United States Government Accountability Office

GAO

Testimony

Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, July 23, 2008

INFORMATION SHARING

Definition of the Results to Be Achieved in Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress

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

July 23, 2008

INFORMATION SHARING

Definition of the Results to Be Achieved in Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-637T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

In 2005, GAO placed the issue of information sharing for homeland security on its high-risk list of federal functions needing broad-based transformation and since then has monitored the government's progress in resolving barriers to sharing. This testimony discusses three key information sharing efforts: (1) the actions that have been taken to guide the design and implementation of the Information Sharing Environment (ISE) and to report on its progress, (2) the characteristics of state and local fusion centers and the extent to which federal efforts are helping to address some of the challenges centers reported, and (3) the progress made in developing streamlined policies and procedures for designating, marking, safeguarding, and disseminating sensitive but unclassified information. This testimony is based on GAO's products issued from March 2006 through July 2008 and selected updates conducted in July 2008.

What GAO Recommends

GAO is recommending that the ISE Program Manager more fully define the ISE's scope, results to be achieved, and stakeholders' roles and responsibilities, including the development of performance measures and defining the federal government's long-term role in relation to fusion centers, including the provision of resources. The ISE Program Manager generally agreed with these recommendations.

To view the full product, including the scope and methodology, click on GAO-08-637T. For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov.

What GAO Found

In a report being released today, GAO concludes that the ISE, under the leadership of a designated Program Manager, has had a measure of success, but lacks a road map for guiding the ISE, ensuring accountability, and assessing progress. The Program Manager's Office issued an implementation plan in November 2006 to guide the design of the ISE, has carried out a number of steps in that plan, and has leveraged existing efforts and resources agencies independently pursued for improving information sharing. However, this plan lacks important elements essential to effectively implement the ISE. Gaps exist in (1) defining the ISE's scope, such as determining all the terrorism-related information that should be part of the ISE; (2) clearly communicating and distinguishing the role of the Program Manager and other stakeholders; and (3) determining the results to be achieved by the ISE (that is, how information sharing is improved) along with associated milestones, performance measures, and the individual projects. Two annual reports on progress have been issued. Each identifies annual goals and individual ISE efforts, but neither reports on the extent to which the ISE has improved information sharing.

GAO reported in October 2007 that fusion centers, established by states and localities to collaborate with federal agencies to improve information sharing, vary widely but face similar challenges—especially related to funding and sustaining operations—that the federal government is helping to address but are not yet resolved. While the centers varied in their level of maturity, capability, and characteristics, most fusion centers focused on processing information on crimes and hazards, as well as terrorism-related information. Fusion center officials reported facing challenges such as obtaining specific, clear guidance and training; obtaining and retaining qualified personnel; and securing funding for center operations over the long term. The Department of Homeland Security and the Federal Bureau of Investigation were helping to address these challenges by, for example, providing technical assistance and training, personnel, and grant funding. Also, legislation has been proposed to clarify how funding may be used to hire and retain intelligence analysts.

Although the myriad of sensitive but unclassified designations has been a long-standing problem, progress has been made in establishing processes for designating, marking, safeguarding, and disseminating this information. In March 2006, GAO reported that each federal agency determined sometimes inconsistent designations to apply to its sensitive but unclassified information and this could lead to challenges in information sharing, such as confusion on how to protect the information. Thus, GAO recommended that the Directors of National Intelligence and the Office of Management and Budget issue a policy that consolidates sensitive but unclassified designations. In a May 2008 memorandum, the President adopted "controlled unclassified information" (CUI) to be the single categorical designation for sensitive but unclassified information throughout the executive branch and provided a framework for designating, marking, safeguarding, and disseminating CUI.

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to summarize the results of our recent reviews of the government's efforts to better share information about possible terrorist threats to protect the homeland. As you know, in 2005, GAO placed the issue of information sharing for homeland security on its high-risk list of federal programs or functions needing broad-based transformation and since then has conducted work to monitor the government's progress in resolving barriers to sharing. What we found is that in the wake of 9/11 and the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act) and Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), agencies at the federal, state, and local levels are taking steps to better share information about possible terrorist threats.[1] New organizations whose mission is information sharing and fusion have been created. New processes, information systems, and networks have evolved to handle the sharing and to encourage communication among the partners who must analyze and act on this information. And Congress and the administration have enacted new laws and issued new policies, guidance, and standards to promote better sharing. But there is still important and critical work left to do. This includes better integrating all of these changes and initiatives into a set of functioning policies, processes, and procedures for sharing; continuing to break down agency stovepipes and cultures that promoted protection over sharing; monitoring and measuring progress; and maintaining momentum.

