

June 2008

INFORMATION
SHARING
ENVIRONMENT

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



Highlights of [GAO-08-492](#), a report to congressional requesters

Why GAO Did This Study

The attacks on 9/11 underscored the federal government's need to facilitate terrorism-related information sharing among government, private sector, and foreign stakeholders. In response, the Intelligence Reform and Terrorism Prevention Act of 2004 mandated the creation of the Information Sharing Environment (ISE), which is described as an approach for the sharing of terrorism-related information. A presidentially appointed Program Manager oversees ISE development with assistance from the Information Sharing Council (ISC), a forum for 16 information sharing officials from federal agencies and departments. GAO was asked to report on (1) what actions have been taken to guide the design and implementation of the ISE and (2) what efforts have been made to report on progress in implementing the ISE.

To perform this work, GAO reviewed related laws, directives, guidance, and ISE planning and reporting documents and interviewed officials from the Program Manager's office and key agencies who serve on the ISC.

What GAO Recommends

GAO recommends that the Program Manager and stakeholders (1) more fully define the scope and results to be achieved by the ISE and (2) develop a comprehensive set of performance measures that show the extent to which the ISE has been implemented and sharing improved. The Program Manager generally agreed with these recommendations.

To view the full product, including the scope and methodology, click on [GAO-08-492](#). For more information, contact Eileen Larence 202-512-8777, LarenceE@gao.gov, or David Powner, 202-512-9286, pownerd@gao.gov.

INFORMATION SHARING ENVIRONMENT

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

What GAO Found

To guide ISE design and implementation, the Program Manager has issued an implementation plan, completed a number of tasks therein, and included other information sharing initiatives in the ISE, but the plan does not include some important elements to implement the ISE. The plan provides an initial structure and approach for ISE design and implementation. For example, the plan includes steps toward protecting information privacy and describes a two-phased approach for implementing the ISE by June 2009 consisting of 89 action items. Completed activities include, among others, development of proposed common terrorism information sharing standards. In addition, other federal, state, and local initiatives to enhance information sharing across the government are being incorporated in the ISE. These initiatives include partnering with state and local area fusion centers—created primarily to improve information sharing within a state or local area—to develop a national network of these centers. Nevertheless, Office of the Program Manager officials said that the 89 action items do not address all the activities that must be completed to implement the ISE. Work remains, including defining and communicating the ISE's scope, such as determining all terrorism-related information that should be part of the ISE, and communicating that information to stakeholders involved in the development of the ISE. In addition, the desired results to be achieved by the ISE, that is, how information sharing is to be improved, the specific milestones, and the individual projects—or initiatives—to achieve these results have not yet been determined. Defining the scope of a program, desired results, milestones, and projects are essential in providing a road map to effectively implement a program. Without such a road map, the Program Manager and stakeholders risk not being able to effectively manage implementation of the ISE.

To report on progress in implementing the ISE, the Program Manager issued an annual report in September 2007, which highlighted individual accomplishments and included several annual performance goals, and has since begun to develop performance measures, but neither effort provides for an assessment of overall progress in ISE implementation and of how much work remains. Some individual accomplishments contributing to the ISE occurred under the implementation plan; others, prior to and separate from ISE creation efforts. In keeping with federal guidance, GAO's work, and the work of others in strategic planning, performance measurement, and program management, the implementation plan contained six strategic goals and the annual report four performance goals for 2008. Also, the Program Manager has begun to develop some performance measures, but they focus on counting activities accomplished rather than results achieved. For example, the measures include the number of ISE organizations with a procedure in place for suspicious activity reports, but not how the reports are used and what difference they are making in sharing to help prevent terrorist attacks. GAO acknowledges that creating such measures is difficult, particularly since the program is still being designed, but until these measures are refined, future attempts to measure and report on progress will be hampered.

Contents

Letter		1
	Results in Brief	5
	Background	8
	Initial Steps to Define a Structure and Approach to Implement the ISE Have Been Taken, but Work Remains to Define What the ISE Is to Include, to Design How it Will Operate, and to Outline Measurable Steps and Time Frames to Achieve Implementation and Desired Results	13
	The Program Manager Has Issued the First Annual Report and Is Developing Initial Performance Measures, but Neither Can Yet Be Used to Determine How Much Progress Has Been Made and What Remains	27
	Conclusions	31
	Recommendations	32
	Agency Comments and Our Evaluation	32
Appendix I	Status of Phase I Action Items as of March 1, 2008	37
Appendix II	Comments from Office of the Program Manager for the Information Sharing Environment	52
Appendix III	GAO Contacts and Acknowledgments	57
Tables		
	Table 1: 7 Priority Areas in the ISE Implementation Plan	14
	Table 2: Strategic Goals Contained in the Implementation Plan	29
	Table 3: 2008 Annual Performance Goals Listed in the Annual Report	29
	Table 4: Comparison of Action Item Status in July 2007 and March 2008	37

Abbreviations

CUI	controlled unclassified information
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOJ	Department of Justice
ISC	Information Sharing Council
ISE	Information Sharing Environment
ISE EAF	Information Sharing Environment Enterprise Architecture Framework
FEA	Federal Enterprise Architecture
ITACG	Interagency Threat Assessment Coordination Group
NCTC	National Counterterrorism Center
NIST	National Institute of Standards and Technology
PM-ISE	Program Manager for the Information Sharing Environment
TSC	Terrorist Screening Center

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



United States Government Accountability Office
Washington, DC 20548

June 25, 2008

Congressional Requesters

Following the terrorist attacks of 2001, the Congress and the Executive Branch took numerous actions aimed explicitly at establishing a range of new security measures to strengthen the nation's ability to identify, detect, and deter terrorism-related activities and protect national assets and infrastructure from attack.¹ One theme common to nearly all these efforts was the need to share current information on terrorism-related matters with a variety of critical stakeholders across all levels of government, the private sector, and foreign countries. Recognizing the need to facilitate this sharing, the Intelligence Reform Act directed the President to create the Information Sharing Environment (ISE).² As amended by the 9/11 Commission Act, the Intelligence Reform Act defines the ISE as “an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate.” In implementing this approach the Program Manager—appointed by the President and responsible for planning for, overseeing, and managing this new approach—envisions an ISE that will be comprised of policies, procedures, and technologies that link people, systems, and information among all critical stakeholders.

In coordinating implementation of the ISE, the Program Manager depends on other federal departments and agencies. In particular, the Information Sharing Council (ISC)—comprised of senior representatives from 16

¹These actions included issuance of the *National Strategy for Homeland Security*, the *National Strategy to Secure Cyberspace* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*; issuance of Homeland Security Presidential Directives 6 and 7, calling, respectively, for the consolidation of the government's approach to terrorism screening and a national policy for identifying and prioritizing critical infrastructures and key resources and protecting them from terrorist attacks, among other things; and the enactment of legislation calling for, among other things, efforts to facilitate the sharing of terrorism-related information. See Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act), Pub. L. No. 108-458, 118 Stat. 3638; Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135.

²See Pub. L. No. 108-458, § 1016 Stat. at 3664-70, amended by Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), Pub. L. No. 110-53, § 504, 121 Stat. 266, 313-17. See also Pub. L. No. 107-296, § 892, 116 Stat. at 2253-54 (requiring the establishment of procedures for the sharing of homeland security information, as defined by this section).

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. The ISC is to advise in developing policies, procedures and guidelines, roles, and standards. In providing such assistance, the ISC, which is chaired by the Program Manager, is responsible for activities such as working to ensure coordination among federal departments and agencies participating in the ISE to establish, implement, and maintain the ISE. In addition to the ISC member departments and agencies, the Program Manager must involve and consider the needs of other stakeholders, to include additional federal departments and agencies; state, local, and tribal entities; the private sector; and foreign partners and allies. It is critical that all of these stakeholders participate in development of the ISE because they both possess and require terrorism-related information in the performance of their missions. Coordinating with this large number of stakeholders—each with its own individual agency’s interests, business processes, and technical capabilities—adds to the complexity of creating the ISE.

Our work since 2001 indicates that the federal government has improved the sharing of terrorism-related information but has struggled in the process. In January 2005, we designated information sharing for homeland security a high-risk function because the government had continued to face formidable challenges in analyzing and disseminating key terrorism-related information in a timely, accurate, and useful manner.³ We reported, at the time, that in the absence of comprehensive information-sharing plans, many aspects of homeland security information sharing remained ineffective and fragmented. We noted, as well, that information is a crucial tool in fighting terrorism and that its timely dissemination is absolutely critical to maintaining the security of our nation.

In March 2006, our report on information-sharing issues stated that more than 4 years after September 11, the nation still lacked the governmentwide policies and processes called for in law to provide a framework for guiding and integrating a myriad of ongoing efforts to share terrorism-related information critical to protecting our homeland.⁴ In that

³GAO, *High Risk Series: An Update*, [GAO-05-207](#) (Washington, D.C.: January 2005).

⁴GAO, *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).

report, we recommended that the Director of National Intelligence, among other things, assess progress in implementing the ISE and identify barriers to achieving ISE deadlines included in an interim implementation plan. The Program Manager is in the process of implementing these recommendations, and this report provides an update on their status. We also suggested in that report and subsequently in a November 2006 report, that the ISE effort was among the areas that needed additional congressional oversight.⁵

You requested that we provide observations on the ISE and how it is being implemented. This report answers the following two questions:

- What actions have been taken to guide the design and implementation of the ISE?
- What efforts have been made to report on progress in implementing the ISE?

To answer these questions, we identified and reviewed key statutes setting out requirements for the Information Sharing Environment, including the Intelligence Reform Act and the 9/11 Commission Act. We further considered the Government Performance and Results Act of 1993,⁶ related guidance issued by OMB,⁷ and our prior⁸ work on results oriented

⁵GAO, *Suggested Areas for Oversight for the 110th Congress*, [GAO-07-235R](#) (Washington, D.C.: Nov. 17, 2006).

⁶Pub. L. No. 103-62, 107 Stat. 285 (1993).

⁷Office of Management and Budget, Circular A-11, *Preparation, Submission, and Execution of the Budget* (July 2007) and Circular A-130, *Management of Federal Information Resources* (Nov. 28, 2000).

⁸See 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); GAO, *Agency Performance Plans: Examples of Practices That Can Improve Usefulness to Decisionmakers*, [GAO/GGD/AIMD-99-69](#) (Washington, D.C.: Feb. 26, 1999); GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: October 2005); GAO, *Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements*, [GAO-04-842](#) (Washington, D.C. Sept. 10, 2004); GAO, *Homeland Security: US-VISIT Program Faces Operational, Technological, and Management Challenges*, [GAO-07-632T](#) (Washington, D.C. Mar. 20, 2007); and GAO, *Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved*, [GAO-04-49](#) (Washington, D.C. Jan. 12, 2004).

government, program management, and federal coordination and collaboration. We also reviewed literature on program management principles, such as the Project Management Institute's *The Standard for Program Management*⁹ and Carnegie Mellon's *Capability Maturity Model Integration (CMMI®)*.¹⁰ Based on our review of these laws, guidance, and literature, we identified standard practices in program and project management for defining, designing, and executing programs. These practices focus on several critical aspects of program management, strategic planning, and performance measurement.

The scope of our review was limited to those ISE activities performed since the *Information Sharing Environment Implementation Plan* (implementation plan) was issued in November 2006 through March 1, 2008. Applying these identified standard practices in program management, we reviewed key ISE planning and reporting documents—the November 2006 implementation plan and the September 2007 *Annual Report to The Congress on the Information Sharing Environment* (annual report)—as well as other ISE-related strategic planning and performance measurement documents and activities. We further interviewed officials at the Office of the Program Manager for the Information Sharing Environment (PM-ISE) and examined planning and reporting documents housed at the office to determine the extent to which actions listed in the implementation plan for the first phase of ISE implementation were complete as of March 1, 2008. We also interviewed officials from five key federal agencies—the departments of Defense, Homeland Security, Justice, and State as well as the Office of the Director of National Intelligence—who serve on the ISE's Information Sharing Council. These federal agencies were chosen because they were identified by the PM-ISE as key participants expected to support the ISE since they collect defense, homeland security, law enforcement, foreign affairs, and intelligence information deemed critical for homeland security. We conducted this performance audit from February 2007 through June 2008, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the

⁹The Project Management Institute, *The Standard for Program Management*© (2006).

