as the FBI, according to the *I&A Strategic Plan*. As a result, DHS officials stated that the department focuses more of its funding and initiatives on fusion centers. We interviewed senior officials from 10 state and major urban area fusion centers, ICE, ODNI, and the FBI.[54] We supplemented our discussions with additional information, such as the results of a 2012 fusion center survey about counterterrorism intelligence and our prior survey on TSA customers.[55] The results of our analysis are summarized below.

- *Fusion centers*: Directors and other senior officials in 8 of 10 fusion centers we spoke with generally found I&A information to be useful.[56] For example, officials at 1 fusion center reported that I&A products keep officials up to date on national and global terrorism trends that may have an impact on their region. In addition, officials at another fusion center stated that reports, such as the Joint Intelligence Briefing from DHS and the FBI on the 10th anniversary of 9/11, and special assessments of security at sporting events, have helped the fusion center provide guidance to state and local law enforcement. Further, in response to an I&A report on radicalization of prison inmates, 1 fusion center's detectives met with corrections department staff to enhance their awareness of prison radicalization and held trainings on suspicious activities and radicalization indicators. Moreover, officials at this center noted that the timely dissemination of reports has improved, that reports are more specific to regional needs than in the past, and that I&A has responded to fusion center feedback. However, officials at 2 other fusion centers we met with stated that I&A information was not always timely. These officials

[54] Because we selected a nonprobability sample of customers to contact, the information we obtained may not be generalized to all customers. We discussed with these entities their satisfaction with information from DHS components, and I&A specifically, but not all entities provided responses for each of these sources of information, and others provided satisfaction with the department as a whole.

[55] GAO, *Transportation Security Information Sharing: Stakeholders Generally Satisfied but TSA Could Improve Analysis, Awareness, and Accountability*, GAO-12-44 (Washington, D.C.: Nov. 21, 2011).

[56] Two fusion centers did not directly answer the question.

reported that sometimes, I&A information is already available through media outlets or other information sources. According to one official, although this practice can be considered a method to verify the recent news media information, the volume of information tends to flood the network and can lead to reduced attention being paid to I&A products. In addition, officials at 2 fusion centers we met with reported that I&A distributes too many reports that are not specific to their region. Further, results from a 2012 Homeland Security Policy Institute survey that asked fusion center staff to order their most important sources of information suggest that DHS may have opportunities to better meet customer needs.[57] On the basis of the fusion center officials who responded—which, according to survey authors come from traditional law enforcement backgrounds that may influence their rankings—DHS ranked sixth after sources such as law enforcement and Joint Terrorism Task Forces. Other sources, such as the National Counterterrorism Center and other fusion centers, ranked lower than DHS.[58]

- *TSA customers*: We previously reported on the extent to which TSA customers are satisfied with the security-related information products they receive and found that they were generally satisfied.[59] Specifically, TSA has developed a series of products to share security-related information with transportation stakeholders, such as annual modal threat assessments that provide an overview of threats to each transportation mode—including aviation, rail, and highway—and related infrastructure. Fifty-seven percent of the customers we surveyed (155 of 275 who answered this question) indicated that they were satisfied with the products they receive.

- *ICE*: ICE directors and analysts in the Homeland Security Intelligence Office did not comment on the information contained in I&A reports, but noted that they were generally dissatisfied with I&A reports primarily because they found it difficult to determine which reports are most relevant to their needs. For example, the officials stated that I&A is not proactive in informing ICE about the products it completes and

[57] The George Washington University Homeland Security Policy Institute, *Counterterrorism Intelligence: Fusion Center Perspectives* (Washington D.C.: June 2012).

[58] The survey results are based on a nonprobability sample. Although these results are not generalizable, they indicate variability in satisfaction among DHS's customer base.

[59] GAO-12-44.

would find useful. ICE officials stated that connectivity and access to I&A products have improved since 2010, but the ease of finding these products and understanding what is relevant to ICE remains problematic.

- *ODNI*: ODNI officials stated that they were generally satisfied with the department's responsiveness to information needs and that collaboration with DHS has improved since 2010. For example, if circumstances necessitate ODNI obtaining passenger manifest data, DHS provides such information more quickly than in the past. In addition, ODNI has successfully used DHS data to counter potential terrorist threats. For example, by cross-checking refugee application data from DHS with other data, ODNI has facilitated numerous arrests and removed over 500 people who posed a potential threat from the refugee stream prior to their arrival in the United States. However, ODNI officials stated that some DHS intelligence reports are not timely enough for their needs. Further, DHS's finished intelligence products are generally not as valuable to the intelligence community because they are generally written for state and local customers.[60]

- *FBI*: Two FBI headquarters divisions responsible for sharing terrorism-related information reported on their satisfaction with information from DHS. Specifically, officials from one of the two FBI divisions reported that, overall, the division was neither satisfied nor dissatisfied with I&A information, and officials from the other division reported their division was somewhat satisfied. These same officials also reported that they were very satisfied with the information received from CBP, ICE, and TSA. For example, the FBI officials reported that its Counterterrorism Division and ICE have enhanced the consistency with which information is shared and have worked toward a transparent and coordinated effort for developing, sharing, and distributing terrorism-related information. The FBI reported that DHS intelligence products are generally not produced for the FBI's use specifically, and that the FBI collaborates with DHS to develop reports on a variety of topics, such as potential terrorist attacks.

