United States Government Accountability Office

GAO

Statement for the Record To the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, October 12, 2011

INFORMATION SHARING

Progress Made and Challenges Remaining in Sharing Terrorism-Related Information

Statement of Eileen R. Larence
Director, Homeland Security and Justice Issues

October 12, 2011

INFORMATION SHARING

Progress Made and Challenges Remaining in Sharing Terrorism-Related Information

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-144T, a statement for the record to the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

A breakdown in information sharing was a major factor contributing to the failure to prevent the September 11, 2001, terrorist attacks. Since then, federal, state, and local governments have taken steps to improve sharing. This statement focuses on government efforts to (1) establish the Information Sharing Environment (ISE), a government-wide approach that facilitates the sharing of terrorism-related information; (2) support fusion centers, where states collaborate with federal agencies to improve sharing; (3) provide other support to state and local agencies to enhance sharing; and (4) strengthen use of the terrorist watchlist. GAO's comments are based on products issued from September 2010 through July 2011 and selected updates in September 2011. For the updates, GAO reviewed reports on the status of Department of Homeland Security (DHS) efforts to support fusion centers, and interviewed DHS officials regarding these efforts. This statement also includes preliminary observations based on GAO's ongoing watchlist work. For this work, GAO is analyzing the guidance used by agencies to nominate individuals to the watchlist and agency procedures for screening individuals against the list, and is interviewing relevant officials from law enforcement and intelligence agencies, among other things.

What GAO Recommends

GAO is not making new recommendations, but has made recommendations in prior reports to federal agencies to enhance information sharing. The agencies generally agreed and are making progress, but full implementation of these recommendations is needed.

View GAO-12-144T. For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov.

What GAO Found

The government continues to make progress in sharing terrorism-related information among its many security partners, but does not yet have a fully-functioning ISE in place. In prior reports, GAO recommended that agencies take steps to develop an overall plan or roadmap to guide ISE implementation and establish measures to help gauge progress. These measures would help determine what information sharing capabilities have been accomplished and are left to develop, as well as what difference these capabilities have made to improve sharing and homeland security. Accomplishing these steps, as well as ensuring agencies have the necessary resources and leadership commitment, should help strengthen sharing and address issues GAO has identified that make information sharing a high-risk area.

Federal agencies are helping fusion centers build analytical and operational capabilities, but have more work to complete to help these centers sustain their operations and measure their homeland security value. For example, DHS has provided resources, including personnel and grant funding, to develop a national network of centers. However, centers are concerned about their ability to sustain and expand their operations over the long term, negatively impacting their ability to function as part of the network. Federal agencies have provided guidance to centers and plan to conduct annual assessments of centers' capabilities and develop performance metrics by the end of 2011 to determine centers' value to the ISE. DHS and the Department of Justice are providing technical assistance and training to help centers develop privacy and civil liberties policies and protections, but continuous assessment and monitoring policy implementation will be important to help ensure the policies provide effective protections.

In response to its mission to share information with state and local partners, DHS's Office of Intelligence and Analysis (I&A) has taken steps to identify these partner's information needs, develop related intelligence products, and obtain more feedback on its products. I&A also provides a number of services to its state and local partners that were generally well received by the state and local officials we contacted. However, I&A has not yet defined how it plans to meet its state and local mission by identifying and documenting the specific programs and activities that are most important for executing this mission. The office also has not developed performance measures that would allow I&A to demonstrate the expected outcomes and effectiveness of state and local programs and activities. In December 2010, GAO recommended that I&A address these issues, which could help it make resource decisions and provide accountability over its efforts.

GAO's preliminary observations indicate that federal agencies have made progress in implementing corrective actions to address problems in watchlist-related processes that were exposed by the December 25, 2009, attempted airline bombing. These actions are intended to address problems in the way agencies share and use information to nominate individuals to the watchlist, and use the list to prevent persons of concern from boarding planes to the United States or entering the country, among other things. These actions can also have impacts on agency resources and the public, such as traveler delays and other inconvenience. GAO plans to report the results of this work later this year.

Chairman Lieberman, Ranking Member Collins, and Members of the Committee:

I am pleased to submit this statement on the progress federal agencies have made and the challenges they face in sharing and managing terrorism-related information.[1] The nation just passed the 10-year anniversary of the September 11, 2001, terrorist attacks. The 9/11 Commission concluded that a breakdown in information sharing was a major factor contributing to the failure to prevent those attacks. Since then, enactment of the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act) and other legislation called for substantial changes in the way agencies share information on terrorist threats.[2] In addition, federal, state, and local governments have taken steps to improve information sharing. However, in part based on the December 25, 2009, attempted airline bombing, questions have been raised about how well the government is using and sharing terrorism-related information to identify potential threats that individuals may pose. These acts of terrorism on U.S. soil underscore the importance of the federal government's continued need to ensure 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.