¹⁰CMMI is registered with the U.S. Patent and Trademark Office by Carnegie Mellon University.

evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

To guide ISE design and implementation, the Program Manager has issued an implementation plan, a number of tasks therein have been completed, and other independent and ongoing information sharing initiatives by federal, state, and local stakeholders have been integrated into the ISE, but the plan does not include some important elements needed to implement the ISE. Issued in November 2006, the plan provides an initial structure and approach for designing and implementing the ISE and addresses ways to meet the ISE requirements set in the Intelligence Reform Act as well as guidelines the administration set for implementation, as the following examples illustrate:

- The plan includes steps toward standardizing procedures for managing, handling, and disseminating sensitive but unclassified information—information that is generally restricted from public disclosure but not designated as classified national security information—as well as protecting information privacy.
- The plan maps out a timeline for further defining what information, business processes, and technologies are to be included in the ISE and exploring approaches for implementing them, describing a two-phased approach for implementing the ISE by June 2009. Phase 1 generally covers set-up activities and building relationships among stakeholders, and Phase 2 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, at the end of Phase 1, only 18 were completed on time. An additional 15 were completed as of March 2008. Completed activities include development of proposed common terrorism information sharing standards and implementation of electronic directory services pages to help identify sources where terrorism information may be located within the federal government. The incomplete action items are generally those that require a greater level of stakeholder involvement and, according to officials at the Office of the Program Manager, are taking longer than anticipated to complete.
- Design and implementation incorporate ongoing federal, state, and local initiatives to enhance information sharing across the government. These initiatives include partnering with state and local area fusion centers—collaborative efforts to detect, prevent, investigate, and respond to criminal and terrorist activity—and developing a national network of these

centers to improve sharing among federal, state, and local entities, as well as the Terrorist Screening Center to consolidate information on known or suspected terrorists who operate within the United States for dissemination to federal agencies that use the information to screen individuals.

In accordance with standard practices for program and project management, the ISE implementation plan identified action items and strategic goals to be achieved. However, work remains in defining and communicating the scope and desired results to be achieved by the ISE, the specific milestones to be attained, the individual projects—or initiatives—and the sequence in which they need to be executed to achieve these results and implement the ISE. For example, in terms of scope, work to determine all the terrorism-related information that should be part of the ISE is yet to be completed. In addition, the desired results to be achieved by the ISE—that is, how information sharing is to be improved and the specific milestones (e.g., time frames), and the projects to achieve these results—have not yet been determined. Although the plan contains 89 action items, officials at the Office of the Program Manager stated that the action items do not address all of the activities that must be completed to implement the ISE. This is because, at the time the plan was produced, agreement on how the ISE is to function and what it is to include had not been reached among the stakeholders and work toward reaching these agreements remains ongoing. Therefore, ISE officials stated that an assessment of the ISE's progress based on the action items identified in the plan alone would not give a true sense of progress toward a fully functioning and executed ISE. In accordance with standard program management practices, specific desired outcomes or results should be conceptualized and defined in the planning process as part of a road map, along with the appropriate projects needed to achieve those results, supporting resources, stakeholder responsibilities, and milestones. Without such a road map, the Program Manager and stakeholders risk not being able to effectively manage and implement the ISE.

To report on progress in implementing the ISE, the Program Manager issued an annual report on the ISE in September 2007 that highlighted individual accomplishments and included several annual performance goals as well as developed some performance measures, but did not provide an assessment of how much progress has been achieved in implementing the ISE and how much remains to be done. More specifically, the report cites accomplishments achieved as part of the implementation plan as well as others achieved prior to the enactment of the Intelligence Reform Act in December 2004 and its requirement to

implement the ISE. Federal guidance as well as our work and the work of others in strategic planning, performance measurement, and program management hold that programs should have overarching strategic goals that are outcome oriented and are expressed so that progress in achieving the goals can be tracked and measured. Moreover, these longer-term strategic goals should be supported by interim performance goals (e.g., annual performance goals) that are also measurable and provide for a way to measure and track annual and overall progress (e.g., through measures and metrics). In keeping with these practices, the implementation plan contained six overall strategic goals, and the annual report contained four performance goals for 2008. In addition, the Program Manager has begun to develop some annual performance measures, but they focus on counting activities accomplished rather than results achieved to show the extent of ISE implementation or progress towards attaining the ISE strategic goals. For example, performance measures developed include the number of ISE organizations with a procedure in place for acquiring and processing reports on suspicious activities potentially related to terrorism. This measure is an important first step in providing quantifiable data for assessing progress made, but does not measure for results, such as what difference the reports are making in sharing to help prevent terrorist attacks. According to officials at the Office of the Program Manager, these performance measures are being refined in consultation with the ISC to provide the needed framework to measure progress made. Yet, our review of a draft of these performance measures showed that they continue to focus on counting activities accomplished rather than results achieved. We acknowledge that creating such measures is difficult, particularly since the program is still being designed, but until these measures are refined to account for and communicate progress and results, future attempts to measure and report on progress will be hampered.

Thus, to help ensure that the ISE is on a measurable track to success, we are recommending that the Program Manager, with full participation of relevant stakeholders (e.g., agencies and departments on the ISC), (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 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.

We requested comments on a draft of this report from the Secretaries of Defense, Homeland Security, and State; the Attorney General; the Director

of National Intelligence; and the Program Manager for the ISE or their designees. The Program Manager provided written comments which are summarized below and included in their entirety in appendix II. The Program Manager generally agreed with our recommendations, but made several comments regarding the report's content. For example, he stated that the ISE is a governmentwide transformational effort and an evolutionary process, not a traditional "program" that can be audited within those parameters. While we agree that the ISE is not a traditional "program," in that it is not operated and funded by a single department or agency, it is an activity that does receive government funding and can be reviewed using program and project management principles. With regards to assessing the ISE's progress, the Program Manager discussed efforts that our report acknowledges. However, our review showed that the performance measures used to assess the ISE's progress focus on counting activities accomplished rather than results achieved and are not presented in a way that explains how they represent progress toward attaining strategic goals. The Secretaries of Defense, Homeland Security, and State; the Attorney General; and the Director of National Intelligence responded that they did not have any comments on the report. Officials in the Office of the Program Manager also provided technical comments on the draft that have been incorporated, as appropriate.

Background

Federal Law and Policy Call for the Development of an ISE

Because of the information-sharing weaknesses among federal departments and agencies that became apparent after September 11, the Congress and the administration have called for a number of terrorism-related information-sharing initiatives, including the development of an ISE, as the following instances illustrate:

- Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act), enacted December 17, 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), enacted August 3, 2007, requires the President to take action to facilitate the sharing of terrorism-related

information by establishing an ISE.¹¹ The Act required the President to, among other things, appoint a Program Manager to plan for, oversee implementation of, and manage the ISE, and established an ISC to assist the President and Program Manager in these duties. In addition, the Act required the President, with the assistance of the Program Manager, to submit to Congress a report containing an implementation plan for the ISE no later than 1 year after the date of enactment (enacted December 17, 2004) and specified 11 elements to be included in the plan. These elements include, among other things, the function, capabilities, resources, and concept for the design of the ISE; project plan; budget estimates; performance metrics and measures; and defined roles for all stakeholders.¹² The Act also required annual performance management reports, beginning not later than 2 years after enactment, on the state of the ISE and of information sharing across the federal government.

- On December 16, 2005, the President issued a memorandum to implement measures consistent with establishing and supporting the ISE.¹³ The memorandum sets forth five information sharing guidelines: (a) defining common standards for how information is acquired, accessed, shared, and used within the ISE; (b) developing a common framework for sharing information between and among executive departments and agencies; state, local, and tribal governments; law enforcement agencies; and the private sector; (c) standardizing the procedures for sensitive but unclassified information; (d) facilitating the sharing of information between executive departments and agencies and foreign governments; and (e) protecting the information privacy rights and other legal rights of Americans. The memorandum also directs the heads of executive

¹¹See Pub. L. No. 108-458, § 1016, 118 Stat. at 3664-70, amended by Pub. L. No. 110-53, § 504, 121 Stat. at 313-17. The term “terrorism-related information” encompasses the definitions of “terrorism information,” “homeland security information,” and “weapons of mass destruction information” in accordance with the Intelligence Reform Act, as amended, as well as law enforcement information relating to terrorism or the security of the homeland, in accordance with the ISE *Implementation Plan*.

¹²See Pub. L. No. 108-458, § 1016(e), 118 Stat. at 3666-67. The Program Manager issued the ISE *Implementation Plan* in November 2006 and, as such, the contents of the Plan may not fully reflect amendments made by the 9/11 Commission Act. For example, whereas before the amendments the ISE focused on the sharing of “terrorism information” as defined in the Act, the ISE now explicitly encompasses “homeland security information,” as defined by the Homeland Security Act, as well as terrorism information, which now includes “weapons of mass destruction information,” as defined by the 9/11 Commission Act.

¹³See 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).

departments and agencies to actively work to promote a culture of information sharing within their respective agencies and that ongoing information-sharing efforts be leveraged in the development of the ISE.

- In October 2007, the President issued a National Strategy for Information Sharing. The strategy is focused on improving the sharing of homeland security, terrorism, and law enforcement information related to terrorism within and among all levels of government and the private sector and articulates the administration's vision on terrorism-related information sharing. The strategy notes guiding principles and efforts taken to improve information sharing across all levels of government, the private sector, and foreign partners to date. It also contains an appendix that elaborates on the roles of federal, state, local, and tribal authorities in information sharing and expands on the role of state and major urban area fusion centers.

Scope and Purpose of the ISE

The ISE is not bounded by a single federal agency or component. While the Program Manager has been placed within the Office of the Director of National Intelligence, from an operational perspective, the ISE is to reach across all levels of government as well as the private sector and foreign partners. As such, the program is a broad-based coordination and collaboration effort among various stakeholders. In essence, the ISE can be viewed as a set of cross-cutting communication links—encompassing policies, processes, technologies—among and between the various entities that gather, analyze, and share terrorism-related information. According to officials at the Office of the Program Manager, their focus is primarily to ensure that all appropriate terrorism-related information is made available to analysts and others who need it when they need it. The Program Manager is not responsible for the collection or analysis of terrorism-related information.

The ISE implementation plan, released by the Program Manager in November 2006, is to be the guiding document describing how the ISE is to be implemented. This plan addressed at a very general and preliminary level the ISE's information-sharing strategy, roles, and needs. The document set out to include: (1) an operational concept; (2) the implementation overview; (3) a summary of desired operational capabilities; (4) means to develop an architecture and standards; (5) an approach to sharing with non-federal partners; (6) ISE enabling activities; (7) implementation management; (8) recommendations on a structure for expansion and future management; and (9) a summary of implementation actions. The plan also acknowledged numerous challenges to be

addressed, including promoting a culture of information sharing, protecting information privacy, and handling terrorism-related information. Under the 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.

Key ISE Players and Roles

ISE leadership lies with the presidentially appointed Program Manager, for whom the Intelligence Reform Act, as amended, lays out specific requirements. Pursuant to the Act, the Program Manager, in consultation with the head of any affected department or agency, has governmentwide authority over the sharing of terrorism-related information within the scope of the ISE and is required to plan for, oversee implementation of, and manage the ISE. For example, the Program Manager, in consultation with the ISC and consistent with the direction and policies issued by the President, the Director of National Intelligence, and the Director of the Office of Management and Budget, is to issue governmentwide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE. In fulfilling this responsibility, the Program Manager must, among other things, take into account the varying missions and security requirements of agencies participating in the ISE and ensure the protection of privacy and civil liberties. The implementation plan further described areas of responsibility in broad terms for the Program Manager. The plan states, for example, that the Program Manager is to “act as the central agent to improve terrorism-related information sharing among ISE participants by working with them to remove barriers, facilitate change, and ensure that ISE implementation proceeds efficiently and effectively.” In interpreting these responsibilities, the Program Manager has exercised discretion by focusing on, for example, facilitating information sharing across the five ISE communities. To support the development of the ISE, as of June 2008 the Program Manager has a staff of about 11 government staff and 31 contractors organized into three divisions—technology, policy and planning, and business process.

Interagency support and advice to the Program Manager on the development of the ISE is provided through the ISC. The ISC is chaired by the Program Manager and is currently composed of 16 other members, each designees of: the Secretaries of State, Treasury, Interior, Transportation, Health and Human Services, Commerce, Energy, and Homeland Security; the Department of Defense’s Office of the Secretary of

Defense as well as the Joint Chiefs of Staff; the Attorney General; the Director of National Intelligence; the Director of the Central Intelligence Agency; the Director of the Office of Management and Budget; the Director of the FBI; and the Director of the National Counterterrorism Center. The ISC is an advisory body, which among other things, is expected to

- advise the President and the Program Manager on development of policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE;
- work to ensure coordination among the federal agencies participating in the establishment, implementation, and maintenance of the ISE; and
- identify and recommend solutions to gaps between existing technologies, programs, and systems used by federal agencies for sharing information and the parameters of the proposed information-sharing environment.