Reports Responding to Customer Needs

DHS also monitors the extent to which I&A finished intelligence products address issues that state, local, and tribal customers deemed as most

[60] Finished intelligence has been reviewed and correlated with data from other available sources.

critical to their needs, which could increase customer satisfaction with products. Customers articulate their critical needs based on 10 threat-based categories, such as Terrorism and Illicit Drug Operations.[61] I&A tags its intelligence products and information reports with relevant "standing information needs" prior to distribution, which enables I&A to monitor the extent to which I&A is distributing products and reports that match customers' needs.[62] The 2011 annual performance report shows that I&A determined that 85 percent of finished intelligence products were directly responsive to its state, local, and tribal customers' information needs, which met the performance target for this measure. I&A data show that the department reached similar conclusions during the first two quarters of 2012.[63] According to DHS officials, additional components are beginning to tag their information reports and intelligence products with relevant standing information needs, which will enable DHS to assess departmentwide contributions to addressing crucial customer needs.

Requests for Information

I&A also provides customers with information based on specific requests and collects data on the extent to which I&A is timely in its responses and customers are satisfied with those responses. Customer satisfaction is based on three factors: quality of communication, the accuracy of the information provided, and satisfaction with the process. Specifically, customers request certain information from I&A—such as background information for a person of interest—and I&A officials are to respond to that request by an agreed-upon time frame.[64] The 2011 annual performance report shows that I&A answered 85 percent of requests

[61] According to an I&A official, going forward, DHS will not report this measure externally because management decided the measure does not broadly apply to the department. However, I&A plans to continue to track the measure and use it for decision making.

[62] I&A defines these critical needs as "any subject, general or specific, for which there is a continuing need for intelligence, which will establish a foundation for guiding intelligence collection efforts and reporting activities." Examples include the need for information on individuals or groups that are capable of attacking critical infrastructure and key resources, and emerging cross-border connections between transnational criminal organizations or gangs.

[63] First quarter 2012 data show that 87 percent of DHS reports were directly responsive to its customers' information needs, while second quarter results were 85 percent.

[64] DHS also collects customer satisfaction data on requests customers send to the National Operations Center. This entity collects and fuses information from more than 35 federal, state, territorial, tribal, local, and private sector agencies. The National Operations Center coordinates information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents.

within the time frame I&A and the customer agreed upon to the customer's satisfaction. Since I&A is currently updating this measure to include other DHS entities, 2012 is a baseline year that the department plans to use to evaluate the extent to which timeliness and satisfaction of information requests are improving over time. Therefore, this measure should help DHS determine to what extent customers are getting the right information at the right time.

Carrying Through on Plans to Develop More Meaningful Ways to Assess the Impacts of Information-Sharing Efforts Will Be Important

DHS has plans that could help it better assess the impact of the department's information sharing on homeland security. After DHS releases its new *Information Sharing and Safeguarding Strategy*, the department plans to develop and implement a new DHS sharing and safeguarding performance management program that is to include the development of performance measures that determine the outcomes its information sharing is to achieve. Our work has shown that DHS is evolving from utilizing process measures that are relatively easy to implement—for example, counting the number of issued reports—to more meaningful measures that determine customer satisfaction with the usefulness of the information provided.[65] Demonstrating results is a standard practice in performance measurement. DHS continues to recognize that it must develop measures that demonstrate the results of its efforts, and department officials noted that such measures will be a crucial part of the *Information Sharing and Safeguarding Implementation Plan* the department is to develop. Specifically, the department's draft planning documents note that the board is to develop information-sharing outcome measures to determine whether federal and nonfederal customers receive DHS information that is timely, accurate, trusted, and useful; meets their needs; and contributes to securing the homeland. For example, DHS could enhance its customer satisfaction performance measures by asking customers what difference the product they reviewed

[65] See, for example, GAO, *Information Sharing: DHS Could Better Define How it Plans to Meet Its State and Local Mission and Improve Performance Accountability*, GAO-11-223 (Washington D.C.: Dec. 16, 2010); *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, GAO-09-399 (Washington, D.C.: Sept. 30, 2009); and *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-454 (Washington, D.C.: Aug. 17, 2007). Performance measures can be categorized as (1) output measures, which describe the direct products or services delivered by a program or activity; (2) process measures, which address the type or level of program activities conducted, such as timeliness or quality; or (3) outcome measures, which describe the results of carrying out a program or activity.

made on their ability to ensure a safe and secure homeland. The board is also to develop measures that assess the impact of information sharing on preventing terrorism and enhancing security, as well as other missions. Further, the board is to develop measures that assess the degree of budget and outcome alignment, and calculate the cost of achieving information-sharing outcomes and target levels of performance.[66]

We will continue to monitor DHS's efforts to assess the results and impact of its sharing efforts. Our work has shown that having the ability to monitor progress and demonstrate results helps to lower the risks posed from implementing programs critical to the nation, such as the sharing of information on terrorist threats. Executing its plans to develop better measures should help DHS assess the progress in sharing information and monitor the extent to which the department is achieving its 2015 vision to provide the right information to the right people at the right time.