Since January 2005, we have designated terrorism-related information sharing as high risk because the government continues to face serious challenges in analyzing key information and sharing it among federal, state, local, and other security partners in a timely, accurate, and useful way. We have since monitored federal efforts to implement the Information Sharing Environment (ISE)—a government-wide approach that facilitates the sharing of terrorism-related information, which may

[1] Terrorism-related information includes homeland security, terrorism, and weapons of mass destruction information. See 6 U.S.C. §§ 482(f)(1), 485(a)(1), (5)-(6).

[2] See, e.g., Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016, 118 Stat. 3638, 3664-70 (codified as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 504, 121 Stat. 266, 313-17, at 6 U.S.C. § 485).

include any method deemed necessary and appropriate.[3] This area remained high risk in our February 2011 update.[4]

A major focus of the ISE has been to improve the sharing of terrorism-related information between the federal government and state and local security partners. After the terrorist attacks of September 11, 2001, state and local governments began to establish fusion centers to address gaps in terrorism-related information sharing that the federal government cannot address alone and provide a mechanism for information sharing within the state. Pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), the Department of Homeland Security (DHS) created the State, Local, and Regional Fusion Center Initiative to establish partnerships with state, local, and regional fusion centers.[5] In coordination with fusion centers and the states, DHS is to take steps to support efforts to integrate the centers into the ISE, assign personnel to centers, and provide training and funding, among other things. In recent years, fusion centers have been credited with being influential in disrupting a planned terrorist attack on the New York City subway system, investigating bomb threats against U.S. airlines, and providing intelligence support to several political conventions and summits. Today, there are 72 fusion centers nationwide.[6]

In addition to supporting fusion centers, DHS has responsibility for, among other things, sharing terrorism-related information with its state and local partners, as appropriate. DHS's Office of Intelligence and Analysis (I&A) is the lead DHS component with responsibilities for

[3] See 6 U.S.C. § 485(a)(3).

[4] GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 16, 2011).

[5] See Pub. L. No. 110-53, § 511, 121 Stat. at 317-24 (codified at 6 U.S.C. § 124h).

[6] All 50 states have designated a primary fusion center to serve as the focal point for information sharing. According to the Office of the Program Manager for the ISE, 1 of the 50 states has not yet established the capabilities to be recognized by the federal government. In general, these fusion centers are statewide in jurisdiction and are operated by state entities, such as the state police or bureau of investigation. In addition, 22 major urban areas have established their own fusion centers, which are regional centers that usually cover large cities with substantial populations and numerous critical infrastructure sites and may be operated by city or county law enforcement or emergency management agencies. For purposes of this report, "fusion centers" is used to refer to both state and major urban area fusion centers.

meeting this mission. We have assessed, at the Congress' request, how well the office has been able to meet this mission and give priority to state and local sharing from among I&A's other competing functions. The results of this work are discussed later in this statement.

Another way the government uses information sharing as a counterterrorism tool is through the terrorist watchlist process. The attempt on December 25, 2009, to detonate a concealed explosive onboard a U.S.-bound aircraft raised questions as to why warnings about the attempted bomber did not result in the U.S. government including him in its consolidated terrorist database. The Terrorist Screening Center—administered by the Federal Bureau of Investigation—is responsible for maintaining this list of known or suspected terrorists and making information from the Terrorist Screening Database (TSDB) available, as appropriate, to agencies that screen individuals for possible threats. For instance, subsets of the TSDB are used by DHS's Transportation Security Administration (TSA) to screen individuals before they board an aircraft and by U.S. Customs and Border Protection to screen travelers entering the United States.

My statement discusses the results of our work in monitoring four important information sharing issues: (1) progress made and work remaining in establishing the ISE; (2) federal agencies' efforts to help fusion centers build capabilities; (3) how DHS has responded to its statutory mission to share terrorism-related information with state and local partners; and (4) government actions to improve the watchlist process as a result of the December 2009 attempted airline bombing.