The ISC and Program Manager are supported by various task and working groups. For example, the Foreign Government Information Sharing Working Group, with coordination and assistance from the PM-ISE, helped develop a checklist of issues to be taken into account in negotiating international agreements. Similarly, an Alerts and Notifications Working Group was established to assist the PM-ISE and ISC members in their efforts to identify the alerts and notifications to be available to federal and non-federal ISE participants.

Another area of roles and responsibilities for the ISE lies with individual federal agencies (including those that belong to the ISC and those that do not), state and local governments, and private sector entities. In accordance with the Intelligence Reform Act, as amended, any federal department or agency using or possessing intelligence or terrorism-related information, operating a system in the ISE, or otherwise participating or expecting to participate in the ISE must fully comply with information-sharing policies, procedures, guidelines, rules and standards established pursuant to the ISE. The departments and agencies must further ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE, ensure full department or agency cooperation in the development of the ISE to implement governmentwide information sharing, and submit, as requested, any reports on the implementation of ISE requirements within the department or agency. State and local governments also play a role in the ISE through, for example, their law enforcement efforts to prevent crimes. As such, these

governments are coordinated with and participate in implementing the ISE. Private sector organizations may share terrorism-related information on a voluntary basis through existing or newly developed ISE mechanisms as well. For example, the ISE leverages existing national plans such as the National Infrastructure Protection Plan, which established mechanisms for public and private sector organizations to share critical infrastructure information on 17 critical infrastructure sectors, such as banking and finance, energy, chemical, and transportation.

Initial Steps to Define a Structure and Approach to Implement the ISE Have Been Taken, but Work Remains to Define What the ISE Is to Include, to Design How It Will Operate, and to Outline Measurable Steps and Time Frames to Achieve Implementation and Desired Results

To guide the design and implementation of the ISE, the Program Manager has issued an implementation plan, completed a number of tasks contained in it, and other independent and ongoing information-sharing initiatives have been integrated into the ISE, but the plan does not include some important elements needed to implement the ISE. The plan provides an initial structure and approach for ISE design and implementation, as well as describes a two-phased approach for implementing the ISE by June 2009. Completed activities include, among other things, development of proposed common terrorism information sharing standards (CTISS) for sharing terrorism-related information. In addition, other federal, state, and local initiatives to enhance information sharing across the government have been or are being incorporated into the ISE. Based on existing federal guidance as well as our prior work and the work of others, standard practices in program and project management for defining, designing, and executing programs include (1) defining the program's scope, roles and responsibilities, and specific results to be achieved, along with the individual projects needed to achieve these results, and (2) developing a road map, or program plan, to establish an order for executing specific projects needed to obtain defined programmatic results within a specified time frame and measuring progress and cost in doing so. While efforts to date may represent the groundwork needed to facilitate terrorism-related information sharing in the future, work remains to define and communicate the scope and desired results to be achieved by the ISE, the specific milestones and time frames for achieving the results, and the individual projects and the sequence of projects needed to achieve these results. Without such elements the Program Manager risks not being able to effectively manage and implement the ISE.

The Implementation Plan Provides an Initial Structure and Approach for Designing and Implementing the ISE

Issued in November 2006, the implementation plan provides an initial structure and approach for ISE design and implementation and incorporates Presidential Guidelines as well as ISE requirements spelled out in the Intelligence Reform Act. For example, the plan includes steps towards developing standardized procedures for managing, handling, and disseminating sensitive but unclassified information as well as protecting information privacy, as called for in the Presidential Guidelines. For the most part, the plan also maps out a timeline for further defining what information, business processes, and technologies are to be included in the ISE and exploring approaches for implementing the ISE. For example, the plan describes a two-phased approach to implementing the ISE by June 2009, with Phase 1 scheduled for the November 2006 to June 2007 time frame and generally covering set-up activities and building relationships among stakeholders and Phase 2, beginning July 2007, covering design as well as implementation. This approach is intended to develop the ISE incrementally over a 3-year period. The two phases are comprised of 89 action items organized by priority areas. These priority areas address important aspects of the ISE, from defining information-sharing capabilities and technologies to protecting privacy and measuring performance (see table 1).

Table 1: 7 Priority Areas in the ISE Implementation Plan

Priority area	Description
Protecting information privacy and civil liberties in the ISE	Helping ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE.
Improved terrorism information handling	Creating standardized, consistent policies and procedures for handling classified and unclassified terrorism information.
Sharing with partners outside the federal government	Improving coordination at the national level for the production and dissemination of terrorism information, and sharing responsibility between federal and state governments for the timely processing and dissemination of information at every level to meet the needs of all end users.
Architecture and standards	Constructing, integrating, and maintaining information resource infrastructures across the federal government; state, local, and tribal governments; the private sector; and foreign partners.
ISE enabling activities	Developing performance management and planning tools as well as programming and budgeting documents.
ISE operational capabilities	Developing the information technology services needed to maximize information sharing.
Promoting a culture of information sharing	Developing a culture that promotes information sharing across the ISE.

Source: Information Sharing Environment Implementation Plan.

Forty-eight of the action items, all part of Phase 1, were to be completed by June 2007. Of these 48, 18 were completed on time and an additional 15

were completed by March 2008 (see app. I for details). Examples of completed activities covered by these action items include:

- The 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. According to the Program Manager, the proposed standards document the rules, conditions, guidelines, and characteristics of business processes, production methods, and products supporting terrorism-related information sharing. These standards are intended to address the Presidential Guideline that required the Director of National Intelligence—in coordination with the Secretaries of State, Defense, Homeland Security, and the Attorney General—to develop and issue such standards. These standards are an important early activity because of the structure they are intended to establish for sharing across all ISE stakeholders.
- The development of procedures and markings for sensitive but unclassified information to facilitate the exchange of information among ISE participants.¹⁴ We reported in March 2006 that federal agencies use numerous sensitive but unclassified designations that govern how this information must be handled, protected, and controlled and that the confusion caused by these multiple designations creates information-sharing challenges.¹⁵ Therefore, we recommended the issuance of a policy that consolidates sensitive but unclassified designations where possible and addresses their consistent application across agencies. Consistent with our recommendation, in May 2008 the Administration established controlled unclassified information (CUI) as the single categorical designation throughout the executive branch and established a corresponding CUI framework for designating, marking, safeguarding, and disseminating information designated as CUI. Once implemented, this effort could help improve access to information and improve information sharing.

¹⁴Sensitive but unclassified information encompasses a large but unquantifiable amount of information—for example, security plans for federal agency buildings—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 safeguarding and restricted dissemination.

¹⁵GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes For Sharing Terrorism-Related and Sensitive but Unclassified (SBU) Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006).

-
- Establishment of an initial operating capability for the Interagency Threat Assessment and Coordination Group (ITACG). The purpose of the ITACG is to support the efforts of the National Counterterrorism Center to produce federally-coordinated terrorism-related information products intended for dissemination to state, local, tribal, and private sector partners through existing channels established by federal departments and agencies. This effort is expected to help address concerns that federally produced terrorism-related information that state, local, tribal, and private sector organizations need for law enforcement and homeland security purposes is sometimes conflicting or not getting to them.
 - The establishment of a Federal Fusion Center Coordination Group to identify federal resources to support the development and maintenance of a network of state-sponsored fusion centers. Most states and many local governments have created state and local fusion centers to address gaps in information sharing, such as those that occurred on 9/11. These centers are collaborative efforts to detect, prevent, investigate, and respond to criminal and terrorist activities. In October 2007, we issued a report on the characteristics of and challenges for fusion centers and stated that the centers were particularly concerned about sustaining their operations over the long term.¹⁶ We recommended that this group, through the ISC and the Program Manager, determine and articulate the federal government's role in, and whether it expects to provide resources to, fusion centers over the long-term to help ensure their sustainability. According to ISE program management officials, work is ongoing to (1) complete a baseline capability assessment of designated state and major urban-area fusion centers and (2) develop a coordinated federal support plan that articulates resources being provided to the fusion centers.
 - The implementation of electronic directory services pages to help identify sources where terrorism information may be located within the federal government, as called for in the Intelligence Reform Act. In meeting this requirement, the electronic directory services are described as a collection of directories that enables ISE users to search for and locate information by accessing the appropriate people, organizations, data, and services related to the counterterrorism mission. The Program Manager expects to develop similar directories for state, local, and tribal stakeholders.

¹⁶GAO, *Homeland Security: Federal Efforts Are Helping Alleviate Some Challenges Encountered by State and Local Fusion Centers*, [GAO-08-35](#) (Washington, D.C.: Oct. 30, 2007).

Furthermore, work has been done towards accomplishing some action items that are not yet complete. For example, agencies, with leadership from the PM-ISE, have been working to develop a core training module intended to provide an introduction to the ISE and to further promote the development of a culture of information sharing. The incomplete action items are generally those that require a greater level of stakeholder involvement and, according to officials at the Office of the Program Manager are taking longer than anticipated to complete, but will not delay work on Phase 2 items. However, the action items do not address all the activities that must be completed to implement the ISE, according to officials at the Office of the Program Manager, and several activities identified in the implementation plan will not be implemented as identified in the plan. For example, one activity identified in the plan included the implementation of an electronic directory of services containing green pages in the unclassified domain. As identified in the plan, the green pages were to provide a searchable listing of counterterrorism-related information-sharing resources, systems, and data repositories to support users searching for specific data and capabilities. Further, the pages were to provide system descriptions and technical and operational contact information for gaining access. However, according to officials at the Office of the Program Manager, aggregating the information for the green pages would no longer enable the information to be posted in an unclassified domain. Therefore, the green pages will no longer be completed for the sensitive but unclassified security domain. Appendix I provides further detail on the status of each Phase 1 action item.

Federal, State, and Local Agency Initiatives Are Being Leveraged to Enhance Information Sharing and Guide Implementation of the ISE

Federal, state, and local agencies have their own initiatives to enhance information sharing across the government that are being leveraged in designing and implementing the ISE. Examples of these initiatives include:

- The Director of National Intelligence (DNI) issued a 100-day plan in April 2007, followed by a 500-day plan in September 2007 that focused on integrating the intelligence agencies and their missions in a collaborative manner.¹⁷ One area of focus in these plans is improved information sharing. As a result of this effort, the DNI reported that an implementation plan was developed to standardize identity and access policies across

¹⁷Under the Intelligence Reform Act, the intelligence community was reorganized under a Director of National Intelligence who oversees the 17 departments and agencies that make up the intelligence community. The intelligence community is one of the 5 communities of interest for the ISE and the Director of National Intelligence is a member of the ISC.

agencies, networks, and systems. The 100-day plan notes that as it is implemented, its results are intended to be leveraged by the Program Manager as part of the ISE because it is anticipated to improve communication within the intelligence community—one of the five communities that have been designated as critical to the ISE.

- The National Counterterrorism Center (NCTC) was established in 2004 in response to recommendations from the 9/11 Commission to operate as a partnership of intelligence agencies so that they can analyze and disseminate national intelligence data. The center works to ensure that intelligence agencies have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative, and mission-oriented analysis.
- As previously noted, in recognition of fusion centers as important mechanisms for information sharing, the federal government—including the Department of Homeland Security (DHS), the Department of Justice (DOJ), and the Program Manager—is taking steps to partner with these centers. Although they were created primarily to improve information sharing within the state or local area, the implementation plan identifies the creation of an integrated national network of fusion centers to promote two-way sharing with the federal government, as discussed earlier. Toward developing this network, the Program Manager and stakeholder agencies have sponsored fusion center conferences and provided staff, technical assistance, and funding to these centers.
- The FBI's Terrorist Screening Center (TSC)—established in September 2003—maintains the U.S. government's consolidated watch list of known or suspected terrorists and sends records from the list to agencies to support terrorism-related screening. The 9/11 Commission determined that agencies' failures to share information they had on several of the terrorists was a major factor in the lead-up to the 9/11 attacks, and we recommended in a 2003 report¹⁸ that agencies develop such a consolidated database of terrorist records. In response, the TSC created its consolidated database, which was completed in 2004. The TSC receives the majority of its watch list records from the NCTC, which compiles the information on known or suspected international terrorists from federal agencies. The FBI provides information on known or suspected terrorists who operate within the United States. The TSC consolidates this information and sends it to federal agencies that use it for screening purposes, such as the screening

¹⁸GAO, *Information Technology: Terrorist Watch Lists Should be Consolidated to Promote Better Integration and Sharing*. [GAO-03-322](#) (Washington, D.C.: Apr. 15, 2003).

of visa applicants and airline passengers. As noted in the annual report, the founding of the TSC is considered to be a key milestone in establishing the ISE. We and the Inspector General for the Department of Justice have also recommended ways in which agencies can enhance the watch list and agencies' terrorist-screening processes, such as addressing vulnerabilities and creating an interagency governing entity.¹⁹

Further Detailing What the ISE Is to Achieve and How It Will Operate Should Better Guide Implementation

The Program Manager, together with the ISE stakeholders, have followed standard practices in program and project management for defining, designing, and executing programs by identifying action items and strategic goals to be achieved in the implementation plan. However, work remains in, among other things, defining and communicating the scope and desired results to be achieved by the ISE, the specific milestones to be attained, and the individual projects—or initiatives—and execution sequence needed to achieve these results and implement the ISE. Standard practices in program and project management include (1) defining the program scope, roles and responsibilities, and specific results to be achieved, along with the individual projects needed to achieve these results, and (2) developing a road map, or program plan, to establish an order for executing specific projects needed to obtain defined programmatic results within a specified time frame and measuring progress and cost in doing so.