Conclusions

Ensuring that terrorism-related information is shared in an efficient manner with stakeholders across all levels of government, the private sector, and foreign countries is a challenging and critical task. DHS has demonstrated a strong commitment to advance information-sharing efforts; its key information-sharing initiatives have made progress, and most have met interim milestones. The department has also taken steps to track its information-sharing efforts and developed information-sharing performance measures that monitor the effectiveness of some information-sharing efforts. However, additional steps could help DHS sustain these efforts. For example, in its *Roadmap Implementation Guide* or other policies and procedures, documenting processes for identifying information-sharing gaps and the results; documenting and implementing a process for analyzing the root causes of those gaps; and establishing and documenting a process for potential future use for identifying, assessing, and mitigating the risk of removing an incomplete initiative from the list would provide DHS with an institutional record to better replicate, and therefore sustain, its information-sharing efforts. Moreover, defining the milestones that initiatives must achieve in order to be

[66] According to DHS officials, these plans are tied to the forthcoming *DHS Information Sharing and Safeguarding Strategy* and its associated implementation plan. As noted earlier in this report, DHS officials stated that they are waiting to release this strategy until after the new *National Information Sharing and Safeguarding Strategy* is released.

considered complete and determining what difference the initiatives are making in information sharing could help the board better track progress in implementing the initiatives, make any necessary course corrections, and make future investment decisions. Further, determining the specific capabilities certain programs must implement in order for DHS to achieve its 2015 vision and subsequently tracking annual progress toward achieving these capabilities could help DHS prioritize programs and investments, and track and assess progress toward meeting homeland security responsibilities.

Recommendations for Executive Action

We recommend that the Secretary of Homeland Security take the following five actions.

- To address information-sharing gaps and risks, direct the Information Sharing and Safeguarding Governance Board to, in either its *Roadmap Implementation Guide* or other related policies and procedures,
  - document its processes for identifying information-sharing gaps and the results;
  - document and implement a process for analyzing the root causes of those gaps; and
  - establish and document processes for identifying and assessing risks of removing initiatives from the list, as well as determining whether other initiatives or alternative solutions are needed to mitigate any significant risks related to the relevant information-sharing gap.

- To improve DHS's ability to track and assess key information-sharing initiatives,
  - direct the Information Sharing and Safeguarding Governance Board to incorporate into the board's existing tracking process milestones with time frames that initiatives must achieve to be considered complete, where feasible, and information to show the impact initiatives are having on information sharing, and
  - direct the Information Sharing and Safeguarding Governance Board and the Office of the CIO to include in the mechanism the board is developing to track programs' achievement of key capabilities the specific capabilities certain programs must implement in order to achieve the department's 2015 information-sharing vision.

Agency Comments and Our Evaluation

We provided a draft of this report to DHS, ODNI, and the FBI on August 14, 2012, for review and comment. On September 5, 2012, DHS provided written comments, which are reprinted in appendix II. In commenting on the report, DHS stated that it concurred with all five recommendations and identified actions taken or planned to implement them.

DHS concurred with the first recommendation, to direct the Information Sharing and Safeguarding Governance Board to document its processes for identifying information-sharing gaps and the results. DHS stated that the department, through the board, has recently initiated an effort to draft a DHS-wide *Information Sharing and Safeguarding Implementation Plan*. The implementation plan is to ensure that DHS's sharing and safeguarding activities align with the forthcoming *Fiscal Year 2012–2017 DHS Information Sharing and Safeguarding Strategy*. DHS stated that the templates that the department will use to develop the implementation plan will identify information-sharing and -safeguarding gaps and the anticipated results. DHS also plans to update its *Roadmap Implementation Guide* to provide the department with an institutional record to better replicate, and therefore sustain, ongoing and future implementation efforts to improve information-sharing and -safeguarding. DHS also concurred with the second recommendation, to direct the Information Sharing and Safeguarding Governance Board to document and implement a process for analyzing the root causes of those gaps. DHS stated that the templates that the department will use to develop the implementation plan will identify the specific root causes of information-sharing and -safeguarding gaps for the initiatives contained in the implementation plan. DHS also plans to update its *Roadmap Implementation Guide* to document the processes by which it identifies the root causes of the gaps. DHS stated that this effort will better ensure that the department invests in the correct information-sharing solutions and effectively reduces risks. DHS concurred with the third recommendation, to direct the Information Sharing and Safeguarding Governance Board to establish and document processes for identifying and assessing risks of removing initiatives from the list, as well as determining whether other initiatives or alternative solutions are needed to mitigate any significant risks related to the relevant information-sharing gap. DHS stated that it plans to establish and document such processes, and also plans to update its *Roadmap Implementation Guide* to document the processes by which it identifies and assesses risks. DHS stated that preliminary planning to address this recommendation has begun.

DHS concurred with the fourth recommendation, to direct the Information Sharing and Safeguarding Governance Board to incorporate into the board's existing tracking process milestones with time frames that initiatives must achieve to be considered complete, where feasible, and information to show the impact initiatives are having on information sharing. DHS stated that the board will incorporate the recommended changes into its tracking process, and that preliminary planning to address this recommendation has begun. DHS also concurred with the fifth recommendation, to direct the Information Sharing and Safeguarding Governance Board and the Office of the CIO to include in the mechanism the board is developing to track programs' achievement of key capabilities the specific capabilities certain programs must implement in order to achieve the department's 2015 information-sharing vision. DHS stated that the board and the Office of the CIO will include the recommended changes in the mechanism, and stated that preliminary planning to address this recommendation has begun.