This statement is based on products we issued from September 2010 through July 2011 and selected updates in September 2011.[7] In conducting our prior work, we analyzed documents, including key statutes, agency policies, and best practices. We also interviewed officials at the various federal, state, and local entities with responsibilities for

[7] This statement is primarily based on our most recent reports on the ISE, fusion centers, and I&A. See, GAO, *Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investments*, GAO-11-455 (Washington, D.C.: July 21, 2011); *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results*, GAO-10-972 (Washington, D.C.: Sept. 29, 2010); and *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).

information sharing initiatives that are discussed in this statement. Our previously published reports contain additional details on the scope and methodology for those reviews. For the updates, we reviewed documentation on the status of DHS's efforts to support fusion centers and interviewed DHS officials regarding these efforts. This statement is also based on our ongoing work on the terrorist watchlist that we are conducting for this Committee, the House Committee on Homeland Security, and the House Committee on Oversight and Government Reform. For this ongoing work, we are analyzing the guidance used by agencies to nominate individuals to the watchlist and agency procedures for screening individuals against the list, and interviewing relevant officials from law enforcement and intelligence agencies, among other things. We conducted all of our work 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.

Agencies Have Improved Sharing as They Build the ISE, but a Better Roadmap and System of Accountability Could Guide Future Development

ISE Has Improved Sharing By Advancing Goals and Priority Programs

In our July 2011 report, we noted that the Program Manager for the ISE and key security agencies have continued to make progress in addressing issues that keep terrorism-related information sharing on our high-risk list.[8] For example, they developed a corrective action plan—or framework—to implement a set of initial goals and priority programs that

[8] GAO-11-455.

help to establish the ISE, partly responding to recommendations we made in 2008.[9] Goals included reducing barriers to sharing and improving information sharing practices with federal, state, local, tribal, and foreign partners. Priority programs included developing common information sharing standards; building a national integrated network of fusion centers; implementing a system whereby state and local partners can report suspicious activity; and controlling and handling sensitive but unclassified information. Activities under the framework also included establishing information sharing incentive programs for federal employees and strengthening privacy, civil rights, and civil liberties considerations. The administration has recognized, however, that the framework was useful in promoting this initial set of programs and activities, but it did not define what the fully functioning ISE is to achieve and include. Therefore, as discussed in the following sections, the framework does not provide the comprehensive roadmap that is needed to further develop and implement the ISE going forward.

More Fully Defining the ISE, Related Costs, and What Work Remains Would Help Provide a Roadmap and Accountability for Results

Defining an End State Vision

The Program Manager has acknowledged the importance of defining what the ISE is intended to achieve and include—or the "end state" vision—and noted that he is doing so as part of ongoing efforts to update the 2007 National Strategy for Information Sharing. He said that this update will drive future ISE implementation efforts and will help individual agencies adapt their information sharing policies, related business processes, architectures, standards, and systems to effectively operate within the ISE. The Program Manager also noted that after development of the end state vision is completed, supporting implementation plans will be needed to help guide achievement of the vision, including plans that define what activities and initiatives will be needed to achieve the end

[9] See 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).

state and guide ISE development and implementation. Such plans would be consistent with our recommendation for a roadmap if they contain key elements such as roles, responsibilities, and time frames for these activities, among other things.

Leveraging Agency Initiatives

Consistent with the Intelligence Reform Act, the ISE is to provide the means for sharing terrorism-related information across five communities—homeland security, law enforcement, defense, foreign affairs, and intelligence—in a manner that, among other things, leverages ongoing efforts. As we reported in July 2011, the ISE has primarily focused on the homeland security and law enforcement communities and related sharing between the federal government and state and local partners, in part to align with information sharing priorities outlined by the administration. We recognize that recent homeland security incidents and the changing nature of domestic threats make continued progress in improving sharing between federal, state, and local partners critical. However, consistent with the Intelligence Reform Act, the ISE is intended to provide the means for sharing terrorism-related information across all five communities.

The Program Manager and ISE agencies have not yet ensured that initiatives within the foreign affairs, defense, and intelligence communities have been fully leveraged by the ISE to enhance information sharing within and across all communities. For example, according to Department of State (State) officials, the department shares terrorism-related information with other agencies through a variety of efforts and initiatives related to national and homeland security, but State initiated these efforts independently and not through the Office of the Program Manager. According to the Program Manager, State also possesses information about entrants to the country that could be valuable to the ISE. However, in April 2011, State officials said that the Office of the Program Manager had not contacted the department's coordinator for the ISE to request information on programs or initiatives related to people entering the country to determine if this information could be useful to the broader ISE communities. Further, intelligence agencies have technology initiatives—including new ways of ensuring that authorized users have access to, and are able to search across, classified systems and networks to facilitate information sharing—but it is not clear to what extent transferring this best practice to non-classified information is being considered under the ISE.