Further Defining and Communicating Key Elements of the ISE Will Help Address the Limitations of the ISE and Further Describe How the ISE Is to Operate

First, toward defining the scope of the ISE, the implementation plan restates the text of the Intelligence Reform Act, noting that the ISE encompasses “the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties” and that the ISE is defined as “an approach that facilitates the sharing of terrorism information.”²⁰ Indeed, this is a broad scope requiring the Program Manager and stakeholders, such as members of the Information Sharing Council, to further define what the ISE, as a

¹⁹GAO, *Terrorist Watch List Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List*. GAO-08-110 (Washington, DC.: Oct. 11, 2007) and U.S. Department of Justice Office of the Inspector General, *Follow-Up Audit of the Terrorist Screening Center*, Audit Report 07-41 (September 2007).

²⁰Program Manager, Information Sharing Environment, *Information Sharing Environment Implementation Plan* (Washington, D.C.: November 2006). As noted earlier, the Program Manager issued the *Implementation Plan* before the 9/11 Commission Act amendments that expressly broadened the scope of information to be shared within the ISE.

program, is to include as well as the scope of what it can address. Fundamentally, the Program Manager and stakeholders are still trying to fully define the scope and design of the ISE, and a more complete set of activities needed to achieve it than those that were included in the implementation plan, including, for example

- all of the terrorism-related information that should be a part of the ISE;
- what types of terrorism-related information ISE participants have and where such information resides;
- how the information can be put into a “shared space” so that a cross-sector of users can easily access and study information from different agencies;
- how this access can be provided while still protecting sensitive information and privacy interests;
- what information systems and networks will be integrated as part of the ISE and how; and
- methods for motivating agencies to invest in the ISE, be held accountable for ensuring that all relevant information is made available to ISE stakeholders, and identifying and implementing the specific projects needed to ensure the ISE runs effectively.

Further, the plan notes that the Intelligence Reform Act requires that the ISE ensure direct and continuous online electronic access to information²¹ and presents several action items intended to identify approaches for sharing information, including the use of technologies. However, the plan does not lay out a set of action items with related milestones for identifying, among other things, needed resources such as all the information to be made available as part of the ISE, the source of the information, and what limitations exist in making this counter-terrorism information available. In accordance with standard practices for program management, these are all elements critical for conveying the scope of what the ISE is to include, garnering an understanding among stakeholders of needs to be met as part of implementing the ISE, and identifying restrictions in stakeholder abilities to do so.

²¹Program Manager, Information Sharing Environment, *Information Sharing Environment Implementation Plan*.

We recognize that defining all of these elements is a complex undertaking, especially because of the numerous ISE stakeholders that need to coordinate and the many existing and often stovepiped or independent methods stakeholders use for meeting their information needs that often were not developed with sharing in mind. Nevertheless, further defining and communicating key elements of the ISE, such as the scope and expected results, along with a road map for meeting needs in accordance with standard practices for program management will help, among other things, communicate the breadth and limitations of the ISE as a program and further describe how the ISE is to operate.

Second, the plan does not communicate the scope, or parameters, of stakeholder roles and responsibilities in such a way that stakeholders can understand what they will be held accountable for in implementing and operating the ISE. For example, the plan identifies the Program Manager's role as responsible for information sharing across the government, overseeing the implementation of and managing the ISE, and working together with the ISC, but does not articulate aspects of how the Program Manager has interpreted this role in contrast to that of other stakeholders. For instance, the officials at the Office of the Program Manager noted:

- The Program Manager's office works on developing or improving existing business processes that affect information sharing among two or more of the five ISE communities, but does not focus on processes that are internal to ISE members unless they directly impact the wider ISE. Agencies, therefore, are to define ISE related business processes and other requirements internal to their organizations along with how the information will be used and drive their own analytical efforts.
- The Program Manager's role focuses on determining if a policy, business process, legal or technical issue is preventing the sharing of information between two or more communities and on helping to resolve these types of issues rather than issues that impact sharing within a community, such as homeland security.

This information on the parameters of the Program Manager's role and responsibilities was not transparently communicated in the plan but is critical for stakeholders, the Congress, and other policy makers to clearly understand, provide for accountability, and ensure the ISE is effectively implemented. Without clearly understanding their roles and responsibilities, stakeholders may not adequately prepare for and provide each other the information and services needed to prevent terrorist attacks. According to officials at the Office of the PM-ISE, departments

and agencies, not the Program Manager alone, are responsible for defining the ISE's scope and expected end state. Accordingly, in November 2007 they held a first-time off-site with ISC members to focus on ISE priorities, clarify responsibilities, and emphasize the importance of everyone's active participation and leadership. Moreover, the meeting was held to rectify any misperceptions and reinforce that all ISE stakeholders are to define the ISE. However, according to officials at the Office of the Program Manager, problems in department and agency participation make it difficult for the ISC to function as an advisory body for ISE implementation. Among other things, officials noted that departments and agencies do not always provide representatives with the authority to speak on behalf of the agency and inconsistent attendance by ISC representatives has been an issue.

Since issuance of the plan, on October 31, 2007, the *National Strategy for Information Sharing*²² was issued, in part, further communicating the scope of the ISE and stakeholder roles. The strategy reaffirmed that stakeholders at all levels of government, the private sector, and foreign allies play a role in the ISE. The strategy also outlined some responsibilities for ISE stakeholders at the state, local, and tribal government levels. In addition, the strategy 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 and improving information sharing versus other ISE stakeholders.

Third, the Program Manager and stakeholders are still in the process of defining the programmatic results to be achieved by the ISE as well as the associated milestones and projects needed, as standard practices in program management suggest 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

²²The White House, *National Strategy For Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*. (Washington, D.C.: Oct. 31, 2007).

will be carried out over a period of time, are outcome²³ oriented, and that are expressed so that progress in achieving the goals can be tracked and measured.²⁴ Moreover, these longer-term strategic goals should be supported by interim performance goals²⁵ (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). The implementation plan, as an early step in planning for the ISE, identifies six strategic ISE goals to be achieved. These goals include, for instance, 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, set up interim or annual goals and associated time sensitive milestones to be built upon to achieve the overall goal, or define how agencies will measure and ensure progress in meeting this goal in the interim or overall. Instead, the plan notes that performance measures will be developed at a later date. Moreover, 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 plan's issuance, officials in the office of the Program Manager and

²³In describing outcomes and output measures, OMB guidance notes the following: Outcomes describe the intended result of carrying out a program or activity. They define an event or condition that is external to the program or activity and that is of direct importance to the intended beneficiaries and/or the public. For a tornado warning system, an outcome measure could be the number of lives saved and property damage averted. In contrast, an output measure is one that describes the level of activity that will be provided over a period of time, including a description of the characteristics (e.g., timeliness) established as standards for the activity. Outputs refer to the internal activities of a program (i.e., the products and services delivered). For example, an output could be the percentage of warnings that occur more than 20 minutes before a tornado forms. While performance measures must distinguish between outcomes and outputs, there must be a reasonable connection between them, with outputs supporting (i.e., leading to) outcomes in a logical fashion. According to OMB, outcome measures are the most informative measures about performance because they are the ultimate results of a program that benefit the public.

²⁴See, 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).

²⁵Performance goals are comprised of performance measures, with targets and time frames, which serve as an indicator to gauge program performance against the goals.

stakeholders have developed several performance measures and, as of March 2008, were in the process of further refining them. Yet, our review of a draft of these performance measures showed that they continue to focus on counting activities accomplished rather than results achieved and do not yet outline the sequence of projects needed to implement the ISE and measurably report on progress in doing so.

Further, the plan identifies seven priority areas to be addressed in implementing the ISE. These include, for example, sharing with partners outside the federal government, promoting a culture of information sharing, and establishing ISE operational capabilities. But like the strategic goals, the priority areas represent general tasks and themes to be addressed as part of the ISE and do not define expected results in a measurable form, along with supporting performance goals, measures, and deadlines for achieving the programmatic results. Without these elements, ISE stakeholders may not understand the interim or final ISE they are to achieve, assess progress towards implementing the ISE, or hold stakeholders accountable for their contributions in ensuring that the ISE succeeds.

Fourth, although required by the Intelligence Reform Act, the implementation plan did not provide a budget estimate that identified the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE but indicated that steps to develop a budget estimate would be taken in the future. In part, this is because the ISE was in such an early stage of development that it would be difficult for agencies to know what to cost out for an estimate. Developing a budget estimate, however, is a commonly used tool for effective program management. While the Program Manager has been working with agencies and the Office of Management and Budget to determine the cost of implementing the ISE, officials at the Office of the Program Manager stated that the total cost of the ISE has not yet been accounted for and that attaining an overall estimate may not be achievable. This is because it is difficult for agencies to isolate and separate out what actions they are undertaking solely to implement the ISE versus ongoing operations. We recognize that attaining an accurate and reliable cost estimate for the ISE is a difficult undertaking, complicated further by the fact that stakeholders are still defining the scope of the ISE, results to be attained, and the projects to support it. However, without information on how much the ISE will cost, Congress and stakeholders will be unable to determine whether the expenses associated with the ISE are worth the results attained and in some cases unable to determine what has been accomplished given the expended resources. Toward addressing this cost issue, the PM-ISE, in

collaboration with OMB, has since issued program guidance intended to assist in estimating and tracking ISE costs in ISE priority areas, such as suspicious activity reporting, developing ISE shared space, and alerts, warnings, and notifications.

Finally, while the implementation plan states that Phase 1 will conclude with the development of a detailed plan for implementation, including goals, measures, and targets, a revised plan will not be issued. Instead, officials at the Office of the Program Manager indicated that they consider the implementation plan to be a living document with initiatives identified at the outset of development being refined as needed based on experience. Officials at the Office of the Program Manager acknowledged that the 89 action items contained in the plan do not address all of the activities that must be completed to implement the ISE. This is because at the time the plan was produced, agreement on how the ISE is to function and what it is to include had not been reached among the stakeholders. Work toward reaching these agreements remains ongoing. Therefore, program officials stated that an assessment of the ISE's progress based on the action items identified in the plan alone would not give a true sense of progress toward a fully functioning and executed ISE. Accordingly, the PM-ISE intends to adjust the plan, beginning with refinements in the next annual report. For example, according to officials at the Office of the Program Manager, to avoid delaying progress, the office plans to revise and update certain implementation plan actions in the course of developing the June 2008 Annual Report. In addition, officials at the Office of the Program Manager stated that based on their experience in Phase 1, they are deleting action items that are no longer valid and updating others to reflect the ISE's current approach for implementation.

Making midcourse corrections to further determine and articulate the end design of the ISE, or at least more accurately specify what is to be achieved in the near term and at various milestones thereafter, is in accordance with standard practices in program and project management. However, given the ISE's many stakeholders and the work that remains to be done in defining the scope of the ISE, the desired results to be achieved, and the supporting projects and milestones, it is important that the revisions, in accordance with standard practices for program management, provide for an effective road map to implement the ISE and measure achieved progress in implementing the ISE and in improving information sharing. Without such a road map, the Program Manager and stakeholders risk not being able to effectively manage and implement the ISE.