Among the many efforts begun to improve information sharing is the creation of the Information Sharing Environment (ISE), a governmentwide "approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate."[2] In implementing this initiative, the Program Manager for the ISE—appointed by the President and responsible for planning, overseeing, and managing this new approach with participation of other federal departments and agencies, such as the Departments of Defense, Justice, and Homeland Security—envisions an ISE that will be comprised of policies, procedures, and technologies that link people, systems, and

[1]See Pub. L. No. 110-53, 121 Stat. 266 (2007); Pub. L. No. 108-458, 118 Stat. 3638 (2004). See also Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[2]See Pub. L. No. 108-458, § 1016, 118 Stat. at 3664-70, amended by Pub. L. No. 110-53 § 504, 121 Stat. at 313-17.

information among all critical stakeholders. In addition, most states and some local areas have created fusion centers to address gaps in homeland security and law enforcement information sharing by the federal government and to provide a conduit for this information within each state. While they vary—reflecting differences in state and local needs—a fusion center is generally a "collaborative effort of two or more federal, state, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." One of the barriers to information sharing with these entities was the many different and sometimes confusing and contradictory ways that agencies were identifying and protecting sensitive but unclassified information. This information encompasses a large but unquantifiable amount of information—for example, sensitive law enforcement information, information about a narcotics-smuggling ring, and terrorism financing information—that does not meet the standards established by executive order for classified national security information, but that an agency nonetheless considers sufficiently sensitive to warrant restricted dissemination.

My testimony today summarizes the findings of our work on the following three information sharing initiatives: (1) the actions that have been taken to guide the design and implementation of the ISE and to report on its progress, (2) the characteristics of state and local fusion centers and the extent to which federal efforts are helping to address some of the challenges centers reported, and (3) the progress made in developing streamlined policies and procedures for designating, marking, safeguarding, and disseminating sensitive but unclassified information. The information in this testimony is based on GAO reports and testimonies issued from March 2006 through June 2008 addressing these three terrorism-related information sharing issues.[3] We also conducted selected

[3]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); *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*, GAO-08-35 (Washington, D.C.: Oct. 30, 2007); *Homeland Security: Federal Efforts Are Helping to Address Some Challenges Faced by State and Local Fusion Centers*, GAO-08-636T (Washington, D.C.: Apr. 17, 2008); *Transportation Security Administration's Processes for Designating and Releasing Sensitive Security Information*, GAO-08-232R (Washington, D.C.: Nov. 30, 2007); and *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.: Mar. 17, 2006).

updates in July 2008 by obtaining and reviewing the *Annual Report to the Congress on the Information Sharing Environment*, dated June 30, 2008, released after our report on the ISE was issued, and the May 2008 *Memorandum for the Heads of Executive Departments and Agencies: Designation and Sharing Controlled Unclassified Information*, released since our work on that issue. We conducted this work according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Summary

In a report we are releasing today, we conclude that one of the primary ways in which Congress and the administration intended to promote sharing—through the ISE under the leadership of a designated Program Manager—has had a measure of success, but lacks a road map that defines the scope of the ISE, roles and responsibilities and the desired results to be achieved (i.e., how information sharing should be improved), and measures for assessing progress. The Program Manager's Office issued an implementation plan in November 2006 to guide the design of the ISE, has achieved a number of steps in that plan, has incorporated into the ISE a number of initiatives that agencies independently pursued to leverage resources, and has issued two annual reports on its progress. However, this progress is tempered by several gaps to be filled, such as:

- The Program Manger and participating agencies have not yet fully defined the scope of the ISE—or what the ISE is and is not to include—and completely answered fundamental questions, such as what information should be shared, where does the information reside, and what systems and networks will be integrated into the ISE. Addressing these gaps is important and necessary to establish a clear road map to guide implementation for all entities involved, ensure that progress is made based on needs, and facilitate future measurement of progress in information sharing.

- The role and responsibilities of the Program Manager versus those of the key agencies involved were not clearly distinguished and communicated, slowing progress. Delineating clear roles and responsibilities will minimize confusion over what each stakeholder is accountable for in implementing and operating the ISE and help minimize unnecessary delays that result.

- The Program Manager and stakeholders have yet to fully define the results to be achieved and milestones, performance measures, and individual projects for assessing progress. Linking measurable long-term and interim goals and clearly defining measurable results to be achieved can help the Program Manager and stakeholders track progress of implementation and improved sharing as well as hold stakeholders accountable for meeting their responsibilities and contributions in ensuring the ISE's success.

The ISE and information sharing for protecting the homeland against terrorism is a complex and ever-evolving challenge. Addressing these gaps, while difficult, is nevertheless necessary to provide Congress and the public reassurance that the flaws leading to 9/11 have been or are being corrected. Therefore, to address these gaps and help ensure that the ISE is on a measurable track to success, we recommended that the Program Manager, with full participation of relevant stakeholders (e.g., agencies and departments on the ISE), (1) more fully define the scope and specific results to be achieved by the ISE along with the key milestones and individual projects or initiatives needed to achieve these results, and (2) develop a set of performance measures that show the extent to which the ISE has been implemented and sharing has been improved—including, at a minimum, what has been and remains to be accomplished—so as to more effectively account for and communicate progress and results. The Program Manager generally agreed with these recommendations. The recently issued 2008 annual report comes closer to addressing these gaps, but acknowledges that work remains to be done to move from measuring individual agency actions and progress to measuring the overall performance of the ISE and the results and outcomes achieved.[4] But our work shows that there are still important questions for the administration and Congress to answer: Does the federal government know where it is going and what it is trying to achieve in the end? How far has it come and how much is left to do? Is this progress good enough? How much better is the sharing and what difference has it made? What will it cost? Finding these answers will be challenging but critical for ensuring homeland security.