The Program Manager also noted that his office has engaged all five communities in ISE activities. For example, in addition to working with the homeland security and law enforcement communities, he said his office

has worked with State to standardize terrorism-related information sharing agreements with foreign governments; with the Department of Defense to develop information technology standards that allow different agencies to exchange information; and the intelligence community to develop terrorism-related information products for state, local, and tribal governments. He also noted that all five communities have been afforded opportunities to help set ISE programmatic priorities. However, the Program Manager and agencies had not yet taken actions to ensure that all relevant information sharing initiatives across the five communities are fully leveraged, which could help enhance information sharing government-wide. In our July 2011 report, we recommended that they take such actions. They generally agreed and have started to address this issue.

Defining Incremental Costs

The Program Manager and agencies have not yet identified the incremental costs necessary to implement the ISE, as envisioned by the Intelligence Reform Act. Our prior work shows that cost information can help agencies allocate resources and investments according to priorities and constraints, track costs and performance, and shift such investments and resources as appropriate.[10] We recognize that developing accurate and reliable incremental cost estimates for the ISE is a difficult undertaking, complicated further by the fact that the Program Manager and agencies are still defining what the ISE is, is to include, and is to attain. In our July 2011 report, we recommended that the Program Manager—in coordination with the Office of Management and Budget—task the key ISE agencies to define, to the extent possible, the incremental costs needed to help ensure successful implementation of the ISE. The Program Manager acknowledged the importance of identifying incremental costs and noted that the Office of the Program Manager will continue to work directly with the Office of Management and Budget to provide agencies with budget guidance that calls for them to identify their costs to implement the ISE.

Demonstrating Progress

The Intelligence Reform Act requires the Program Manager to, among other things, monitor implementation of the ISE by federal departments and agencies to ensure adequate progress is being made and regularly report the findings to Congress. In June 2008, we reported that the Office of the Program Manager was monitoring ISE implementation—as

[10] See GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

demonstrated through its annual report to Congress—but that such monitoring did not include an overall assessment of progress in implementing the ISE and how much work remained. Thus, we recommended, among other things, that the Program Manager develop a way to measure and demonstrate results and to show the extent to which the ISE had been implemented, as well as more fully define the key milestones needed to achieve the ISE.[11] The Program Manager generally agreed and in January 2011, the Information Sharing and Access Interagency Policy Committee (ISA IPC) and the Office of the Program Manager initiated an effort to make ISE priority programs and related goals more transparent and to better monitor progress.[12] Specifically, according to the Deputy Program Manager, agencies that are responsible for implementing ISE priority programs are leading efforts to establish 3-, 6-, and 12-month goals for these programs. Information on progress made in reaching these goals may be included in future ISE annual reports. In addition he explained that the Office of the Program Manager is working with agencies to develop a performance management framework that will be linked to the updated national strategy. These actions should help to provide an accurate accounting for progress to Congress and other stakeholders and would be consistent with the criteria we use to evaluate a program's risk, which calls for a way to demonstrate progress and results.

Governing the ISE

Our prior work on high-risk issues shows that a strong commitment from top leadership to address problems and barriers to sharing terrorism-related information is important to reducing related risks. In July 2009, the White House established the ISA IPC to subsume the role of its predecessor interagency body—the Information Sharing Council.[13] The Program Manager at that time cited concerns about the Program Manager's authority and provided recommendations intended to help

[11] GAO-08-492.

[12] Interagency Policy Committees—within the Executive Office of the President—are the main day-to-day fora for interagency coordination of national security policy, providing policy analysis and ensuring timely responses to decisions made by the President. See, Executive Office of the President, *Presidential Policy Directive-1: Organization of the National Security Council System* (Washington, D.C.: Feb. 13, 2009).

[13] The Information Sharing Council—composed of senior representatives from federal departments and agencies, some of who possess and acquire terrorism-related information—was established in accordance with the Intelligence Reform Act to assist the President and the Program Manager with their ISE responsibilities. See 6 U.S.C. § 485(g).

strengthen the ISE effort.[14] For example, among other things, he recommended that the Program Manager be appointed by the President and serve as co-chair of the ISA IPC. Subsequently, both changes were implemented, which were intended to bring high-level policy decision making and oversight to the development of the ISE. At the time of our review, it was too early to tell how the new structure would impact the continued development and implementation of the ISE and if the Program Manager's new role would provide him sufficient leverage and authority to ensure that agencies fully participate in the ISE.