An ISE Enterprise Architecture Framework Has Been Developed, but Its Usefulness May Be Limited without Further Defining ISE Results

Subsequent to the implementation plan, in August 2007, the Program Manager issued the *ISE Enterprise Architecture Framework Version 1.0* (ISE EAF), a planning document and tool intended to further inform ISE implementation efforts, but its usefulness in guiding the ISE to meet terrorism-related information-sharing needs may be hindered by the lack of defined programmatic results to be achieved. As reported by the Program Manager, the ISE EAF is to help improve information-sharing practices, reduce barriers to sharing, and institutionalize sharing by providing a new construct, or framework, for planning, installing, and operating nationwide information resources within the ISE. Such resources may include, for example, business processes and information technologies. Further, as noted in the EAF, it is to be used to guide the implementation of the ISE, accounting for current capabilities and setting the direction and steps towards the envisioned or To-Be capabilities. Because the ISE is composed of many organizations, the ISE EAF can be looked at as a collection of independent stakeholder enterprise architectures²⁶ that were initially designed to support individual missions, but are now being leveraged to facilitate terrorism-related information sharing among these organizations. In doing so, the ISE EAF is to assist in identifying the relationships needed to facilitate terrorism information sharing among these organizations and is to serve as a tool for understanding what, where, and for what purpose current capabilities and resources, such as information technology systems, may exist.

Enterprise architectures generally use strategic planning elements to align potential system solutions with program needs. While the ISE EAF is intended to augment organizations' enterprise architectures for the purpose of sharing terrorism-related information, work remains to determine the ISE's desired program outcomes or specific results to be achieved, potentially limiting the effectiveness of the ISE EAF in guiding the ISE to meet terrorism-related information sharing needs. Unlike agency enterprise architectures, the ISE EAF does not seek to identify, for example, business processes and information flows at an operational level,

²⁶Generally speaking, an enterprise architecture is to connect an organization's strategic plan with program and system solution implementations by providing the details needed to guide investments in a consistent, coordinated, and integrated fashion. An enterprise architecture is intended to provide a clear and comprehensive picture of an entity, whether it is an organization (e.g., federal department) or a functional or mission area that cuts across more than one organization (e.g., homeland security). This picture is to consist of snapshots of both the enterprise's current or "As Is" operational and technological environment and its target or "To Be" environment, as well as a capital investment road map for transitioning from the current to the target environment.

the level at which organizations determine how specific investments in technologies will be used to support business needs and provide needed information. Instead, the ISE EAF relies on the prerogative of individual departments and agencies to define operational processes and information flows as part of their enterprise architectures. Officials at the Office of the Program Manager noted that OMB and the ISC agencies were very specific about the level of detail the ISE EAF was to take, noting that the ISE EAF helps inform, but not direct, how departments and agencies do their work at the operational level—individually or together. However, without further defining outcomes to be achieved and identifying how individual agencies are to work together to meet ISE information-sharing needs at the level where work is done, the ISE EAF may be limited in its usefulness for improving the sharing of terrorism-related information.

The Program Manager Has Issued the First Annual Report and Is Developing Initial Performance Measures, but Neither Can Yet Be Used to Determine How Much Progress Has Been Made and What Remains

To describe progress in implementing the ISE to date, the Program Manager issued an annual report—in response to the Intelligence Reform Act’s requirement for a yearly performance management report—in September 2007 that highlighted individual accomplishments and included annual performance goals and has since developed some performance measures, but neither effort shows how much measurable progress has been made toward implementing the ISE and how much remains to be done. In keeping with federal guidance, our work, and the work of others in strategic planning, performance measurement, and program management, the annual report contained four performance goals for 2008. Additionally, some initial performance measures have been developed, but they do not address all aspects of the annual performance goals or strategic goals and do not show how they represent interim milestones to ensure attainment of desired results or outcomes. According to officials at the Office of the Program Manager, these performance measures are currently being refined in consultation with the ISC to provide the needed framework to measure real progress made. We acknowledge that creating such measures is difficult, particularly since the program is still being designed, but until these measures are refined to account for and communicate progress and results, future attempts to measure and report on progress will be hampered.

The Annual Report Cited Accomplishments Made in Implementing the ISE, but Not the Extent of Progress Achieved and Remaining Work

The annual report conveyed individual ISE-related accomplishments as of September 2007 but did not provide Congress and policy makers with information on what portion of the ISE has been completed as a result of this work and what portion remains. The report lists the preliminary actions taken to prepare for establishing the ISE, such as designation of the Program Manager, the President's memorandum providing guidelines for the ISE, and submission of the implementation plan to the Congress. The report also cites individual accomplishments that contribute to the ISE, some of which were accomplished under the implementation plan—such as establishment of an electronic directory service for users to find contact information for organizations that have counter-terrorism missions—and others achieved prior to and or separate from efforts to create the ISE. For instance, the report cites several accomplishments attained prior to the December 2004 Intelligence Reform Act and its call for an ISE, including the creation of the National Counterterrorism Center (NCTC) in August 2004 and the establishment of the Terrorist Screening Center (TSC) in 2003. In part, because ISE implementation remains in the early stages, the annual report highlighted these discrete accomplishments without putting them in an overall context that showed how much progress has been made and remains toward implementing the ISE. While, as previously noted, the implementation plan identified a two phased approach for implementing the ISE along with 89 action items—the only means presented in the implementation plan for tracking completion of ISE implementation—the report did not provide a one-for-one reporting on the status of these action items as steps for implementing the ISE or identify how much of the implementation had been completed. Thus, the Congress and policy makers do not yet have the information they need to assess the amount and rate of progress, remaining gaps, and the need for any intervening strategies.

Performance Measures Are Being Developed Although They Do Not Yet Address All Aspects of the Annual Performance Goals

In accordance with existing federal guidance as well as our work and the work of others in strategic planning, performance measurement, and program management, programs should have overarching strategic goals that state the program's aim or purpose, define how it will be carried out over a period of time, are outcome oriented, and are expressed so that progress in achieving the goals can be tracked and measured. Moreover, these longer-term strategic goals should be supported by interim performance goals²⁷ (e.g., annual performance goals) that are also

²⁷Performance goals are comprised of performance measures, with targets and time frames, which serve as indicators to gauge program performance against the goals.

measurable, define the results to be achieved within specified time frames, and provide for a way to measure and track annual and overall progress (e.g., through measure and metrics). Accordingly, the implementation plan contained six overall strategic goals and the annual report contained four annual performance goals for 2008, as shown in tables 2 and 3.

Table 2: Strategic Goals Contained in the Implementation Plan

1. Facilitate the establishment of a trusted partnership among all levels of government, the private sector, and foreign partners.
2. Promote an information-sharing culture among ISE partners by facilitating the improved sharing of timely, validated, protected, and actionable terrorism information supported by extensive education, training, and awareness programs for ISE participants.
3. To the maximum extent possible, function in a decentralized, distributed, and coordinated manner.
4. Develop and deploy incrementally, leveraging existing information sharing capabilities while also creating new core functions and services.
5. Enable the federal government to speak with one voice on terrorism-related matters, and to promote more rapid and effective interchange and coordination among federal departments and agencies and state, local, and tribal governments, the private sector, and foreign partners, thus ensuring effective multi-directional sharing of information.
6. Ensure sharing procedures and policies protect information privacy and civil liberties.

Source: Information Sharing Environment Implementation Plan, November 2006.

Table 3: 2008 Annual Performance Goals Listed in the Annual Report

ISE functional areas	2008 ISE performance goals
Improving sharing practices	Establish a set of activities and strategic approaches to facilitate sharing among all levels of government, private sector, and foreign partners.
Creating a culture of sharing	Develop a shared set of values that change behavior of ISE participants through established training programs, trained personnel, incentive programs, and privacy protections among ISE participants.
Reducing barriers to sharing	Establish operability that facilitates sharing through a common ISE information technology security framework to include approved ISE-wide information assurance solutions, governmentwide physical and personnel security practices, as well as controlled unclassified information framework across the ISE.

ISE functional areas	2008 ISE performance goals
Institutionalizing sharing	Establish capabilities that allow ISE participants to create and use quality terrorism-related information by improving business processes, developing a common enterprise architecture framework, refining common standards, and instituting effective resource management for governmentwide programs.

Source: Annual Report to the Congress on the Information Sharing Environment, September 2007.

While not reflected in the first annual report, the Program Manager and agencies have begun to develop performance measures to improve future reporting on progress in implementing the ISE and information sharing overall, but these measures focus on counting activities accomplished rather than results achieved to show the extent of ISE implementation and attaining the ISE’s strategic goals. In accordance with our work and federal guidance on strategic planning and performance measurement, the newly developed measures represent an effort to more concretely and quantitatively assess progress in implementing the ISE and improving information sharing. 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. Indeed, these measures are an important first step in providing quantitative data for assessing progress made in information sharing and help to inform Congress and other stakeholders on specific information sharing improvements. But, taking the measures to the next step—from counting activities to results or outcomes—while difficult, is important to assess results achieved.

The Program Manager and ISE stakeholders have not yet developed measures to address all aspects of the annual performance goals. For example, one 2008 performance goal identified in the annual report is to establish capabilities that allow ISE participants to create and use quality terrorism-related information by improving business processes, developing a common enterprise architecture framework, refining common standards, and instituting effective resource management for governmentwide programs. Based on the description of this performance goal, one ISE performance measure that supports this goal includes attaining the percentage of applicable ISE organizations that have adopted

the common terrorism information sharing standards during the past or preceding fiscal year(s). However, performance measures in support of all topics identified in the goal, such as instituting effective resource management for governmentwide programs, have not been developed. Further, the performance measures are not presented in a way that explains how they represent milestones toward attaining the strategic goals or intended outcomes. According to officials at the Office of the Program Manager, as of March 2008, they are refining their measures in consultation with the ISC to provide an improved framework to measure progress made. Yet, our review of a draft of these performance measures showed that they continue to focus on counting activities accomplished rather than results achieved. We acknowledge that creating such measures is difficult, particularly since the program is still being designed, but until these measures are refined to account for and communicate progress and results, future attempts to measure and report on progress will be hampered.

Conclusions

Although the Program Manager and stakeholders have made progress in implementing a number of initiatives, successfully implementing the ISE remains a daunting task. While efforts to date may represent the groundwork needed to facilitate terrorism-related information sharing in the future, over 3 years after passage of the Intelligence Reform Act, the ISE is still without a clear definition of the specific results to be achieved as part of the ISE or the projects, stakeholder contributions, and other means needed to achieve these results. The Program Manager, together with the ISE stakeholders, have followed standard practices in program and project management for defining, designing, and executing programs by identifying action items and strategic goals to be achieved in the implementation plan. However, work remains in, among other things, defining and communicating the scope and desired results to be achieved by the ISE, specific milestones to achieve the results, and the individual projects and execution sequence needed to achieve these results and implement the ISE. Until this work is complete, further efforts may result in independent contributions to improving information sharing rather than an ISE with improved and coordinated sharing of terrorism-related information among stakeholders, a critical need exposed by the terrorist attacks of September 11. Given that the ISE requires extensive buy-in from stakeholders and the Program Manager is relying on stakeholders to provide technology and other resources to make the ISE work, it is critical to develop a road map for implementing the ISE and improving information sharing that communicates the scope and specific results to be achieved by the ISE, the key milestones and individual projects needed

to implement the ISE, needed resources, and stakeholder responsibilities. Without such a road map, the Program Manager risks not being able to effectively manage and implement the ISE.

Furthermore, efforts to report on progress to date have provided examples of individual actions taken to improve information sharing but have not yet included an accounting of how far the Program Manager and stakeholder agencies are in achieving an effectively functioning ISE and what remains to be done. By not doing so, stakeholders do not have a measurable way to ensure that the sharing of terrorism-related information has improved and by how much, nor the information needed to understand the resources and time frames required to achieve the intended results of the ISE. Until the Program Manager and stakeholders more fully define the specific results the ISE is to attain and develop a set of measures to assess progress in achieving the goals—including, at a minimum, what has been done and what remains to be accomplished—Congress and stakeholders will not know how far the nation has come in implementing an ISE intended to improve governmentwide information sharing.

Recommendations

To help ensure that the ISE is on a measurable track to success, we are recommending that the Program Manager, with full participation of relevant stakeholders (e.g., agencies and departments on the ISC), take the following two actions

- 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
- 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.

Agency Comments and Our Evaluation

We requested comments on a draft of this report from the Secretaries of Defense, Homeland Security, and State, as well as the Attorney General, the Director of National Intelligence, and the Program Manager for the ISE or their designees. In a June 6, 2008, letter, the Program Manager for the ISE provided written comments, which are summarized below and included in their entirety in appendix II.

The Program Manager generally agreed with our recommendations to more fully define the scope and results to be achieved by the ISE and develop a comprehensive set of performance measures that show the extent to which the ISE has been implemented and sharing improved.