With respect to our work on information fusion centers, we reported in October 2007 that these centers vary widely and that a number of them

[4]Program Manager, Information Sharing Environment, *Annual Report to the Congress on the Information Sharing Environment* (Washington, D.C.: June 30, 2008).

face several similar challenges—especially related to funding and sustaining operations—that the federal government is helping to address but that are not yet resolved. More specifically, our work showed that states and localities generally created these centers to improve information sharing across levels of government and to prevent terrorism or other threats. At the time of our review, the centers varied in level of maturity and capability, but most focused on processing information related to crimes or hazards, not just terrorism-related information. As we reported, most were led by law enforcement entities; had a variety of partnerships with other federal, state, and local agencies; and had federal personnel assigned. Among the challenges fusion center officials reported that they faced were managing a high volume of information from multiple systems, obtaining specific and clear guidance and training on operational issues, obtaining and retaining qualified personnel, and securing federal grant or state and local funding for center operations over the long term. We reported in October 2007 that the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) were helping to address these challenges by, among other things, providing access to information systems and networks as well as technical assistance and training, deploying personnel to centers, and providing grant funding. However, to improve efforts to create a national network of fusion centers as envisioned for the ISE, we recommended that the federal government determine and articulate its long-term fusion center role and whether it expects to provide resources to centers to help ensure their sustainability. To some extent, the administration did so in the *National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-Related Information*, issued in October 2007, by stating that the federal government will support the establishment of fusion centers and help sustain them. The 9/11 Commission Act further reflects this and legislation has been proposed to clarify how Homeland Security Grant Program funding may be used to hire and retain intelligence analysts.

Finally, as to the barriers to sharing posed by agency practices in protecting sensitive information, we found that although the myriad of sensitive but unclassified designations has been a long-standing problem, a recently issued policy should help to streamline and standardize the process for designating, marking, safeguarding, and disseminating this information. In March 2006, we reported that U.S. government agencies had varying and disparate designations—such as law enforcement sensitive, for official use only, and unclassified controlled nuclear information—for identifying sensitive but unclassified information. At that time, there were no governmentwide policies or procedures that described the basis on which agencies should designate, mark, and handle this type

of unclassified information, resulting in each agency deciding how to do this on its own. We reported that such inconsistency could lead to challenges in information sharing, such as confusing those receiving the information—including local and state law enforcement agencies—who in turn must understand and safeguard the information according to each federal agency's rules. Consequently, we recommended the issuance of a policy that consolidates sensitive but unclassified designations where possible and addresses their consistent application across agencies, as well as a directive requiring that agencies have in place internal controls for the designation and use of this information. To address this concern and in line with our recommendations, in a May 2008 memorandum, the President adopted "controlled unclassified information" (CUI) to be the single categorical designation for sensitive but unclassified information throughout the executive branch; outlined a framework for identifying, marking, safeguarding, and disseminating this information; and made the National Archives and Records Administration (NARA) responsible, through its new CUI Office, for implementation and oversight. While the new policy is a good start, our work has demonstrated that monitoring agencies' compliance to ensure that they implement guidelines, training, and internal controls will help ensure that the policy is employed consistently across the federal government. The Transportation Security Administration's (TSA) program on managing information it designates as sensitive security information could serve as a model to guide other agencies' implementation of CUI. We found that the program institutes many of these key components, such as employee training on how to decide what information to designate as sensitive security information, and internal controls, such as supervisory review to ensure that employees are appropriately making these designations.

Stakeholders Are Taking Steps to Improve Terrorism-Related Information Sharing, but Existing Gaps Present Challenges for Implementing the ISE and Measuring Its Progress

ISE stakeholders are taking steps to improve terrorism-related information sharing, but work remains to define the scope of the ISE, roles and responsibilities, the desired results to be achieved—that is, how information sharing should be improved—and measures for assessing progress, all elements in establishing a road map for meeting information sharing needs and implementing the ISE. For example, because these gaps, such as the need to better define roles and responsibilities, have not been fully addressed, additional effort has been spent reinforcing that all stakeholders are accountable for defining the ISE, not just the Program Manager. For example, in response to the Intelligence Reform Act, the President appointed a Program Manager for the ISE and on December 16, 2005, issued a memorandum to implement guiding principles—the presidential guidelines—consistent with establishing and supporting the ISE.[5] In addition, an Information Sharing Council (ISC), chaired by the Program Manager and currently composed of 16 other members—including designees of the Departments of State, Justice, and Homeland Security—has been established to provide interagency support and advice to the Program Manager on the development of the ISE. A step in planning for the ISE and putting it into operation included the issuance of the *Information Sharing Environment Implementation Plan* in November 2006. This plan provides an initial structure and approach for designing and implementing the ISE and addresses ways to meet the ISE requirements set forth in the Intelligence Reform Act as well as the presidential guidelines. For example:

- The plan includes steps toward standardizing procedures for protecting information privacy. One such activity identified in the plan includes having the Program Manager and key stakeholders establish a process for ensuring that nonfederal organizations participating in the ISE implement appropriate policies and procedures for providing protections.