The Enterprise Architecture Management Foundation for Supporting ISE Implementation Could Be Improved

In our July 2011 report, we noted that the process of defining an enterprise architecture (EA) for the ISE could help the Program Manager and agencies in their efforts to define the current operational and technological capabilities within the ISE, the future capabilities needed, and a plan to transition between the two.[15] Under an EA approach, agencies are to define the business processes involved in information sharing, map out the exchange of information to be achieved, and build the technology and other resources they need to accomplish the sharing in their EA plans and budget requests, among other things. Doing so could help the government more fully define the necessary components of the ISE. We reported that agencies had begun to build ISE initiatives, such as suspicious activity reporting, into their EAs. To better define ISE EA guidance and effectively manage EA architecture, we recommended that the Program Manager, ISA IPC, and agencies establish an EA management plan for the ISE to improve ISE EA management practices and address missing architecture content and a mechanism to ensure implementation. The Program Manager and the Office of Management

[14] Beyond ISE Implementation: Exploring the Way Forward for Information Sharing: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security, 111th Cong. 5 (2009) (statement of Ambassador Thomas E. McNamara, Program Manager, Information Sharing Environment, Office of the Director of National Intelligence).

[15] An EA can be viewed as a reference or "blueprint" for achieving strategic business goals and outcomes, including maximizing information sharing within and across organization boundaries. A well-defined EA provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., federal department or agency) or a functional or mission area that cuts across more than one organization (e.g., homeland security) by documenting the entity's current operational and technological environment and its target environment, as well as a plan for transitioning from the current to the target environment.

and Budget generally agreed and are taking steps to address the intent of this recommendation.

Federal Agencies Are Helping Fusion Centers Build Capabilities, but Have More Work to Help Them Sustain Operations and Measure Their Value

Federal Agencies Have Provided Resources to Develop a National Fusion Center Network, but Centers Are Concerned about Sustaining Operations

The federal government recognizes that fusion centers represent a critical source of local information about potential threats, including homegrown terrorism, and a means to disseminate terrorism-related information and intelligence from federal sources. DHS, which has a statutory lead for state and local information sharing, in collaboration with the Department of Justice (DOJ) and the Program Manager for the ISE, has taken steps to partner with and leverage fusion centers—a top priority for the ISE. In accordance with the 9/11 Commission Act, over the years, DHS has provided centers with a variety of support, including personnel assigned to centers, access to classified and unclassified homeland security and terrorism information and systems, training and technical assistance, and federal grant funding. For instance, as of July 2010, DHS had deployed 74 intelligence officers to fusion centers. In addition, states have reported to DHS that they have used about $426 million in grant funding from fiscal year 2004 through 2009 to support fusion-related activities nationwide.[16]

[16] The $426 million in grant funding was as of June 16, 2010, and included all Federal Emergency Management Agency (FEMA) preparedness grant programs. This funding was for activities aligned to project types that support fusion center activities, such as the following: establish/enhance a terrorism intelligence/early warning system, center, or task force; establish/enhance public-private emergency preparedness program; and develop/enhance homeland security/emergency management organization and structure. Funding data are self-reported by grantees and, according to FEMA officials, are not validated to ensure that funds were exclusively used to support fusion center activities.

In September 2010, we reported that fusion centers cited federal funding as critical to their long-term sustainability and to achieving and maintaining a set of baseline capabilities. These baseline capabilities were defined by the federal government and fusion centers as being necessary for centers to be considered capable of performing basic functions in the national information sharing network. They include, for example, capabilities related to information gathering, recognition of indicators and warnings, and intelligence and information dissemination. According to a survey of all fusion centers conducted by DHS and the Program Manager for the ISE, of the 52 fusion centers that responded, on average, over half of their 2010 budgets were supported by federal funding.[17]

Concerns about and challenges related to funding for sustainability are long-standing issues. Fusion centers do not have their own federal funding source but must compete each year with other state homeland security, law enforcement, and emergency management agencies and missions for a portion of the total federal homeland security grant funding awarded to each state. We and others have reported on the centers' concerns about the lack of a predictable funding source. For example, in September 2010 we reported that officials in all 14 fusion centers we contacted stated that without sustained federal funding, centers could not expand operations to close the gaps between their current operations and the baseline capabilities, negatively impacting their ability to function as part of the national network.[18]

Senior DHS officials have acknowledged the fusion centers' concerns and in an effort to further prioritize the development of the national network of fusion centers, DHS revised fiscal year 2011 grant guidance. It now requires, among other enhancements, that (1) each state submit a fusion center investment justification and (2) the justification must be related to mitigating capability gaps.[19] Nevertheless, concerns about federal funding

[17] This figure is based on information reported to the Program Manager of the ISE by 52 of 72 fusion centers. Information was aggregated, but not verified, by the Program Manager or GAO.