While the Program Manager agreed with our recommendations, he commented that the ISE is a governmentwide transformational effort—emphasizing that the ISE is an evolutionary process—and not a traditional “program.” Therefore, according to the Program Manager, trying to audit this interagency initiative strictly within program parameters presents problems. We agree that the ISE is a governmentwide transformational effort, that it is not a traditional “program,” and that it involves an evolutionary process. In fact, our report states that the ISE is not bounded by a single federal agency or component and that it is a broad-based coordination and collaboration effort among various stakeholders. While we agree that the ISE is not a traditional “program,” in that it is not operated and funded by a single department or agency, it is an activity that does receive government funding and can be reviewed using program and project management principles. As such, we based our evaluation of the ISE on a broad set of program and project management criteria, including the Government Performance and Results Act of 1993, related guidance issued by OMB, and our prior work on results-oriented government, program management, and federal coordination and collaboration. Further, while we recognize that approaches to implementing the ISE and improving information sharing may evolve over time as technologies and needs change, calling the ISE an evolutionary process does not exempt it from following the practices outlined in our report. Following these practices will help ensure that reports of progress by the Program Manager on behalf of the ISE at large are based on measures of results achieved toward implementing the ISE—that is measured based on what the ISE is to be, include, and accomplish in, for example, 3 years—rather than ad-hoc claims of progress.

With regard to efforts for assessing the ISE’s progress, the Program Manager noted that in the 2007 annual report he introduced a performance management approach and his office has since established a performance baseline—in the fall of 2007— and measured agencies’ progress against this baseline through an assessment performed in the spring of 2008. Our report acknowledges these efforts. However, our review of the performance measures developed in support of the performance management approach shows that these measures: (1) focus on counting activities accomplished rather than results achieved to show the extent of ISE implementation and attaining the ISE’s strategic goals and (2) are not

presented in a way that explains how the measures represent milestones toward attaining the strategic goals identified in the implementation plan or intended outcomes. In his comments, the Program Manager further noted that the June 2008 annual report, which was not released by the time we issued this report, would provide more current data on performance measurement. However, our review of a draft of the measures to be incorporated in the 2008 report showed that they continue to focus on counting activities accomplished rather than results achieved. Unless the 2008 report corrects these shortfalls and establishes a performance management mechanism whereby short-term annual goals serve as steps for assessing the ISE's progress towards achieving longer-term strategic goals, it and future reports on progress will fail to provide the Congress and other policy makers the meaningful information needed to understand what progress has been made in attaining the defined strategic results for the ISE and improving information sharing.

Finally, the Program Manager said that although the report mentions that one of the challenges of the ISE is interagency attention and priority to ISE initiatives, the report does not make any recommendations in this regard. We agree that interagency collaboration in the ISE is a challenge and individual departments and agencies, not the Program Manager alone, have responsibilities in implementing the ISE. However, to effectively hold these agencies accountable for ISE progress, existing issues identified in our report—such as defining the outcomes to be achieved and defining clear roles and responsibilities—must first be addressed. Given the ISE's many stakeholders and recognizing the Program Manager's key leadership role for *managing* the ISE, we maintain that these issues must be addressed by the Program Manager, with full participation of relevant stakeholders (e.g., agencies and departments on the ISC). Without doing so, the Program Manager may continue to face challenges in attaining agency buy-in and holding stakeholders accountable for ISE progress.

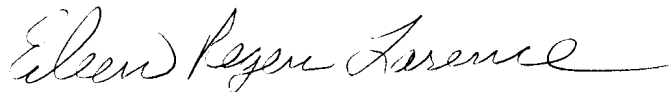
Officials in the Office of the Program Manager also provided technical comments on the draft that have been incorporated, as appropriate.

The Secretaries of Defense, Homeland Security, and State; the Attorney General; and the Director of National Intelligence responded that they did not have any comments on the report.

As agreed with your offices, unless you publicly release the contents of this report earlier, we plan no further distribution until 30 days from the report date. We will then send copies of this report to the Program

Manager for the ISE, the Director of National Intelligence, and the Secretaries of the Departments of Defense, Homeland Security, Justice, and State; and interested congressional committees. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, please contact either Eileen Larence at 202-512-8777 or larencee@gao.gov, or David Powner at 202-512-9286 or pownerd@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.



Eileen R. Larence
Director, Homeland Security and Justice Issues



David A. Powner
Director, Information Technology
Management Issues

List of Congressional Requesters

The Honorable Joseph Lieberman
Chairman

The Honorable Susan Collins
Ranking Member
Committee on Homeland Security
and Government Affairs
United States Senate

The Honorable Daniel K. Akaka
Chairman
Subcommittee on Oversight of Government
Management, the Federal Workforce and the
District of Columbia
Committee on Homeland Security
and Governmental Affairs
United States Senate

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

The Honorable Jane Harman
Chair
Subcommittee on Intelligence, Information Sharing,
and Terrorism Risk Assessment
Committee on Homeland Security
House of Representatives

Appendix I: Status of Phase I Action Items as of March 1, 2008

Table 1 below provides the status of each of the 48 Phase 1 action items identified in the ISE implementation plan as of July 9, 2007, nine days after their planned completion date and as of March 1, 2008. These action items encompass many areas for development in the ISE, ranging from activities such as identifying capabilities and technology to privacy protection and performance measures. As the table indicates, based on our analysis of status information reported by the Program Manager, at the end of phase one's scheduled completion, 18 of 48 action items had been completed and 30 remained incomplete. Eight months later, 33 of 48 action items had been completed, with 15 remaining incomplete. In determining the status of the action items, we reviewed documentation provided by the Program Manager, but did not evaluate the effectiveness of the actions taken.

Table 4: Comparison of Action Item Status in July 2007 and March 2008

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
1.01 The Program Manager for the Information Sharing Environment (PM-ISE) and Information Sharing Council (ISC) members will identify the alerts and notifications to be available to federal and non-federal ISE participants and the enabling policies and business processes necessary to implement the alert and notification capability. (Planned completion: March 2007)	Not complete but in process	Not complete but in process	An initial survey of alerts and notifications has been conducted to identify, among other things, the alerts and warnings that departments and agencies provide to ISE partners as well as the method for distributing the alerts and notifications. According to officials at the PM-ISE, ISC agency representatives are validating this survey and preliminary findings, with draft information flows for major alerts and warnings functions being developed for potential inclusion in the next published version of the Information Sharing Environment Enterprise Architecture Framework (ISE EAF). These officials further noted that expected future activities include further assessing the remaining ISC agencies' alerts and warnings efforts, surveying state, local, and tribal participants, and developing an ISE-wide framework for terrorism-related alerts, warnings, and notifications.

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
<p>1.02 The PM-ISE and ISC members will identify existing technologies, capabilities, and programs (e.g., Homeland Security Presidential Directive-12 and Federal Information Processing Standard 201) that provide easier user access, but still support identity management through audits, authentication, and access controls. The ISC will assess the technologies and pilot programs to determine whether or not the technologies support its user base and are suitable for ISE adoption. (Planned completion: June 2007)</p>	<p>Not complete but in process</p>	<p>Not complete but in process</p>	<p>According to PM-ISE officials, the action specified in Task 1.02 did not adequately support the needs of the ISE, resulting in an altered approach for addressing identity management and user access across the ISE. PM-ISE officials told us that existing identity management solutions support the individual participant's mission needs, but the many differing identity management schemes throughout the ISE participants' networks do not directly support the ISE as a whole. Therefore, the ISE expects to leverage existing identity management schemes, but not create a new identity management solution specific to the ISE. Accordingly, in December 2007, the PM-ISE's Business Process Working Group produced the <i>Business Process Analysis Paper on Access Process</i>. This paper identified five requirements to enable ISE user access to terrorism-related information. According to PM-ISE officials, these requirements are being incorporated into ISE architecture documents and are expected to enable departments and agencies to derive lower level requirements. Further, according to officials, this paper is being used in an ongoing initiative to evaluate PM-ISE sponsored pilots that demonstrated capabilities in remote wireless access, federated identity management (referenced in Action 1.03) and role-based search.</p>
<p>1.03 The PM-ISE and ISC members will determine what ISE-wide identity management capabilities are practical and develop a detailed set of requirements and Project Plan for implementation of such capabilities in a time frame consistent with technology maturity and available budgetary resources. (Planned completion: June 2007)</p>	<p>Not complete but in process</p>	<p>Not complete but in process</p>	<p>The PM-ISE is currently sponsoring a pilot project on identity management and access intended to demonstrate an initial capability to share electronic identity information and use that information to enable assured access to information stored across the different ISE communities. According to PM-ISE officials, the pilot is building an operational, federated access management capability by leveraging existing identity management solutions and evaluating technologies, policies, and procedures for potential ISE identity management solutions. The completion of the pilot is expected to result in documenting which identity management capabilities may provide the most value to the ISE.</p>

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
1.04 The PM-ISE and ISC members will investigate existing or emerging capabilities that discover data and information within the federal government and industry. The initial implementation of enterprise search will apply a search engine to index both structured and unstructured data. This activity will include the evaluation of several ongoing pilot programs using technologies that integrate data across heterogeneous networks and data stores to enhance the "findability" of relevant information and the interoperability of data and information. (Planned completion: June 2007)	Complete	Complete	Complete
1.05 The PM-ISE and the ISC will work with the Cross Domain Management Office to establish a process to ensure that cross-domain solutions developed through this office meet the needs of ISE participants. (Planned completion: March 2007)	Complete	Complete	Complete
1.06 The PM-ISE and ISC members will identify existing collaborative tools that are used and operational in the counterterrorism or other analytic or investigative communities and review the feasibility of adopting common tools for use across the ISE. (Planned completion: March 2007)	Complete	Complete	Complete
1.07 The PM-ISE and ISC members will develop requirements to implement new and emerging collaborative technologies. (Planned completion: June 2007)	Not complete but in process	Not complete but in process	A Business Process Analysis paper on the Collaboration Process, dated October 1, 2007, has been developed. The stated purpose of the document includes conveying key user requirements, implementation considerations, and describing a future-state process description for the ISE Collaboration Process. According to officials at the office of the PM-ISE, this paper was disseminated to the Business Process Working Group in December 2007 as part of a larger analysis of ISE service processes. They further noted that the requirements identified through this effort are being incorporated into the ISE EAF documents.

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
1.08 The PM-ISE and the ISC members will implement the Electronic Directory Services Blue, Yellow, and Green Pages in the sensitive compartmented information, secret, and sensitive but unclassified security domains. (Planned completion: June 2007)	Not complete but in process	Complete	Complete (Note: The PM-ISE subsequently altered this action item, deciding it would no longer complete the Green Pages in the sensitive-but-unclassified security domain due to aggregation issues. According to officials at the Office of the PM-ISE, aggregating the information for the Green Pages would no longer enable the information to be posted in an unclassified domain.)
1.09 The PM-ISE and the ISC members will implement Electronic Directory Services White Pages in the secret compartmented information and secret security domains. (Planned completion: June 2007)	Not complete but in process	Complete	Complete (Note: The ISC altered this action item, deciding it would no longer complete the White Pages in the secret security domain).
1.10 The PM-ISE, in consultation with the ISC, will publish a preliminary version of the <i>ISE Enterprise Architecture Framework</i> (ISE EAF) Document providing the models with major portions of the ISE and their attributes. (Planned completion: December 2006)	Not complete but in process	Complete	Complete
1.11 The Office of Management and Budget, in the Federal Enterprise Architecture (FEA) Business Reference Model, will include "Information Sharing" as a new government subfunction, Business Reference Model code 143, with the "Information and Technology Management" Line of Business, Business Reference Model code 404. (Planned completion: December 2006)	Not complete but in process	Complete	Complete (Note: Action item 1.11 is complete, except the code 143 is actually 262.)
1.12 The PM-ISE will work with National Security Agency, the National Institute of Standards and Technology, Director of National Intelligence/Chief Information Officer, and the Committee on National Security Systems on incorporating network security and information assurance policies and practices for the ISE EAF and associated functional standards. (Planned completion: March 2007)	Not complete but in process	Complete	Complete

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
1.13 The PM-ISE, in consultation with the ISC, will publish a fully documented ISE EAF Document and a Federal Enterprise Architecture-ISE profile. The development process will be worked in collaboration with the Office of Management and Budget, department and agency chief information officers, and ISC members. (Planned completion: March 2007)	Not complete but in process	Not complete but in process	Version 1.0 of the ISE EAF has been published and a draft version of the ISE profile has been developed and is undergoing review by the Chief Information Officers Council as a formal FEA Profile in the E-Gov program. Officials at the Office of the PM-ISE noted that an approval letter for the FEA Profile is pending signature by the Office of Management and Budget.
1.14 The PM-ISE, in consultation with the ISC, will develop a configuration management process for the control and management of updates to the ISE EAF document and Federal Enterprise Architecture-ISE profile. (Planned completion: December 2006)	Not complete but in process	Complete	Complete
1.15 The Office of Management and Budget, in the Federal Enterprise Architecture Reference Models, will add the ISE EAF and the Federal Enterprise Architecture-ISE profile as compliance requirements in the <i>Federal Transition Framework</i> , a catalog of cross-agency initiatives, and the <i>Federal Enterprise Architecture Program: Enterprise Architecture Assessment Framework</i> , the maturity assessment guide for Federal enterprise architectures. (Planned completion: March 2007)	Complete	Complete	Complete
1.16 DHS will work with the PM-ISE to review existing policies and procedures for ascertaining relevant and effective approaches to migrate the ISE EAF models and attributes into the private sector. (Planned completion: June 2007)	Complete	Complete	Complete