- The plan maps out a timeline for further defining what information, processes, and technologies are to be included in the ISE and exploring approaches for implementing these processes and technologies. The plan consists of a two-phased approach for implementing the ISE by June 2009. Phase 1, originally scheduled to be completed by June 2007, generally covers setup activities such as investigating existing or

[5]See Presidential Memorandum, *Memorandum from the President for the Heads of Executive Departments and Agencies, Subject: Guidelines and Requirements in Support of the Information Sharing Environment* (ISE) (Dec. 16, 2005).

emerging search technologies for use in the ISE, and relationship building among stakeholders through participation on the ISC. Phase 2, that was to commence in July 2007, covers design as well as implementation of the ISE. The two phases are comprised of 89 total action items organized by priority areas, such as improved terrorism information handling. While 48 action items were to be completed by June 2007, by the end of Phase 1, only 18 were completed. Completed activities include development of proposed common terrorism information sharing standards—a set of standard operating procedures intended to govern how information is to be acquired, accessed, shared, and used within the ISE—and implementation of electronic directory services pages to help identify sources where terrorism information may be located within the federal government and whom to contact to access it.

- Design and implementation also incorporate independent initiatives that federal, state, and local agencies had under way to enhance information sharing across the government. This is in accordance with the Intelligence Reform Act's call to build upon existing systems capabilities in use across the government. These initiatives include the fusion centers state and local governments created and plans to develop a national network of these centers to improve sharing among federal, state, and local entities. They also include the FBI's Terrorist Screening Center, which consolidates information on known or suspected terrorists who operate within the United States for dissemination to federal agencies that use the information to screen individuals for possible terrorist links.

The plan also includes several gaps, however, which have tempered progress in implementing the ISE. Components needed to remediate these gaps include more fully defining the scope of the ISE, clarifying stakeholder roles and responsibilities (i.e., that of the Program Manager as distinguished from those of the departments and agencies that own and must share terrorism-related information), and defining the results to be achieved by the ISE as well as the associated milestones, performance measures, and projects needed for effective program planning and performance measurement. These are all important elements for establishing a road map for and ensuring stakeholders are held accountable in meeting information sharing needs, implementing the ISE, and measuring progress.

To expand on each of these three points, first, the Program Manager and the federal agencies that are key to making the ISE work—such as the Departments of Defense, Homeland Security, Justice, and State—still have

work to do to define the scope of the ISE, or what is and is not to be included in it. For instance, the Program Manager and stakeholders are still addressing fundamental questions, such as what information should be shared, where the information resides, how the information will be shared yet protected, how to provide access to information yet respect privacy, and what systems and networks will be used as part of the ISE. We recognize that the ISE will evolve over time and that these questions will need to be revisited and the answers updated and incorporated into the ISE. Answering these questions, at least for the near term, is important and necessary because it helps determine the elements critical for conveying what the ISE is to include and identifying available stakeholder resources—all components needed to establish a clear road map to successfully implement the ISE.

Second, the implementation plan did not clearly communicate and distinguish the role and responsibilities of the Program Manager from those of the key agencies in implementing the ISE and improving information sharing. This has ultimately led to confusion over what each stakeholder will be held accountable for in implementing and operating the ISE. In describing the role of the Program Manager, officials at the Office of the Program Manager noted that his role is primarily as a facilitator and, for example, one who focuses on improving existing business processes or remaining barriers that affect information sharing among two or more of the five ISE communities[6] that make up the ISE. However, the Program Manager does not focus on processes that are internal to ISE members unless they directly impact the wider ISE. Agencies, on the other hand, are accountable for identifying and sharing the terrorism information they own if the ISE is to succeed. However, at the time of our review agencies reported that they were unclear about the Program Manager's role or what their agencies were to provide in support of the ISE. Meanwhile, program officials reported that agencies were not participating consistently and effectively. As a result, this conflict has slowed progress in implementing the ISE, as evidenced by the fact that 30 of 48 Phase 1 implementing action items remained incomplete at the end of the phase in June 2007. To address these concerns, the President in

[6]As described in the ISE implementation plan, the ISE is comprised of five "communities of interest," encompassing intelligence, law enforcement, defense, homeland security, and foreign affairs. Each community may comprise multiple federal organizations and other stakeholders; information is to be shared across these communities.

October 2007 released the *National Strategy for Information Sharing*[7] that reaffirmed that stakeholders at all levels of government, the private sector, and foreign allies play a role in the ISE and further defined the role of the Program Manager as also assisting in the development of ISE standards and practices. However, the strategy did not further clarify the parameters of the Program Manager's role and what is within the scope of his responsibilities in "managing" the ISE versus other ISE stakeholders. In November 2007, the Program Manager held a first-time, off-site meeting with ISC members to focus on ISE priorities, clarify responsibilities, and emphasize the importance of everyone's active participation and leadership—with the intent of rectifying any misperceptions and reinforcing that all ISE stakeholders are responsible for the ISE. Further delineating clear roles and responsibilities will minimize confusion over what each stakeholder is accountable for in implementing and operating the ISE and help minimize unnecessary delays that result.

Finally, work also remains in further defining the results to be achieved by the ISE, the projects needed for implementing the ISE, and the milestones to be attained—all important elements for effective program planning and performance measurement. Existing federal guidance as well as our work and the work of others indicates that programs should have overarching strategic goals that state the program's aim or purpose, that define how it will be carried out over a period of time, are outcome oriented, and that are expressed so that progress in achieving the goals can be tracked and measured.[8] Moreover, these longer-term strategic goals should be supported by interim performance goals (e.g., annual performance goals) that are also measurable, define the results to be achieved within specified time frames, and provide for a way to track annual and overall progress (e.g., through measures and metrics). Following these practices can help the Program Manager and stakeholders track progress and hold stakeholders accountable for meeting their responsibilities and contributions in ensuring the ISE's success. The Program Manager and stakeholders have taken action in accordance with these program

[7]The White House, *National Strategy For Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (Washington, D.C.: Oct. 31, 2007).