[18] GAO-10-972.

[19] A fusion center typically contributes to the development of a state's federal grant application by providing information on how it will use the proposed funding needed, called an investment justification.

could be exacerbated given that overall homeland security grant funding of $2.1 billion for fiscal year 2011 is $780 million less than the previous year.

Federal Agencies Plan to Assess Centers' Capabilities and Develop Performance Metrics to Determine Centers' Value to the ISE

Consistent with efforts to develop this national network of fusion centers, federal agencies have also issued a series of guidance documents, including the baseline capabilities, to support fusion centers in establishing their operations.[20] The baseline capabilities are intended to help ensure that a fusion center will have the necessary structures, processes, and tools in place to support the gathering, processing, analysis, and dissemination of terrorism, homeland security, and law enforcement information.

As a first step, the Program Manager for the ISE, DHS, and DOJ conducted a systematic assessment of centers' capabilities in 2010 and analyzed results to identify strengths, gaps, and weaknesses across the national network of fusion centers. The assessment specifically focused on four operational capabilities identified as critical which are generally defined as a fusion center's ability to receive, analyze, disseminate, and gather information.[21] The assessment also focused on centers' progress in implementing privacy, civil rights, and civil liberties protections. The results of this assessment and a subsequent survey effort conducted in January 2011 showed that over half of the 72 fusion centers had developed and implemented a final written plan, policy, or standard operating procedure to achieve three of the four capabilities—receive (44 centers), disseminate (46 centers), and gather (42 centers). However, 37 centers indicated that they had not implemented a plan related to developing capabilities to analyze time sensitive information.

[20] Global Justice Information Sharing Initiative, *Baseline Capabilities for State and Major Urban Area Fusion Centers, A Supplement to the Fusion Center Guidelines* (September 2008).

[21] According to DHS, personnel from DHS, the Program Manager for the ISE, and DOJ coordinated with state and local government representatives and fusion center officials to jointly identify these critical operational capabilities to be prioritized in developing the national network of fusion centers. Specifically, the four operational capabilities are defined as: (1) receive: ability to receive classified and unclassified information from federal partners; (2) analyze: ability to assess local implications of threat information through the use of a formal risk assessment process; (3) disseminate: ability to further disseminate threat information to other state, local, tribal, territorial, and private sector entities within their jurisdiction; and (4) gather: ability to gather locally generated information, aggregate it, analyze it, and share it with federal partners as appropriate.

According to DHS officials who oversee the fusion center initiative, using the results of the 2010 assessment, along with feedback obtained from fusion center directors, DHS developed and implemented a Fusion Center Assessment Process in 2011. This process will be conducted annually to identify capability gaps, enable gap mitigation planning, and continue to drive the allocation of resources to mitigate those gaps. DHS expects to release the results of the 2011 assessment in January 2012, according to DHS officials.

We also reported in September 2010 that if centers are to receive continued federal financial support, it is important that they are also able to demonstrate their impact and value added to the national network and the nation's overall information sharing goals. However, the federal government had not established standard performance measures that it could use across all fusion centers to assess their contributions. We recommended that DHS define the steps it needed to take to design and implement a set of measures and commit to a target timeframe for their completion. According to senior DHS officials overseeing the office, in March 2011, the State and Local Program Office and a representative group of fusion center directors began developing an overarching strategy document to define the vision, mission, goals, objectives, and specific outcomes that fusion centers will be expected to achieve, and associated performance measures for the national network of fusion centers. According to these officials, such performance measures are to be in place by the end of 2011.