If fully implemented, DHS's planned efforts will address the intent of the five recommendations.

DHS and the FBI also provided us with technical comments, which we considered and incorporated in the report where appropriate. ODNI did not have comments on the draft report.

We are sending copies of this report to the Secretary of Homeland Security, the Director of National Intelligence, the Attorney General, and appropriate congressional committees. This report is also available at no charge on GAO's web site at http://www.gao.gov.

If you or your staff have any questions, please contact me at (202) 512-6510 or larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Staff acknowledgments are provided in appendix III.

Eileen Regen Larence

Eileen R. Larence
Director
Homeland Security and Justice Issues

List of Requesters

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

The Honorable Peter T. King
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Patrick Meehan
Chairman
The Honorable Brian Higgins
Ranking Member
Subcommittee on Counterterrorism and Intelligence
Committee on Homeland Security
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our reporting objectives were to review the extent to which the Department of Homeland Security (DHS) (1) has made progress since 2010 in achieving its information-sharing mission, and what related challenges exist, if any, and (2) tracks and assesses information-sharing improvements.[1] To determine the extent to which DHS has made progress in achieving its information-sharing mission, we analyzed relevant strategic planning documents, such as DHS's January 2011 *Integrated Strategy for High Risk Management*, the *DHS Information Sharing Strategy*, the *2007 National Strategy for Information Sharing*, and the *Office of Intelligence & Analysis (I&A) Strategic Plan 2011-2018*.[2] In addition, to determine the extent of DHS leadership's demonstrated commitment to information sharing, we analyzed documents related to DHS's governance structure for information sharing, including charters that are current as of September 2012 and meeting minutes for relevant governing bodies from January 2011 through April 2012.

To determine the extent to which DHS has developed information-sharing plans and identified key efforts, we analyzed documents related to DHS's plans and initiatives for sharing, such as DHS's list of key information-sharing initiatives, and analyzed documents from one initiative—the Law Enforcement Information Sharing Initiative (LEISI)—which is led by DHS's U.S. Immigration and Customs Enforcement (ICE). We selected this initiative as an example case study of DHS's actions related to information-sharing initiatives because it is a priority initiative and an established program.[3] To determine the extent to which DHS's other key information-sharing initiatives have made progress, we analyzed DHS documents tracking those initiatives. To determine the extent to which DHS has the resources needed to achieve its information-sharing mission, we analyzed documents related to DHS's budget, including the DHS fiscal year 2013 Budget in Brief, and the funding status of key information-sharing initiatives. To determine the extent to which DHS has the technology needed for information sharing, we analyzed documents related to DHS's technology framework for information sharing, such as

[1] Although the high-risk area focuses on sharing terrorism-related information, many of the programs and efforts discussed in this report relate to DHS's efforts to share types of information beyond terrorism-related information.

[2] While DHS has made recent efforts to also improve the safeguarding of information, this was outside the scope of our review and is therefore not addressed in this report.

[3] LEISI was 1 of DHS's 18 key information-sharing initiatives as of September 2012.

the *Information Sharing Segment Architecture Transition Plan*, among other things.

In addition, we interviewed program officials within DHS's I&A to obtain information on the department's information-sharing mission, goals, programs, activities, and funding; the Segment Architecture; efforts to improve terrorism-related information sharing; and related challenges. We interviewed ICE officials about LEISI's progress and their experiences working with I&A on improving DHS's information sharing. To determine the progress DHS has made on the technology framework for information sharing and on the funding of information-sharing programs, we interviewed officials from DHS's Office of the Chief Information Officer (CIO). We assessed DHS's plans and efforts against *Standards for Internal Control in the Federal Government* and criteria that we use in assessing high-risk issues.[4] We also reviewed DHS's efforts related to its Segment Architecture against our prior report and federal guidance on defining architecture content.[5]

To determine the extent to which DHS tracks and assesses information-sharing improvements, we analyzed relevant strategic planning documents, such as the *I&A Strategic Plan* for fiscal years 2011-2018 and the February 2010 *Quadrennial Homeland Security Review* (QHSR). Furthermore, to determine how DHS tracks progress and results in its information-sharing initiatives, we analyzed documentation and examples of DHS's tracking mechanisms for its information-sharing efforts. We analyzed documentation and data on DHS's performance measures for fiscal years 2011 and 2012 to determine the extent to which DHS is monitoring the effectiveness of information sharing. We also used these DHS performance measurement data to determine if DHS could demonstrate progress in information sharing by analyzing data for customer feedback and customer information needs, among other areas. To assess the reliability of the data obtained from DHS, we analyzed performance measurement documentation and interviewed officials knowledgeable about the controls over the integrity of the data. On the basis of our assessments, we determined that the performance measurement data were sufficiently reliable for the purposes of this

[4] See GAO/AIMD-00-21.3.1 and GAO-01-159SP.

[5] See GAO-11-455. See also Federal Segment Architecture Working Group, *Federal Segment Architecture Methodology Version 1.0,* December 2008.

report. In addition, we interviewed program officials within I&A and from DHS's Office of the CIO on I&A's and DHS's progress in sharing terrorism-related information, and on mechanisms they use to monitor effectiveness.