[8]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); GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1996); Office of Management and Budget, Circular A-11, *Preparation, Submission, and Execution of the Budget* (July 2007); and The Project Management Institute, *The Standard for Program Management*© (2006).

management principles, but gaps remain. For example, the implementation plan identifies six longer-term strategic ISE goals. For example, one of these goals is that to the maximum extent possible, the ISE is to function in a decentralized, distributed, and coordinated manner. However, the plan does not define what this goal means or set up interim or annual goals and associated time-sensitive milestones to be built upon to achieve the overall goal. Furthermore, the plan does not define how agencies will measure and ensure progress in meeting the strategic goal in the interim or overall. Instead, the plan notes that performance measures will be developed at a later date. Moreover, with regard to identifying the steps to be taken in implementing the ISE, the plan does not present the projects and the sequence in which they need to be implemented to achieve this strategic goal in the near term or in the future, or the specific resources needed and stakeholder responsibilities. Therefore, work remains in developing the road map for achieving this strategic goal.

Since the issuance of the implementation plan, the Program Manager and participating agencies have taken steps to assess progress and improve the ISE's road map by issuing two annual reports and defining annual goals and performance measures, in part consistent with federal guidance for program planning and performance measurement. But taken together, these efforts do not yet provide methods to hold agencies accountable for ensuring that the necessary sharing of terrorism information is under way and effective. More specifically, the first annual report issued by the Program Manager in September 2007 describes overall progress by citing advancements in implementing individual initiatives that contribute to the ISE. Some of these were accomplished under the implementation plan—such as the formation of the electronic directory services—and others were achieved prior to or separate from efforts to create the ISE—such as the establishment of the FBI's Terrorist Screening Center. However, the report does not show how much measurable progress has been made toward implementing the ISE, how much remains to be done, or a road map for completion. For example, the only means to track progress that was set up in the implementation plan was the two-phased approach and the 89 action items. But the progress report did not provide an accounting of the status of these action items or identify how much of the implementation had been completed. Moreover, while the 2007 annual report identifies four performance goals for 2008, information necessary for assessing progress in meeting these goals—such as a defined starting point or baseline against which to assess progress, targets to be reached, or supporting performance measures and interim milestones to be achieved in implementing the ISE—is not identified.

In the fall of 2007 the Program Manger, with input from ISE participating agencies, developed performance measures in support of the four performance goals identified in the annual report. These measures are intended to improve reporting on progress in implementing the ISE and represent an important first step in providing quantitative data for assessing progress made in information sharing and in helping to inform Congress and other stakeholders of specific information sharing improvements. However, there are several gaps in these measures. For instance, they focus on counting activities accomplished rather than results achieved to show the extent to which ISE strategic goals and implementation have been attained. The performance measures include, for example, the number of ISE organizations with a procedure in place for acquiring and processing reports on suspicious activities potentially related to terrorism, but not how the reports are used and what difference they are making in sharing to help prevent terrorist attacks. Similarly, the measures attempt to assess the creation of a culture of sharing by tabulating the percentage of relevant ISE organizations that have an information sharing governance body or process in place, but not by measuring the outcome—such as how and to what extent cultural change is being achieved. Taking the next step—from counting activities to measuring results or outcomes—will be difficult, particularly since the program is still being designed, but critical for accurately providing Congress and policymakers with the information they need to assess the amount and rate of progress, remaining gaps, and the need for any intervening strategies.

Though issued after we completed our June 2008 report,[9] we subsequently reviewed the second ISE annual report dated June 30, 2008 and determined that the Program Manager has taken steps to improve assessments of progress in the ISE as program officials noted they would during our review. However, gaps still remain in defining key aspects of a road map—such as its scope, roles and responsibilities, and results to be achieved. One improvement, for instance, is that the Program Manager tried to better align agency activities according to the five guidelines and two requirements presented by the President in his 2005 memorandum[10] rather than listing them independently. For example, toward addressing

[9]GAO-08-492.

[10]See Presidential Memorandum, *Memorandum from the President for the Heads of Executive Departments and Agencies, Subject: Guidelines and Requirements in Support of the Information Sharing Environment (ISE)* (Dec. 16, 2005).

guideline 2—"Develop common standards for the sharing of information between and among executive departments and agencies and state, local, and tribal governments, law enforcement agencies, and the private sector"—the 2008 annual report identifies the status of efforts to generate, disseminate, and receive terrorism-related alerts, warnings, and notifications between the federal government and state, local, and tribal stakeholders. Also, the Program Manager laid out annual performance goals that list specific and measurable activities to be accomplished in 2009, such as completing initial efforts to implement the new suspicious activity reporting process—an initiative for streamlining the process for sharing information on suspicious activities or incident information with a potential terrorism nexus between federal, state, local, and tribal partners. Nevertheless, while the performance goals incorporate some quantitative data for assessing progress, they continue to focus on counting activities rather than measuring outcomes. For example, one performance goal states that agencies will increase fusion centers' access to terrorism-related information and ISE capabilities but does not define what this goal means and provide information on how it will be measured. Such information might include identifying the level of access centers currently have to information for use as a baseline from which to measure progress, the target increase agencies are expected to achieve, and how much achieving this goal is expected to improve sharing. While the activities identified in the performance goals and the information provided through the performance measures will likely enhance the fabric of what will ultimately be the ISE, they do not yet identify the overall road map for the ISE and provide answers to key questions regarding what the ISE will include and will not include and how the ISE will function in, for example, the next 3 years.