DHS and DOJ Are Helping Centers Develop Privacy and Civil Liberties Policies and Protections but Monitoring Implementation Will Be Important

Because fusion centers collect, analyze, and disseminate information on potential criminal and terrorist threats, some entities, such as the American Civil Liberties Union, have raised concerns that centers are susceptible to privacy and civil liberties violations. We reported in September 2010 that consistent with federal requirements, DHS and DOJ have provided technical assistance and training to help centers develop privacy and civil liberties policies and protections. For example, DHS and DOJ provided fusion centers with guidance and technical assistance, including a template on which to base a privacy policy and a process for reviewing centers' policies to ensure they are consistent with federal requirements. DHS reported that all operational fusion centers now have a final, approved privacy policy in place that is at least as comprehensive

as the ISE Privacy Guidelines.[22] With respect to training, we reported that DHS, in partnership with DOJ and other entities, has implemented a three-part training and technical assistance program in support of fusion centers' efforts to provide appropriate privacy, civil rights, and civil liberties training for personnel. We also reported that DHS, in conjunction with DOJ and the Program Manager for the ISE, was taking steps to assess the implementation of centers' privacy protections to ensure that the protections described in centers' policies were implemented in accordance with all applicable privacy regulations, laws, and constitutional protections. Federal agencies are also encouraging centers to assess their own protections to identify any existing privacy and civil liberties risks and to develop strategies to mitigate the risks. Continuous assessment and monitoring are key steps to help ensure that fusion centers are implementing privacy and civil liberties protections and that DHS, and other federal agencies, are supporting them in their efforts.

DHS Has Enhanced Support to State and Local Partners but Could Better Define the Actions It Will Take to Meet This Mission and Measure Progress

In addition to supporting fusion centers, DHS is responsible for sharing terrorism-related information with its state and local partners, and within DHS, I&A is the designated lead component for this mission. In December 2010, we reported that I&A had initiatives underway to identify state and local information needs, developing intelligence products to meet these needs, and obtaining more detailed feedback on the timeliness and usefulness of these products, among other things.[23] I&A also provided a number of services to its state and local partners—primarily through fusion centers—that were generally well received by the state and local officials we contacted. For example, in addition to deploying personnel and providing access to networks disseminating classified and unclassified information, I&A provides training directly to state and local personnel and operates a 24-hour service to respond to state and local requests for information and other support.

[22] In 2006, the Program Manager for the ISE issued the ISE Privacy Guidelines, which establish a framework for sharing information in the ISE in a manner that protects privacy and other legal rights. The ISE Privacy Guidelines apply to federal departments and agencies and, therefore, do not directly impose obligations on state and local government entities. However, the ISE Privacy Guidelines do require federal agencies and the Program Manager for the ISE to work with nonfederal entities, such as fusion centers, seeking to access protected information to ensure that the entities develop and implement appropriate policies and procedures that are at least as comprehensive as those contained in the ISE Privacy Guidelines.

[23] GAO-11-223.

We also reported that a Congressional committee that had been trying to hold I&A accountable for achieving its state and local mission was concerned about I&A's inability to demonstrate the priority and level of investment it is giving to this mission compared to its other functions, as evidenced by hearings conducted over the past several years. We reported that, historically, I&A had focused its state and local efforts on addressing statutory requirements and responding to I&A leadership priorities. However, I&A had not yet defined how it plans to meet its state and local information-sharing mission by identifying and documenting the specific programs and activities that are most important for executing this mission. Our prior work has found that successful organizations clearly articulate the programs and activities that are needed to achieve specified missions or results, and the organization's priorities, among other things.[24]

Further, we reported that I&A had not defined what state and local information-sharing results it expected to achieve from its program investments and the measures it would use to track the progress it is making in achieving these results. For example, all of I&A's state and local measures provided descriptive information regarding activities and services that I&A provided, such as the percentage of fusion centers with I&A personnel and the number of requests for support. However, none of these measures accounted for the actual results, effects, or impacts of programs and activities or the overall progress I&A is making in meeting its partners' needs. For example, the personnel measure did not provide information related to the effectiveness of the I&A personnel or the value they provide to their customers, such as enhanced information sharing, analytic capabilities, and operational support.

To help I&A strengthen its efforts to share information with state and local partners, we recommended, among other things, that I&A (1) identify and document priority programs and activities related to its state and local mission, and (2) take actions to develop additional performance measures that gauge the results that I&A's information-sharing efforts have achieved and how they have enhanced homeland security. By taking these steps, I&A could potentially increase the usefulness of its products and services; the effectiveness of its investments; and the

[24] See, for example, GAO, *Results-Oriented Government: GPRA Has Established a Solid Foundation for Achieving Greater Results*, GAO-04-38 (Washington, D.C.: Mar. 10, 2004).

organization's accountability to Congress, key stakeholders, and the public. DHS agreed with these recommendations and expects to address them as part of new strategic planning efforts.