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
<p>1.17 The PM-ISE will convene and chair a new working group, the Common Terrorism Information Sharing Standards Working Group, with representatives from all ISC members, the National Communications System, the National Institute of Standards and Technology (NIST), and the Committee on National Security Systems tasked with selecting and issuing information-sharing standards, approved through the ISC, and formally published by NIST. The Common Terrorism Information Sharing Standards may include new standards that agencies will introduce to affect on-going investment activities as project schedules and funding permit. Future funded investments incorporating the Common Terrorism Information Sharing Standards will be compatible with the federal enterprise architecture and national security system enterprise architectures, and identified in normal agency submittals to the Office of Management and Budget. The Common Terrorism Information Sharing Standards Working Group will issue common terrorism information sharing standards recommendations to the ISC for information sharing standards for non-federal government agencies. (Planned completion: December 2006)</p>	Complete	Complete	Complete

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
<p>1.18 Departments and agencies will begin to incorporate the common terrorism information sharing standards into investment planning, consistent with ISE EAF incorporation, with full common terrorism information sharing standards incorporation into investments beginning execution in fiscal year 2009. This will include both civil and national security system investments. Agencies will also incorporate the common terrorism information sharing standards into information resource lifecycle processes to include capital planning and investment control processes. The common terrorism information sharing standards will provide the source of functional standards for information sharing in the Federal Enterprise Architecture's Technical and Data Reference Models. (Planned completion: June 2007)</p>	<p>Not complete but in process</p>	<p>Not complete but in process</p>	<p>In December 2006, the Office of Management and Budget released the Federal Transition Framework Version 1.0. The Office of Management and Budget described the Federal Transition Framework as a single source for clear and consistent information describing government-wide information technology policy objectives and cross-agency initiatives, such as the E-Gov and line of business initiatives. According to officials at the Office of the PM-ISE, having the ISE descriptions in the Federal Transition Framework was a first step in ensuring that the PM-ISE and the Common Terrorism Information Sharing Standards are part of each agency's capital planning and investment control investment life-cycle.</p> <p>In October 2007 the <i>Common Terrorism Information Sharing Standards Program Manual, Version 1.0</i> was published. According to PM-ISE officials, they plan to conduct ISE management reviews (IMRs) with departments and agencies to assess if departments and agencies have incorporated the Common Terrorism Information Sharing Standards into investment planning. These reviews are expected to occur in April or May of 2008. PM-ISE officials further noted that they, in conjunction with the Office of Management and Budget, plan to conduct enterprise architecture reviews with departments and agencies in March 2008 that, in part, are based on the <i>Federal Transition Framework Catalog</i>.</p>

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
<p>1.19 The PM-ISE, in consultation with the ISC, will develop the common terrorism information sharing standards, version 2.0 addressing additional processes, including those with foreign partners, and releasing priority functional standards supporting suspicious activity reports, cargo management and tracking, and general identity management. (Planned completion: June 2007)</p>	<p>Not complete but in process</p>	<p>Not complete but in process</p>	<p>The <i>Common Terrorism Information Sharing Standards Program Manual, Version 1.0</i>, was published in October 2007. According to PM-ISE officials, specific functional standards will be developed and published as required. According to officials at the Office of the PM-ISE, efforts to date include:</p> <ul style="list-style-type: none"> • development of functional standards for ISE suspicious activity reports; • coordination of cargo management and tracking standards currently underway; and • efforts to evaluate identify management technologies and processes remain underway through the Identity Management Pilot. Best practices and recommendations are to be developed as a result of this pilot and are intended to lead to the development of functional standards, as appropriate. <p>According to PM-ISE officials, efforts to coordinate with foreign partners will commence with the initiation of the second phase of the Foreign Government Information Sharing Working Group and Guideline 4 efforts.</p>
<p>1.20 Within 30-days of approval of the proposed Guideline 2 framework, the PM-ISE, in consultation with the ISC, will establish a Senior Level Advisory Group—consisting of ISC members or their designees—to ensure accountability, oversight, and governance for the effective operation of the framework. The advisory group will report the results of its oversight to the PM-ISE and the ISC. The advisory group will meet at least once per month during the first year of implementation. (Planned completion: December 2006)</p>	<p>Complete</p>	<p>Complete</p>	<p>Complete</p>

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
<p>1.21 Within seven days of approval of the proposed framework, there will be established an implementation team—comprised of representatives from the Department of Defense; the Department of the Interior; the Department of Homeland Security; the Federal Bureau of Investigation; the National Counterterrorism Center; appropriate state, local, tribal, and private sector advocates; and the PM-ISE—to develop an implementation plan for the Interagency Threat Assessment and Coordination Group framework and to ensure its timely execution. The implementation team will develop and implement plans to notify state, local, and tribal officials of the Interagency Threat Assessment and Coordination Group’s mission and responsibilities. (Planned completion: December 2006)</p>	Complete	Complete	Complete
<p>1.22 The Interagency Threat Assessment and Coordination Group implementation team will submit semiannual reports to the PM-ISE that identify successes and shortcomings in implementing and operating the ISE within the Guideline 2 framework and outline steps to refine and improve the framework’s operation. (Planned completion: Ongoing with first report due in the first quarter of Calendar Year 2007)</p>	Complete	Complete	Complete
<p>1.23 The PM-ISE will establish a federal fusion center coordination group to identify federal resources to support the development of a network of state-sponsored fusion centers charged to share information at all levels of the ISE and will recommend funding options. (Planned completion: December 2006)</p>	Complete	Complete	Complete
<p>1.24 The Department of Justice and the Department of Homeland Security will work with governors or other senior state and local leaders to designate a single fusion center to serve as the statewide or regional hub to interface with the federal government and through which to coordinate the gathering, processing, analysis, and dissemination of terrorism information. (Planned completion: March 2007)</p>	Not complete but in process	Complete	Complete

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
1.25 The Department of Justice and the Department of Homeland Security, to the extent possible and practicable, will assume the responsibility for technical assistance and training to support the establishment and operation of these fusion centers. (Planned completion: March 2007)	Complete	Complete	Complete
1.26 Appropriate federal departments and agencies will assess resources and develop and coordinate plans to assign representative personnel to state and local fusion centers. These representatives will work to the extent possible to further integrate—and where appropriate collocate—federal and state/regional resources. (Planned completion: March 2007)	Not complete but in process	Not complete but in process	A DHS/FBI Joint Deployment Plan was drafted in response to this action item, but remained in draft form at the end of Phase 1. This deployment plan is seen as a first step with additional coordination with stakeholders remaining to fully address this action item.
1.27 The Private Sector Subcommittee will produce a plan that implements elements of the framework as it affects the private sector. This plan must be consistent with statutes and presidential direction and ensure that information and privacy and legal rights are adequately protected. (Planned completion: June 2007)	Not complete but in process	Not complete but in process	A plan for implementing this action item was not in place by the end of Phase 1. However, several steps were taken towards meeting this action item. For example, DHS and members of the Critical Infrastructure Partnership Advisory Council jointly established a working group on information-sharing. The PM-ISE stated that this working group is expected to be the ISC conduit into the Critical Infrastructure Partnership Advisory Council and its private sector members, consisting of designated representatives from all the critical infrastructure and key resources sectors. The responsibilities of this working group are expected to include supporting the universe of government information-sharing initiatives coordinated by the PM-ISE that require engagement with the private sector (critical infrastructure and key resources owner/operator representatives) under the Critical Infrastructure Partnership Advisory Council structure. Further, an initial framework for private sector participation was drafted.
1.28 The Foreign Government Information Sharing Working Group, with coordination and assistance from the PM-ISE, will develop recommendations on Privacy Act systems of records notices and routine uses for the Guideline 5 Working Group. (Planned completion: March 2007)	Complete	Complete	Complete

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
1.29 The Foreign Government Information Sharing Working Group, with coordination and assistance from the PM-ISE, will develop a checklist of issues that need to be taken into account in negotiating international agreements, including privacy protections and possible review procedures. (Planned completion: June 2007)	Not complete but in process	Complete	Complete
1.30 Federal departments and agencies, with coordination and assistance from the PM-ISE, will encourage bilateral and multilateral efforts whenever feasible and appropriate to develop "best practices" on terrorism information sharing (e.g., protocols on what to do if there is a "hit"). (Planned completion: Ongoing with a first progress report in the second quarter of Calendar Year 2007)	Not complete but in process	Not complete but in process	Work towards this action item was underway at the end of phase 1. For example, according to officials at the Office of the PM-ISE, work towards establishing a baseline on information-sharing agreements was underway. Further, an initial progress report on this effort is expected to be provided as part of an overall project plan from implementation guideline 4, which addresses facilitating information-sharing with foreign partners.
1.31 The Department of State's Foreign Service Institute, supported by the working group of ISC training representatives, will develop the core training module that will serve as the common educational baseline for the ISE. (Planned completion: June 2007)	Not complete but in process	Not complete but in process	Development of the core training module to serve as the common educational baseline for the ISE has been underway. To date, the Foreign Service Institute and ISC have undergone several iterations of review and comment on draft versions of the training course. According to PM-ISE officials, a November 2007 review of the course by the ISC led to further revision and updating of the course outline and content, with the intent to incorporate additional computer based training capabilities. Also, in February 2008 a focus group met to further revise the course content and structure.

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
1.32 The PM-ISE, in consultation with the ISC, will review departmental incentives for sharing of terrorism information and will measure their effectiveness. (Planned completion: June 2007)	Not complete but in process	Not complete but in process	According to a PM-ISE status report on the identification of incentives for information-sharing, the PM-ISE is in the process of developing guidance to federal departments and agencies to assist them, where necessary, in expanding current or developing new capabilities to recognize efforts that further promote a culture of terrorism information sharing across federal agencies and non-federal government entities. Also, an initial measure to identify whether or not departments and agencies have adopted incentives for sharing has been developed. As an initial step towards assessing the effectiveness of these incentives, the PM-ISE is also seeking to collect information on how best practices for incentives have been shared.
1.33 Each agency will ensure that one or more ISE Privacy Officials are designated in accordance with paragraph 12.a of the privacy guidelines. (Planned completion: December 2006)	Complete	Complete	Complete
1.34 The PM-ISE will establish and designate a chair for the ISE Privacy Guidelines Committee. (Planned completion: December 2006)	Complete	Complete	Complete
1.35 The PM-ISE, in consultation with the ISE Privacy Guidelines Committee and the ISC, will establish a process for ensuring that non-Federal organizations participating in the ISE implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in the Guidelines. (Planned completion: March 2007)	Complete	Complete	Complete
1.36 The ISE Privacy Guidelines Committee will provide an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections, to be included in the President's first annual ISE performance report. (Planned completion: June 2007)	Not complete but in process	Complete	Complete

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
1.37 The Guideline 3 Coordinating Committee will complete its work and submit recommendations for sensitive but unclassified standardization through the White House policy process to the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for National Security Affairs. (Planned completion: March 2007)	Complete	Complete	Complete
1.38 To align timelines, the PM-ISE will work with ISC members and other partners to establish cut-off dates for the yearly ISE performance management reports. (Planned completion: March 2007)	Not complete but in process	Complete	Complete
1.39 Federal departments and agencies will use their information sharing and terrorism-related Fiscal Year 2006 goals, measures, and outcomes as input to the ISE Performance Management Report. (Planned completion: June 2007)	Not complete but in process	Complete	Complete (Note: According to officials at the Office of the PM-ISE, federal departments and agencies will be expected to use the performance management framework defined in the 2007 annual report to management information sharing performance in 2008.)
1.40 Federal departments and agencies will reflect ISE goals in their individual performance management plans. (Planned completion: March 2007)	Not complete but in process	Not complete but in process	While departments and agencies provided examples of terrorism-related information sharing accomplishments they have participated in, reflecting ISE goals in individual department and agency performance management plans remains a work in process.
1.41 Federal departments and agencies will specify support to the ISE as part of their strategic plans and performance management efforts for the 2006-2007 cycle. (Planned completion: June 2007)	Not complete but in process	Not complete but in process	The September 2007 annual report contained the first set of ISE performance goals. Performance management efforts at individual departments and agencies have incorporated elements of these goals. For example, as reported to the PM-ISE, 10 of 12 ISE related departments and agencies responding the Program Manager's request for baseline information reported that they have established governance bodies specifically to handle information sharing issues.