We appreciate that the ISE and information sharing for protecting the homeland against terrorism is a complex and ever-evolving challenge, making development of a road map for the ISE with which to assess progress, hold stakeholders accountable, and provide Congress and the public with assurance that efforts are being taken to strengthen information sharing ever more important. Therefore, to help ensure that the ISE is on a measurable track to success, we recommended that the Program Manager, with full participation of relevant stakeholders (e.g., agencies and departments on the ISE), (1) more fully define the scope and specific results to be achieved by the ISE along with the key milestones and individual projects or initiatives needed to achieve these results; and (2) develop a set of performance measures that show the extent to which the ISE has been implemented and sharing improved—including, at a minimum, what has been and remains to be accomplished—so as to more

effectively account for and communicate progress and results. The Program Manager generally agreed with these recommendations. In an effort to address these concerns, the Program Manager recently noted in the 2008 annual report that as the ISE matures, he expects the performance management approach will itself mature to move from measuring individual agency progress to measuring the overall performance of the ISE.

Fusion Centers Vary in Their Characteristics, and Federal Efforts Are Under Way That Address Many of the Challenges That Centers Reported Encountering

After September 2001, state and local governments began to establish fusion centers to improve information sharing across levels of government and varying disciplines and to prevent terrorism or other threats. By September 2007, almost all states and several local governments had established, or were in the process of establishing, fusion centers. As we reported in October 2007, these centers varied in their level of maturity, capability, and characteristics. For example, while some centers were just starting out, officials in many (43 of the 58) fusion centers we contacted described their centers as operational. Of these operational centers, 9 opened in the couple of years after September 2001, while 34 opened since January 2004. In terms of capability, we reported that these centers ranged from a center with analysts and access to networks and systems from DHS, FBI, and state and local entities operating at a Top Secret level to a center that had just appointed an officer in charge and lacked access to any of these federal networks and systems. However, our work showed that most of the operational fusion centers we contacted had adopted scopes of operations and missions that included more than just counterterrorism-related activities. For instance, officials in just over half of the operational centers we contacted said that their scopes of operations included all-crimes or all-crimes and terrorism, and several noted the link between crimes and terrorism as a rationale for adopting a broader scope of operations. Officials in about half of the operational centers said that their centers included all-hazards information, such as that related to public health and safety or emergency response. Overall, center officials we contacted during our review told us that adopting a broader focus than counterterrorism helped provide information about all threats, and including additional stakeholders that could provide staff and support could help increase the centers' sustainability. In terms of organization and partnerships, law enforcement entities, such as state police, were the lead or managing agencies in the majority of the centers we contacted. While the centers varied in their staff sizes and partnerships with other agencies, the majority of the operational fusion centers we contacted had federal personnel, including staff from DHS's Office of

Intelligence and Analysis or the FBI, assigned to them as of September 2007.

In our October 2007 report, we identified a variety of challenges—many of which were related to information sharing—that fusion center officials reported encountering in establishing and operating their centers. Among these challenges were managing the high volume of information and the multiple systems and networks, obtaining specific and clear guidance and training on operational issues, obtaining and retaining qualified personnel, and securing federal grant or state and local funding for center operations over the long term. We also reported that to help address these challenges, the Program Manager for the ISE, DHS, and the Department of Justice (DOJ) had several efforts under way, and as we reported in April 2008,[11] many of these efforts were ongoing.

- The Program Manager for the ISE along with DHS and DOJ have efforts under way to streamline systems, including reviewing the most commonly used sensitive but unclassified systems to examine users' needs to identify potential areas in which to streamline system access.[12] In addition, these agencies are taking steps to improve the quality and flow of information through the establishment of the Interagency Threat Assessment and Coordination Group, which became a statutorily mandated body by the 9/11 Commission Act.[13] The group is to include state, local, and tribal representative detailees who are to provide a nonfederal perspective to the intelligence community to produce clear, relevant, federally coordinated terrorism-related information products intended for dissemination to state, local, and tribal officials and to the private sector. In April 2008, we reported that four state and local law enforcement representatives had been detailed to this group. Further, the group's advisory council has been focusing on recruitment for next year's detailees and determining a concept of operations for a detailee fellowship program, according to the ISE 2008 annual report.

[11]GAO-08-636T.

[12]These systems include DHS's Homeland Security Information Network, DOJ's Law Enforcement Online, and the Regional Information Sharing Systems, which is a nationwide initiative to share sensitive but unclassified criminal intelligence among law enforcement, first responders, and private sector stakeholders.

[13]See Pub. L. No. 110-53, § 521, 121 Stat. at 328-32 (adding section 210D to subtitle A, title II of the Homeland Security Act, Pub. L. No. 107-296, 116 Stat. 2135).