To supplement the steps we took to assess how DHS tracks and assesses information-sharing improvements, we also obtained information from various customers of DHS's information sharing on the usefulness of I&A and other DHS components' products. Specifically, we obtained information from 10 of 77 fusion center customers, 1 of 7 DHS operational components who participate in the DHS Intelligence Enterprise, and 2 of DHS's 16 intelligence community customers.[6] We interviewed or received written input from directors and other senior officials from 10 fusion centers—where states and major urban areas collaborate with federal agencies to improve information sharing—including the President of the National Fusion Center Association. The national network of fusion centers is the hub of much of the two-way intelligence and information flow between the federal government and state, local, tribal and territorial partners, making fusion centers key customers of I&A's intelligence reports. Because we selected a nonprobability sample of fusion centers to contact, the information we obtained from these locations may not be generalized to all fusion centers nationwide. However, because we selected these centers based on, among other things, geographic dispersion and variation in risk based on the Department of Justice's (DOJ) 25 Cities Project, the information we gathered from these locations provided us with an understanding of similarities and differences in fusion centers' satisfaction with DHS's information sharing across different centers.[7] We interviewed ICE officials

[6] According to the Under Secretary for Intelligence and Analysis, departmental intelligence programs, projects, activities, and personnel—including the intelligence elements of key operational components, as well as I&A—make up the DHS Intelligence Enterprise.

[7] The 25 Cities Project refers to the High-Risk Metropolitan Area Interoperability Assistance Project, a DOJ Wireless Management Office grant program that identified the top 25 metropolitan areas that were considered likely targets for terrorist attack and provided communication solutions to federal and local authorities such as fire, police, and emergency medical services. Projects differ from city to city.

from the Homeland Security Investigations and Intelligence office[8] and officials from the Office of the Director of National Intelligence's (ODNI) National Counterterrorism Center (NCTC).[9] Further, we received written input from two headquarters divisions of the Federal Bureau of Investigation (FBI) that are responsible for sharing terrorism-related information. We selected ICE, ODNI, and the FBI because they are key customers of DHS's intelligence products or partner with I&A to create these products. ICE is a DHS component that shares terrorism-related information and leads two of DHS's key information-sharing initiatives. ODNI and the FBI are federal agencies that have key roles in analyzing terrorism threats to the United States and jointly issue products with DHS. The FBI also has the primary role in carrying out investigations within the United States of threats to national security. The views of ICE, ODNI, and the FBI are not generalizable to all of DHS's federal customers, but they provided us with a general understanding of the perspectives about DHS's information sharing held by different customer types nationwide. To supplement these views, we reviewed our prior work on DHS customer satisfaction and analyzed a report from a survey on information sharing conducted by the George Washington University Homeland Security Policy Institute and discussed the report with a representative who conducted the survey.[10] In January and February 2012, the institute administered a 78 question self-completion survey to individuals working in 72 state and major urban area fusion centers, and 71 individuals voluntarily took the survey. On average, 48 to 49 individuals answered each question. Our analysis included reviewing the methodology and assumptions of the study, and discussing the study's scope and conclusions with the George Washington University Homeland Security

[8] ICE's Homeland Security Investigations directorate is responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within, and out of the United States. The Homeland Security Investigations Intelligence Office is an intelligence force that supports the enforcement needs of ICE's executive leadership and operational field units.

[9] NCTC serves as the primary organization in the federal government for integrating and analyzing intelligence pertaining to counterterrorism, except for information pertaining exclusively to domestic terrorism. NCTC integrates foreign and domestic analysis from across the intelligence community and produces a wide range of detailed assessments designed to support senior policymakers and other members of the policy, intelligence, law enforcement, defense, homeland security, and foreign affairs communities.

[10] See GAO-12-44 and the George Washington University Homeland Security Policy Institute, *Counterterrorism Intelligence: Fusion Center Perspectives*.