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
1.42 Federal departments and agencies will work with the PM-ISE to develop specific ISE-wide program outcome goals and measures (performance measures and threshold values), as appropriate, for the goals listed in Section 1.5. (Planned completion: June 2007)	Not complete but in process	Not complete but in process	The September 2007 annual report contained the first set of annual performance goals for the ISE. Work remains in developing outcome oriented goals and measures for the ISE. Nevertheless, performance measures, with ISC contributions, were developed and distributed to agencies for a baseline assessment in September of 2007. These measure have been further refined for use the Spring 2008 assessment and are expected to inform the June 2008 Annual Performance Management Report.
1.43 Federal departments and agencies will provide their mid-year reviews of goals and measures to the PM-ISE (midyear reviews are required by the Information Sharing Guidelines and Requirements). (Planned completion: June 2007)	Not complete but in process	Complete	Complete. (Note: According to PM-ISE officials, this action item was met by completing the ISE's initial baseline assessment of goals and measures conducted in Fall 2007.)
1.44 The PM-ISE, in coordination with the Office of the Director of National Intelligence, will illustrate interdependencies through a "crosswalk" of the ISE, <i>National Intelligence Strategy</i> , and <i>National Implementation Plan</i> goals and measures. The "crosswalk" will be completed by or before December 2006. (Planned completion: December 2006)	Not complete but in process	Complete	Complete
1.45 The PM-ISE and ISC members will develop performance objectives and measures, in cooperation with state, local, and tribal and private sector subcommittees, to address progress against the Guideline 2 framework. (Planned completion: June 2007)	Not complete but in process	Complete	Complete
1.46 The PM-ISE will support the Office of Management and Budget, which will provide federal departments and agencies with budget guidance for fiscal year 2008. (Completed: September 2006)	Complete	Complete	Complete

Action item	Status as of July 9, 2007	Status as of March 1, 2008	Description of status as of March 1, 2008
1.47 The PM-ISE will work with the Office of Management and Budget during the fall budget process to review federal departments' and agencies' investments with ISE priorities and the Office of Management and Budget will provide additional budget guidance to departments and agencies, as appropriate. (Planned completion: December 2006)	Complete	Complete	Complete
1.48 The PM-ISE, with support from the Office of Management and Budget and the ISC, will begin planning for subsequent budget cycles. (Planned completion: March 2007)	Not complete but in process	Complete	Complete
Total complete:	18	33	
Total not complete:	30	15	

Source: GAO analysis based on the Program Manager's reporting.

Appendix II: Comments from Office of the Program Manager for the Information Sharing Environment

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT
WASHINGTON, DC 20511

6 June 2008

Ms. Eileen Larence
Director, Homeland Security and
Justice Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Larence:

The PM-ISE appreciates the efforts of GAO in developing this assessment of the Information Sharing Environment, GAO-08-492. We have worked closely with your very good team throughout this audit and will continue to make every effort to accommodate the principal GAO recommendations to (1) “more fully define the scope and results to be achieved by the ISE and (2) develop a comprehensive set of performance measures that show the extent to which the ISE has been implemented and sharing improved.”

Your report attempts to present the ISE Implementation Plan (November 2006) actions in summary fashion. I suggest that a more up-to-date status report on the ISE can be found in the 2008 ISE Annual Report to Congress (June 2008), which is more current than the data used for this report. The Office of the PM-ISE has now had three years’ experience working the information sharing problem. We are pioneering, at least within the Federal Government, in building a true, extensive government-wide information sharing environment. No one, to my knowledge, has attempted this before. No one, to my knowledge, knows with certainty the correct path, or sees a clear end state of the ISE. Indeed, there is no end state in the true meaning of that term, only a vision.

Of course, many of the principles and practices of program management cited in this report correctly apply to the ISE. But, I do not need to emphasize to you that there is no “school solution” to the problem of information sharing; one size does not fit all; and implementation plans must be flexible and dynamic to adjust to the unforeseen and the unintended.

In retrospect, I deem it a PM-ISE responsibility to convey a better appreciation to GAO for the evolutionary nature of these activities and for what actually has been accomplished in the two particular areas cited in this report. However, I also caution that the ISE is not a traditional “program” as the report describes, and therefore trying to audit an interagency initiative strictly within program parameters presents problems. We are not suggesting that the Program Manager or the Interagency should not be held responsible and accountable for progress, but rather, that trying to audit the ISE as if it

were a formal “program” with clearly identified resources can distract decision and policy makers from understanding actual progress, as well as existing impediments.

Scope of the ISE—“What the ISE is to include”

I would emphasize that the ISE is an evolutionary process that requires attention to both structure and function. ISE stakeholders have been involved in the incremental development of processes, protocols and technology standards that have been documented in a series of publications -- key aspects of which are summarized here to facilitate the task of communicating a better understanding of the full scope and purpose of the ISE. These include the foundations, vision, and purpose for the ISE, as well as a description of the framework and the process invoked to build the ISE.

Foundations: The foundations of the ISE were set forth in the President’s information sharing guidelines and requirements, refined in the ISE Implementation Plan (IP), and fully synthesized in the *National Strategy for Information Sharing (NSIS)*. The President’s guidelines described ISE capabilities in terms of interrelated policies, business processes, standards, and systems, which together constitute the sharing environment envisioned in the Intelligence Reform and Terrorism Prevention Act (IRTPA) and the *NSIS*. The *NSIS* recognizes progress made in information sharing to date and describes the Administration’s “expectations and plans for achieving improvements in the gathering and sharing of information related to terrorism.” It also reaffirmed the vision, goals, and strategies embodied in the ISE Implementation Plan, while acknowledging that today’s sharing environment serves as a *platform* from which to continuously improve the sharing of terrorism-related information among all levels of government, the private sector, and foreign partners.

Vision: The critical question addressed by PM-ISE in developing the future ISE was how best to deliver this vision of the environment—of “a trusted partnership between all levels of government in the United States, the private sector, and our foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America by the effective and efficient sharing of terrorism information.” The challenge lay in reconciling myriad policy, process and technology differences among multiple organizations tasked to perform a variety of disparate missions. These differences posed real impediments to ISE success, including conflicting or incompatible policies, processes, and procedures for information classification, access vetting, security and privacy; incompatible or non-interoperable legacy systems and data formats; conflicting approaches to information sharing; and conflicting management structures for overseeing information sharing partners. With these challenges in mind, PM-ISE, in consultation with the Information Sharing Council, has pursued the following clearly defined purpose for the ISE.

Purpose: The purpose of the ISE is to *rationalize, standardize, and simplify* the policies, business processes, standards, and systems used to share information. Although the ISE strives to achieve as much uniformity as possible, actual

**Appendix II: Comments from Office of the
Program Manager for the Information Sharing
Environment**

implementation varies from community to community due to disparate mission needs and the immediate capabilities of each. By way of example, State and local processes and policies will not be identical to those of the Federal Government; nor will the needs of most cities be the same as those of major urban areas. Accordingly, rather than striving to develop identical implementation across the ISE, the intent has consistently focused on being able to achieve the best possible capabilities—based on a common framework supplemented by mutually agreed, mostly common policies, business processes, standards, and systems—but flexibly tailored to diverse ISE participant requirements.

Requirements:

In an *evolutionary process* without a *fixed end-point*, policies, business processes, standards, and systems all have to be regularly reviewed and refreshed—through discrete phases or maturity levels—from “ad hoc” to “managed” to “defined,” and ultimately, to “optimized.” The current state of the ISE is that it is moving from “managed” to “defined” as a result of the significant steps taken to break down barriers and improve sharing practices in selected critical areas. To reach the “optimized” phase, organizational cultures must progress to a point where sharing is fully institutionalized and ingrained into all aspects of day-to-day operations.

The ISE Implementation Plan (which formed the basis for the majority of the GAO conclusions and recommendations in this report), is a particularly useful document that accomplished its intended purpose—to prepare the effort of building the ISE. The ISE Implementation Plan was not intended, however, to control every step made in furtherance of the ISE. It was a plan to implement a vision, not to complete a program.

What made sense in the 2006 plan requires reassessment and modification at each juncture in the development process. That plan was developed in response to a number of drivers. Among them was the need:

- to further define and scope the ISE;
- to identify a course of action that was timely and strategically responsive to Congress (IRTPA) and the President (Guidelines and Requirements);
- to meet immediate, tactical requirements of ISE participants – federal, state, local, tribal governments, the private sector, and foreign allies and partners

Creating the ISE defined by Congress—an “*approach that facilitates the sharing of terrorism information*”—required the PM-ISE to establish a plan to incrementally examine the full range of available, but evolving, technology, policy and governance structures, and the dimensions of structural transformation. Absent any specific ownership of the information sharing problem – it requires highly decentralized systems and networks capable of serving the full range of ISE stakeholders with the equities of each taken into account.

Performance Measures – what has been achieved

Progress in implementing the ISE is a function of four steps: (1) identifying, prioritizing, and measuring continuous improvements to ISE capabilities by modifying processes or creating new ones; (2) issuing guidance and standards to ISE participants; (3) providing demonstrable evidence of the effects of these changes through selected information sharing pilots and evaluation environments; and (4) incorporating these improvements into established government resource management processes. The following paragraphs describe how ISE progress is being measured and how it influences department and agency investment strategies.

PM-ISE introduced a performance management approach in the 2007 Annual Report to Congress to systematically assess ISE implementation, identify improvement opportunities, comply with applicable mandates, and bolster long-term, sustainable performance management. This approach aligns ISE performance measurement areas to each of the 2008 Performance Goals, which in turn are aligned to the four ISE functional areas presented in the 2008 Annual Report. PM-ISE developed 2008 Performance Goals for each of the functional areas to articulate the expected results of ISE implementation, and established measurement areas, including a suite of both current and planned measures, to demonstrate progress for each of the Performance Goals. Using that approach and the performance measures, PM-ISE established an ISE baseline of performance in fall 2007, and measured agencies' progress against this baseline through an assessment performed in spring 2008. The result provided better insight into how the ISE fared in response to the 2008 Performance Goals. Performance goals for 2009 have also been revised to ensure alignment with relevant ISE IP and NSIS themes.

For the first time, the fall 2007 and spring 2008 performance assessments provided the PM-ISE with fact-based data to support decisions and report ISE implementation progress against the information sharing mandates of IRTPA, the 9/11 Commission Act, the President's Guidelines and Requirements, and the NSIS. The comprehensive set of performance measures required to assess ISE implementation as well as improvements in the state of information sharing were developed in conjunction with ISE stakeholders. The 2008 ISE Performance Goals reflect corresponding ISE functional areas and provide the target levels of performance against which actual achievement can be compared. These performance measures are now being applied successfully; each is reported more fully in the 2008 Annual Report to Congress.

Conclusion

There is mention in the report that one of the challenges of the ISE is interagency attention and priority to ISE initiatives. However, there is no accompanying recommendation that, as the President clearly delineated in his December 2005 Guidelines and Requirements Memorandum (addressed directly to "Heads of Executive Branch Departments and Agencies), and then re-emphasized in his October 2007 NSIS, that such "heads of executive departments and agencies must actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism information sharing, by

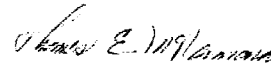
**Appendix II: Comments from Office of the
Program Manager for the Information Sharing
Environment**

reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information.” Agencies and their leaders must be evaluated and held directly accountable for ISE progress and they must put effective information sharing strategies and programs in place within their agencies.

The ISE is a government-wide transformational effort that needs to be evaluated as such. It must not be looked at as simply a project or program of the PM-ISE. This is not to say that programmatic evaluations are not useful, helpful, and necessary in a broader evaluation of the ISE effort; they are. But they are not sufficient.

We appreciate the opportunity to work with you on this assessment and look forward to a continued dialog.

Sincerely,



Thomas E. McNamara

Appendix III: GAO Contacts and Acknowledgments

GAO Contacts

Eileen R. Larence (202) 512-8777 or larencee@gao.gov, or David A. Powner at 202-512-9286 or pownerd@gao.gov

Acknowledgments

In addition to the contact named above, Susan H. Quinlan, Assistant Director; Richard Ascarate; Jason Barnosky; Amy Bernstein; Joseph Cruz; Thomas Lombardi; Lori Martinez; and Marcia Washington made key contributions to this report.

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