- The Program Manager, DHS, and DOJ have taken steps to develop specific, clear guidance and provide technical assistance and training. For example, they have outlined federal and fusion center roles and responsibilities in the *National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-Related Information*, which the administration issued in October 2007. They have also disseminated specific guidance in the form of baseline capabilities that outline minimum operational standards for centers to ensure that they have the necessary structures, procedures, and tools in place to support gathering, processing, analysis, and dissemination of terrorism-related information. In addition, DHS and DOJ's technical assistance program for fusion centers offers training and guidance on, among other things, operational issues such as establishing a privacy and civil liberties policy. These agencies along with the Program Manager for the ISE and others have also sponsored regional and national conferences designed to support fusion centers and provide information about ongoing federal efforts.

- To facilitate information sharing and support fusion centers, DHS and the FBI have deployed personnel, including intelligence officers and special agents. We reported in April 2008 that according to these agencies, DHS had deployed 23 officers to fusion centers and had plans to place officers in as many as 35 centers by the end of fiscal year 2008, and the FBI had assigned about 200 personnel to 44 fusion centers.[14]

- In terms of funding, DHS reported that from fiscal years 2004 through 2007, about $257 million in DHS grant funds supported information sharing and intelligence activities,[15] including 415 projects designated by states and territories for intelligence and fusion center initiatives.

Despite DHS and FBI efforts to deploy personnel to fusion centers and DHS's grant funding, fusion center officials were concerned about long-term sustainability—both the extent of federal support they could expect as well as the roles of their state or local jurisdictions. For example, we reported in October 2007 that challenges for fusion centers included

[14]These deployments may be to fusion centers other than the 58 centers that were included in our October 2007 report.

[15]This includes State Homeland Security Program, Urban Areas Security Initiative, Urban Area Security Initiative Transit Security Program, Law Enforcement Terrorism Prevention Program, Citizen Corps Program, Emergency Management Performance Grants, Metropolitan Medical Response System, Buffer Zone Protection Program, Trucking Security Grant Program, and Transit Security Program grant funding.

uncertain or declining federal funding, finding adequate funding for specific components of their centers' operations, and obtaining state or local funding. One of the specific funding challenges fusion center officials cited was time limits on the use of grant funds for personnel. Some officials expressed concerns about maintaining their personnel levels, such as the 2-year limit on the use of fiscal year 2007 DHS grant funds for personnel. This limit made retaining personnel challenging because state and local agencies may lack the resources to continue funding the position, which could affect the centers' ability to continue to operate. In our October 2007 report, we recommended that the federal government determine and articulate its long-term fusion center role and whether it expects to provide resources to help ensure their sustainability. The *National Strategy for Information Sharing* stated that the federal government will support the establishment of fusion centers and help sustain them through grant funding, technical assistance, and training to achieve a baseline level of capability. Similarly, the 9/11 Commission Act includes provisions for allowing grant funding through the State Homeland Security and Urban Areas Security Initiative grant programs to be used for a variety of fusion-related activities, including paying salaries for personnel. However, we reported in April 2008 that there was still uncertainty among fusion center officials about how specifically the federal government was planning to assist state and local governments in sustaining their fusion centers, in particular with respect to grant funding for intelligence analysts. Specifically, under the fiscal year 2008 Homeland Security Grant Program guidance, costs associated with hiring intelligence analysts were allowable for 2 years but were limited to the hiring of new analysts. After 2 years, states and urban areas are responsible for supporting the sustainment costs of those intelligence analysts. Legislation introduced in May 2008, and reported by the House Committee on Homeland Security July 10, 2008, seeks to clarify what constitutes allowable costs under these grants.[16] The committee found that the federal government has placed restrictions on the use of these funds that make long-term planning for fusion centers unmanageable. The proposed legislation would, among other things, permit states and localities receiving funds under either the State Homeland Security Program or the Urban Areas Security Initiative program to use grant funds toward salaries

[16]Personal Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act, H.R. 6098, 110th Cong. (2008) (proposing amendments to the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, to improve the financial assistance provided to state, local, and tribal governments for information sharing activities). See also H.R. Rep. No. 110-752 (July 10, 2008).

for analysts regardless of whether the analysts are current or new full-time employees or contract employees and without limitations on the period of time that these analysts can serve under the awarded grants. In addition, to support the establishment and sustainment of a national integrated network of fusion centers, among the federal government's planned activities, the ISE 2008 annual report includes the development of a national investment strategy to sustain fusion center operations, including a delineation of current and recommended future federal and nonfederal costs.

A New Policy Is Intended to Streamline Processes for Sharing Sensitive but Unclassified Information

In March 2006, we reported on a survey of 26 federal agencies[17] that showed they were using more than 50 different designations to protect information that they deem critical to their missions—such as law enforcement sensitive, for official use only, and unclassified controlled nuclear information. At that time, there were no governmentwide policies or procedures that described the basis on which agencies should designate, mark, and handle this information. In this absence, each agency determined what designations to apply. We reported that such inconsistency can lead to challenges in information sharing. In fact, more than half of the agencies reported encountering challenges in sharing sensitive but unclassified information. For example, 11 of the 26 agencies reported concerns about the ability of other parties to protect sensitive but unclassified information, while another 6 of these agencies said that the lack of standardized criteria for defining what constitutes sensitive but unclassified information was a challenge in their sharing efforts. In addition, we found that the prevalence of designations can confuse those receiving the information, such as local and state law enforcement agencies, which in turn must understand and safeguard the information according to each federal agency's rules. This is problematic because, as we found, most agencies did not determine who and how many employees could make sensitive but unclassified designations, provide them training on how to do so, or perform periodic reviews of how well their practices are working. Moreover there were no governmentwide policies that