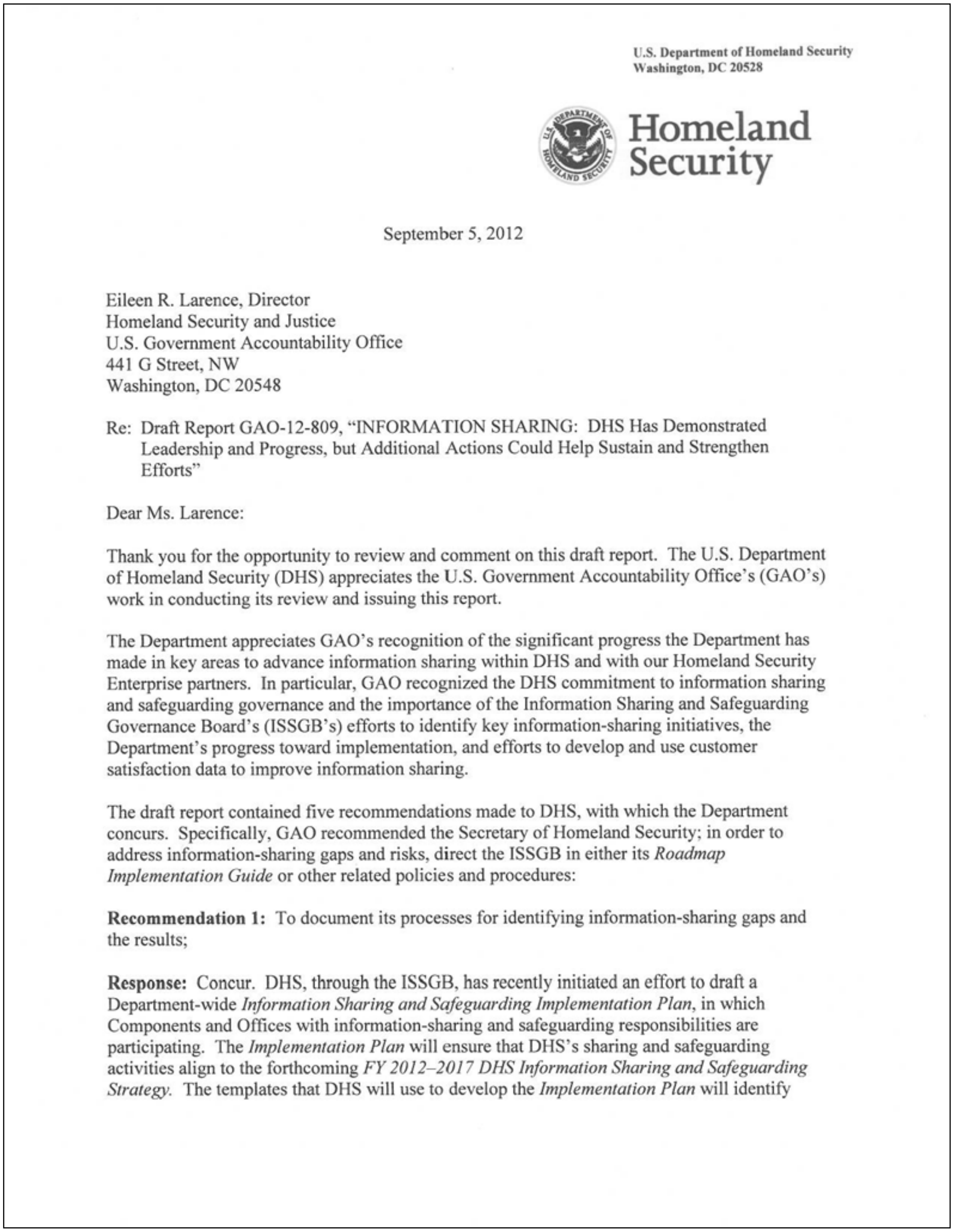
Policy Institute.[11] As a result of our review and analysis, we determined that the study and its results were appropriate for use in our report. We assessed DHS's mechanisms to track and assess information-sharing improvements against criteria for practices in program management.[12]

We conducted this performance audit from November 2011 through September 2012 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.

[11] Founded in 2003, the George Washington University Homeland Security Policy Institute is a nonpartisan think tank whose mission is to build bridges between theory and practice to advance homeland security through an interdisciplinary approach.

[12] For example, see Project Management Institute, *The Standard for Program Management*®; GAO-05-927; and GAO/GGD-00-204.

Appendix II: Comments from the Department of Homeland Security



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

Homeland
Security

September 5, 2012

Eileen R. Larence, Director
Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-12-809, "INFORMATION SHARING: DHS Has Demonstrated Leadership and Progress, but Additional Actions Could Help Sustain and Strengthen Efforts"

Dear Ms. Larence:

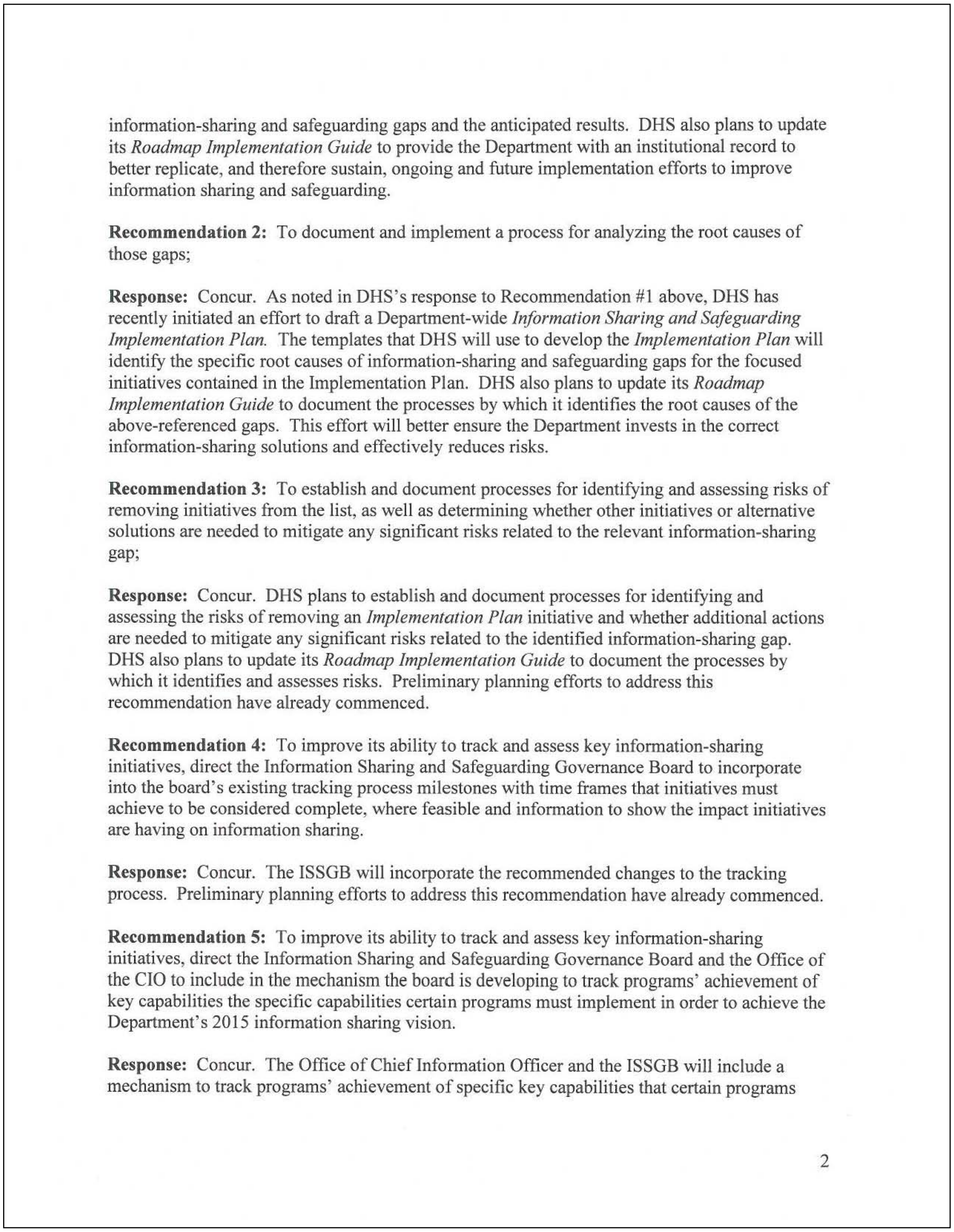
Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in conducting its review and issuing this report.

The Department appreciates GAO's recognition of the significant progress the Department has made in key areas to advance information sharing within DHS and with our Homeland Security Enterprise partners. In particular, GAO recognized the DHS commitment to information sharing and safeguarding governance and the importance of the Information Sharing and Safeguarding Governance Board's (ISSGB's) efforts to identify key information-sharing initiatives, the Department's progress toward implementation, and efforts to develop and use customer satisfaction data to improve information sharing.

The draft report contained five recommendations made to DHS, with which the Department concurs. Specifically, GAO recommended the Secretary of Homeland Security; in order to address information-sharing gaps and risks, direct the ISSGB in either its *Roadmap Implementation Guide* or other related policies and procedures:

Recommendation 1: To document its processes for identifying information-sharing gaps and the results;

Response: Concur. DHS, through the ISSGB, has recently initiated an effort to draft a Department-wide *Information Sharing and Safeguarding Implementation Plan*, in which Components and Offices with information-sharing and safeguarding responsibilities are participating. The *Implementation Plan* will ensure that DHS's sharing and safeguarding activities align to the forthcoming *FY 2012–2017 DHS Information Sharing and Safeguarding Strategy*. The templates that DHS will use to develop the *Implementation Plan* will identify



information-sharing and safeguarding gaps and the anticipated results. DHS also plans to update its *Roadmap Implementation Guide* to provide the Department with an institutional record to better replicate, and therefore sustain, ongoing and future implementation efforts to improve information sharing and safeguarding.

Recommendation 2: To document and implement a process for analyzing the root causes of those gaps;

Response: Concur. As noted in DHS's response to Recommendation #1 above, DHS has recently initiated an effort to draft a Department-wide *Information Sharing and Safeguarding Implementation Plan.* The templates that DHS will use to develop the *Implementation Plan* will identify the specific root causes of information-sharing and safeguarding gaps for the focused initiatives contained in the Implementation Plan. DHS also plans to update its *Roadmap Implementation Guide* to document the processes by which it identifies the root causes of the above-referenced gaps. This effort will better ensure the Department invests in the correct information-sharing solutions and effectively reduces risks.

Recommendation 3: To establish and document processes for identifying and assessing risks of removing initiatives from the list, as well as determining whether other initiatives or alternative solutions are needed to mitigate any significant risks related to the relevant information-sharing gap;