Agencies Are Addressing Watchlisting Gaps but Could Benefit from Assessing Impacts of Changes

The Executive Office of the President's review of the December 2009 attempted airline bombing found that the U.S. government had sufficient information to have uncovered and potentially disrupted the attack, but shortcomings in the nominations process resulted in the failure to nominate the attempted bomber for inclusion in the Terrorist Screening Database.[25] Thus, screening agencies that could have identified him as a potential threat were unable to identify him and take action. The Executive Office of the President tasked departments and agencies to undertake a number of corrective actions to help address such gaps.[26] We have ongoing work to assess the changes implemented and their impacts. This work is assessing (1) the actions the federal government has taken since the attempted attack to strengthen the watchlist nominations process, as well as any resulting challenges and impacts; (2) how the composition of the TSDB changed as a result of agency actions; and (3) how screening agencies are addressing vulnerabilities exposed by the attempted attack, the outcomes of related screening, and the extent to which federal agencies assessing the impacts of this screening.

Our preliminary observations show that federal agencies have made progress in implementing corrective actions to address problems in watchlist-related processes that were exposed by the December 2009 attempted attack. These actions are intended to address problems in the way agencies share and use information to nominate individuals to the TSDB, and use the watchlist to prevent persons of concern from boarding planes to the United States or entering the United States at a port of entry. For example, according to TSA, the agency's assumption of the screening function from air carriers—under the Secure Flight program—has improved the government's ability to correctly determine whether passengers are on the No Fly or Selectee lists and has resulted in more individuals on these lists being identified and denied boarding an aircraft

[25] Executive Office of the President, *Summary of the White House Review of the December 25, 2009, Attempted Terrorist Attack* (Washington, D.C.: Jan. 7, 2010).

[26] Executive Office of the President, *Memorandum on Attempted Terrorist Attack on December 25, 2009: Intelligence, Screening, and Watchlisting System Corrective Actions* (Washington, D.C.: Jan. 7, 2010).

or subjected to additional physical screening before they board, as appropriate. Also, in April 2011, TSA began screening airline passengers against a broader set of TSDB information, which has helped mitigate risks. As part of its border and immigration security mission, CBP implemented the Pre-Departure Targeting Program to expand its practice of identifying high-risk and improperly documented passengers—including those in the TSDB—before they board flights bound for the United States, and recommending that air carriers deny boarding to individuals that the agency would likely deem inadmissible upon arrival at a U.S. airport. This program has resulted in more known or suspected terrorists being denied boarding.

Our preliminary work also suggests that the outcomes of these DHS programs demonstrate the homeland security benefits of terrorist-related screening, but such screening could have impacts on agency resources and the traveling public. For example, new or expanded screening programs have could require agencies to dedicate more staff to check traveler information against watchlist information and take related law enforcement actions. Also, new or expanded screening programs could result in more individuals misidentified as being in the TSDB, which can cause traveler delays and other inconvenience. It will be important for agencies to monitor and address these impacts as appropriate moving forward. We plan to issue a report with the final results or our work later this year.

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, this concludes my statement for the record.

Contacts and Acknowledgments

For additional information regarding this statement, please contact Eileen R. Larence at (202) 512-6510 or larencee@gao.gov. In addition, Eric Erdman, Mary Catherine Hult, Thomas Lombardi, Victoria Miller, and Hugh Paquette made key contributions to this statement. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

Related GAO Products

Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11. GAO-11-881. Washington, D.C: September 7, 2011.

Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investments. GAO-11-455. Washington, D.C: July 21, 2011.

High-Risk Series: An Update. GAO-11-278. Washington, D.C.: February 2011.

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.: December 16, 2010.

Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results. GAO-10-972. Washington, D.C.: September 29, 2010.

Terrorist Watchlist Screening: FBI Has Enhanced Its Use of Information from Firearm and Explosives Background Checks to Support Counterterrorism Efforts. GAO-10-703T. Washington, D.C.: May 5, 2010.

Homeland Security: Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security. GAO-10-401T. Washington, D.C.: January 27, 2010.

Information Sharing: Federal Agencies Are Sharing Border and Terrorism Information with Local and Tribal Law Enforcement Agencies, but Additional Efforts Are Needed. GAO-10-41. Washington, D.C.: December 18, 2009.

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.

Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers. GAO-08-35. Washington, D.C.: October 30, 2007.

Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public. GAO-06-1031. Washington, D.C.: September 29, 2006.

Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information. GAO-06-385. Washington, D.C.: March 17, 2006.

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

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548