[17]As identified in our March 2006 report (see GAO-06-385), these federal agencies were generally selected because they are defined as those subject to the Chief Financial Officers Act. In addition, we also included the Federal Energy Regulatory Commission and the U.S. Postal Service because our previous experience with these agencies indicated that they used sensitive but unclassified designations.

required such internal control practices.[18] We reported that if guidance and monitoring is not provided, there is a probability that the designation will be misapplied, potentially restricting material unnecessarily or resulting in dissemination of information that should be restricted. Therefore, we recommended the issuance of a policy that consolidates sensitive but unclassified designations where possible and addresses their consistent application across agencies, as well as a directive requiring that agencies have in place internal controls that meet our *Standards for Internal Control in the Federal Government*—including implementing guidance, training, and review processes.[19]

Consistent with our recommendations and the President's December 2005 mandates calling for standardization of sensitive but unclassified information designations, on May 9, 2008, the President issued a memorandum that adopted CUI as the single categorical designation used for sensitive but unclassified information throughout the executive branch.[20] Specifically, CUI refers to information that is outside the standard National Security Classification system (e.g., Secret, Top Secret, etc.) but that is (1) pertinent to the national interests of the United States or to the important interests of entities outside the federal government and (2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or set limits on exchange or dissemination. Furthermore, the memo outlined a framework for designating, marking, safeguarding, and disseminating information identified as CUI. In doing so, the memo outlines the following three markings:

- Controlled with standard dissemination, meaning the information requires standard safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.

[18]Internal controls are an integral component of an organization's management that provides reasonable assurance that the following objectives are achieved: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations. See GAO, *Standards for Internal Controls in Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

[19]GAO-06-385.

[20]See Presidential Memorandum, *Memorandum for the Heads of Executive Departments and Agencies: Designation and Sharing Controlled Unclassified Information* (May 9, 2008).

- Controlled with specific dissemination, meaning the information requires safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Material contains additional instructions on what dissemination is permitted.

- Controlled enhanced with specified dissemination, meaning the information requires safeguarding measures more stringent than those normally required since the inadvertent or unauthorized disclosure would create the risk of substantial harm. Material contains additional instructions on what dissemination is permitted.

The memo made NARA responsible for overseeing and managing the implementation of the CUI framework. In response, NARA established the CUI Office to accomplish the new tasks associated with implementing the CUI policy. The new office is to undertake nine steps for the implementation and standardization governing CUI policy. Chief among these are (1) establishing new safeguards and dissemination controls, (2) publishing standards in a new official CUI Registry, (3) monitoring department and agency compliance with CUI policy and standards, (4) establishing required training and an associated training program for departments and agencies, and (5) providing appropriate documentation regarding the CUI framework to Congress; state, local, tribal, and private entities; and foreign partners. Issuing the new policy and laying out responsibilities is a good first step. Our work has demonstrated that monitoring agencies' compliance with CUI policies and standards to ensure that they implement guidelines, training, and internal controls will help ensure that the policy is employed consistently across the federal government and facilitate the sharing of terrorism-related information.

Our November 2007 review of TSA's program on managing sensitive security information[21] showed that in response to our prior recommendations on establishing guidance and procedures for using TSA regulations to determine what constitutes sensitive security information, TSA's program had instituted key components critical for the sharing of unclassified sensitive information and could serve as a model to guide other agencies' implementation of CUI. TSA has also shared its criteria and

[21]Sensitive security information is a statutorily established category of sensitive but unclassified information that includes information obtained or developed in the conduct of security activities that, for example, would be detrimental to transportation security. See 49 U.S.C. § 114(s); see also 49 C.F.R. pt. 1520. Sensitive security information is not subject to the CUI requirements.

examples used to help employees determine what is sensitive security information with other DHS components. Representatives we interviewed from these other DHS components have recognized opportunities to adapt TSA's criteria to their offices' unique needs. Furthermore, TSA has appointed sensitive security information coordinators at all program offices, such as the Office of Law Enforcement/Federal Air Marshal Service, among other things, to implement sensitive security information determination policies. TSA's Office for Sensitive Security Information is in the process of providing training to all TSA employees and contractors on how to handle sensitive security information in accordance with its newly adopted policies and procedures. The office has a "train the trainer" program that instructs sensitive security information program managers and coordinators who are then expected to train appropriate staff in their respective agencies and programs. Several aspects of the sensitive security information training program that we evaluated are consistent with GAO-identified components of a strategic training program.[22] Within this effort, TSA also has processes for responding to requests for sensitive security information from federal, state, local, and tribal government entities. Furthermore, TSA's sensitive security information program has internal controls in place that are consistent with governmentwide requirements and respond to our recommendation. For example, TSA is in the process of conducting an audit to identify existing sensitive security information and its use, as well as evaluating a portion of records marked as containing such information.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the committee may have at this time.

Contacts and Acknowledgments

For further information on this testimony, please contact Eileen Larence at (202) 512-8777 or larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page

[22]GAO, *A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: Mar. 2004).

of this statement. Individuals making key contributions to this testimony include Susan Quinlan, Assistant Director; Mary Catherine Hult, Assistant Director; Joseph Cruz; and Anish R. Bhatt.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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