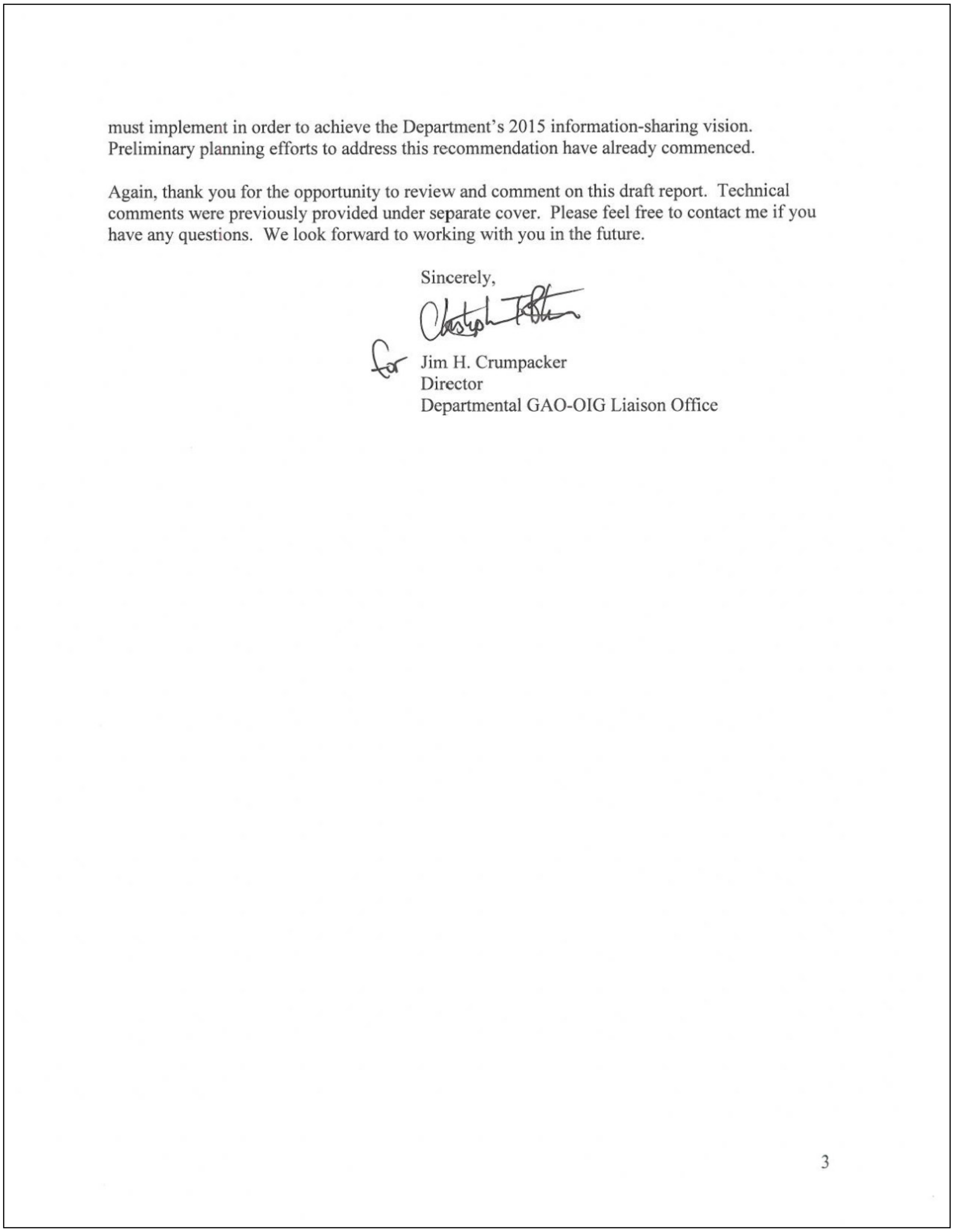
Response: Concur. DHS plans to establish and document processes for identifying and assessing the risks of removing an *Implementation Plan* initiative and whether additional actions are needed to mitigate any significant risks related to the identified information-sharing gap. DHS also plans to update its *Roadmap Implementation Guide* to document the processes by which it identifies and assesses risks. Preliminary planning efforts to address this recommendation have already commenced.

Recommendation 4: To improve its ability to track and assess key information-sharing initiatives, direct the Information Sharing and Safeguarding Governance Board to incorporate into the board's existing tracking process milestones with time frames that initiatives must achieve to be considered complete, where feasible and information to show the impact initiatives are having on information sharing.

Response: Concur. The ISSGB will incorporate the recommended changes to the tracking process. Preliminary planning efforts to address this recommendation have already commenced.

Recommendation 5: To improve its ability to track and assess key information-sharing initiatives, direct the Information Sharing and Safeguarding Governance Board and the Office of the CIO to include in the mechanism the board is developing to track programs' achievement of key capabilities the specific capabilities certain programs must implement in order to achieve the Department's 2015 information sharing vision.

Response: Concur. The Office of Chief Information Officer and the ISSGB will include a mechanism to track programs' achievement of specific key capabilities that certain programs



must implement in order to achieve the Department's 2015 information-sharing vision. Preliminary planning efforts to address this recommendation have already commenced.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

for Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

3

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Eileen R. Larence, (202) 512-6510 or larencee@gao.gov

Staff Acknowledgments

In addition to the contact named above, David A. Powner (Director), Eric Erdman (Assistant Director), Anh Le (Assistant Director), Paul A. Hobart, Karl W. Seifert, Rebecca Kuhlmann Taylor, and Ashley D. Vaughan made significant contributions to the report. Also contributing to this report were Virginia A. Chanley, Tracy J. Harris, Eric D. Hauswirth, Kevin J. Heinz, Lisa Humphrey, Jeff R. Jensen, Justine C. Lazaro, Thomas Lombardi, Jan B. Montgomery, Jessica S. Orr, Anthony K. Pordes, and William M. Reinsberg.

(441021)

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 website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://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 website, 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.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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